BY ORDER OF THE SECRETARY OF THE AIR FORCE

SPACE FORCE INSTRUCTION 13-604

30 AUGUST 2023

SPACE OPERATIONS COMMAND

Supplement

2 MAY 2025

Nuclear, Space, Missile, Command and Control

SYSTEM ACCEPTANCE

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: This publication is 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: SF/COO/X

Certified by: SF/COO
(Lt Gen DeAnna Burt)

Supersedes: AFSPCI10-605, 20 June 2016

Pages: 40

(SPOC)

OPR: HQ SpOC/S553

Certified by: HQ SpOC/CD

Pages: 24

This publication implements Air Force Policy Directive (AFPD) 13-6, *Space Policy*, and Department of the Air Force Policy Directive (DAFPD) 63-1, *Integrated Life Cycle Management*. It provides guidance and procedures on system acceptance throughout the Space Force. This publication applies to uniformed members of the United States Space Force (USSF) and Department of the Air Force (DAF) civilian employees. This publication does not apply to the United States Air Force (USAF). USSF information systems processing both Special Access Program (SAP) and Sensitive Compartmented Information (SCI) will adhere to the more restrictive policies of each of the respective SAP and SCI communities. This publication may be supplemented. This publication may be supplemented at any level, but all supplements must be routed to the Office of Primary Responsibility (OPR) listed above for coordination prior to certification and approval. Refer recommended changes and questions about this publication to the OPR listed above using the DAF Form 847, *Recommendation for Change of Publication*; route DAF Forms 847 from the field through the appropriate chain of command. The authorities to waive delta/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See DAF Manual (DAFMAN) 90-161, *Publishing*

Processes and Procedures for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the requestor's commander for non-tiered compliance items. Ensure all records generated as a result of processes prescribed in this publication adhere to Air Force Instruction (AFI) 33-322, *Records Management and Information Governance Program*, and are disposed in accordance with (IAW) the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System.

(SPOC) SPFI 13-604, *System Acceptance*, is supplemented as follows: This supplement provides further guidance and procedures on system acceptance throughout Space Operations Command (SpOC). This publication applies to all civilian employees and uniformed members of SpOC and all reserve and guard components in support of SpOC missions. This publication does not apply to the USAF. This publication may be supplemented at any level, but all supplements must be routed to the Office of Primary Responsibility (OPR) listed above for coordination prior to certification and approval. Refer recommended changes and questions about this publication to the OPR listed above using the DAF Form 847, *Recommendation for Change of Publication*; route DAF Forms 847 from the field through the appropriate chain of command. The authorities to waive delta/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See DAF Manual (DAFMAN) 90-161, *Publishing Processes and Procedures* for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the requestor's commander for non-tiered compliance items. Ensure all records generated because of processes prescribed in this publication adhere to Air Force Instruction (AFI) 33-322, *Records Management and Information Governance Program*, and are disposed in accordance with (IAW) the Air Force Records Disposition Schedule, located in the Air Force Records Information Management System.

SUMMARY OF CHANGES

This document supersedes AFSPCI 10-605, Operational Acceptance Process, 20 June 2016. This instruction contains an increased scope to cover fielding and operational acceptance, authorities and processes within the current USSF organization structure, distinction between systems developed for force presentation and those not for presentation.

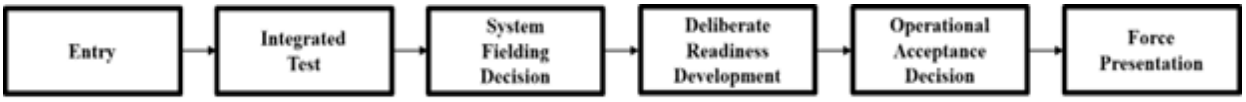
Chapter 1

INTRODUCTION

1.1. Overview. This instruction defines the USSF system acceptance process necessary to ensure new systems meet operational and institutional requirements, and have the necessary elements required to support mission execution. System acceptance is implemented through a thorough and scalable process to deliver essential space warfighting capabilities to the war fighter in accordance with (IAW) Chief of Space Operations (CSO) strategic objectives. System includes, but is not limited to, a weapon system intended for operational employment as part of the joint force, institutional capabilities, service-retained capabilities, software, permanent modifications to existing systems, training systems, and test and evaluation systems.

1.1.1. This instruction defines the six-step process of intentional activities and decision points for transferring systems to the operational unit and fielding the force. These steps, as shown in **Figure 1.1** are: (1) Entry, (2) Integrated Test, (3) Fielding Decision, (4) Deliberate Readiness Development, (5) Operational Acceptance, and (6) Force Presentation.

Figure 1.1. Systems Acceptance Process.



1.1.2. The system acceptance process allows the USSF to receive multiple categories of systems from disparate sources. These categories of systems are further defined in **paragraph 3.3**.

1.1.3. The system acceptance process has two exit points. These are driven by the end goal of the system under development.

1.1.3.1. **USSF Institutional Systems.** Systems developed to meet USSF institutional requirements (e.g., test, training, and experimental systems) do not require the full scope of the system acceptance process and are not intended for operational employment. These systems will not be presented to a combatant command (CCMD). These systems exit the process of systems acceptance once the fielding decision is made and the system is fielded as part of an Institutional Force.

1.1.3.2. **Systems for Presentation to CCMDs.** Systems developed to be presented to a CCMD will exit this process when the system is declared operationally accepted and made available for force presentation to CCMDs. Although the system may not be immediately presented to a CCMD, all stakeholders have tested and evaluated the system against development and operational criteria and requirements, and the operational acceptance authority has declared the system suitable for operational use.

1.2. Cross-Command and Multi-Service Cooperation. Delivery of new systems may involve stakeholders from other commands, services, agencies, commercial, or allied partners. The processes outlined in this instruction rely on mutual support among stakeholders and a clear understanding of what each contributes to the system acceptance process. These stakeholders are responsible to participate in the system acceptance process and provide input to decisions. The system acceptance process generates products and outcomes providing leadership with the

necessary information to make informed decisions. Decision points are inherent in the process to provide the operational acceptance approval authority and stakeholders the opportunity to review and evaluate system performance prior to an operational acceptance decision. These decision points should be completed for approval and advancement to the next step or return to a previous step for further development, test, or evaluation as determined by the approval authority (reference **chapter 2** for organizational roles and responsibilities).

Chapter 2

ORGANIZATIONAL ROLES AND RESPONSIBILITIES

2.1. The Deputy Chief of Space Operations for Operations, Cyber and Nuclear (Chief Operations Officer (COO) or SF/COO).

2.1.1. The operational acceptance approval authority for systems intended for the USSF as determined by the Chief Operations Officer.

2.1.2. The early use approval authority for all systems intended for the USSF.

2.1.3. The rapid deployment approval authority for all systems intended for the USSF.

2.1.4. Recommends the addition of operationally accepted systems to forces assigned or allocated to CCMDs in the Global Force Management processes IAW Chairman of the Joint Chiefs of Staff (CJCSI) 3100.01E, *Joint Strategic Planning System*.

2.1.5. Recommends the removal of systems from assigned or allocated forces IAW CJCSI 3100.01E.

2.1.6. Recommends apportionment of SAP systems into IJSTO IAW DoDD 5205.07, Special Access Program (SAP) Policy and CJCSI 3120.08D, Integrated Joint Special Technical Operations.

2.2. Field Command (FLDCOM) Commander.

2.2.1. The operational acceptance approval authority for all USSF systems for which it has, or will, have overall operational responsibility. Exceptions are those cases when the Chief Operations Officer directs approval at the Service level.

2.2.1.1. **(Added-SPOC)** Operational acceptance and early use approval authorities within SpOC are further delegated per **Table 2.1** except in those cases when the SpOC Commander decides to retain those authorities. Operational acceptance and/or early use approval authority may be raised to a higher level or delegated as determined by SpOC and Mission Delta leadership. Strategic implications and operational risk will be considered when raising or delegating approval authority to ensure decision authority is appropriately aligned with mission requirements.

2.2.2. The gaining FLDCOM Commander, along with the Milestone Decision Authority (MDA), as applicable, is the fielding decision authority for all USSF systems coming to their FLDCOM.

2.2.2.1. **(Added-SPOC)** The SpOC fielding decision authority is further delegated per **Table 2.1** except in those cases when the SpOC Commander decides to retain fielding decision authority. Fielding decision authority may be raised to a higher level or delegated as determined by SpOC and Mission Delta leadership. Strategic implications and operational risk will be considered when raising or delegating approval authority to ensure decision authority is appropriately aligned with mission requirements.

Table 2.1. (Added-SPOC) Fielding Decision (FD)/Operational Acceptance (OA)/Early Use (EU)Approval Authority.

Approval Authority*	Programs/Activity
- SpOC Deputy Commander (SpOC/CD) - SpOC Assistant Deputy Commander for Operations, Plans, Training, and Force Development (SpOC/DS3/5/7)	• Acquisition Category (ACAT) I & II programs • Urgent Capability Acquisition (UON/JUON/JEON) • Section 804 (Middle Tier of Acquisition) programs (Major System) • Programs executing software acquisition pathway with Research, Development, Test, and Evaluation (RDT&E) ≥ $525M • Incoming capabilities from other Services/agencies • Space C2 software pilot program
- SpOC Assistant Deputy Commander for Operations, Plans, Training, and Force Development (SpOC/DS3/5/7) - SpOC/S-Staff Directors (within their mission area)	• ACAT III programs • Section 804 (Middle Tier of Acquisition) programs (Non-Major System) • Programs executing software acquisition pathway with RDT&E < $525M • Capabilities that cross multiple mission areas/Deltas • Space C2 software pilot program
- Mission Delta Commander or Deputy Commander - SpOC/S10 or Deputy S10 for USNDS (*Not further delegable; however, OA Authority may be retained at Headquarters (HQ) SpOC for high-risk deliveries based on SpOC leadership determination.*)	• Permanent modifications of existing weapon systems within their mission area
***NOTE: Foreign exchange officers serving in this role are not authorized to serve as approval authority in accordance with applicable law and policy.*	

2.2.3. Develops and executes an operational acceptance plan and acceptance criteria to include full Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities, and Policy (DOTMLPF-P) elements.

2.2.4. The gaining FLDCOM Commander is the approval authority for interorganizational transfer of a previously operationally accepted system with residual capability for Institutional Forces (e.g., a system transferred from Space Operations Command [SpOC] to Space Training and Readiness Command [STARCOM] for training and/or testing purposes).

2.2.5. Ensures cybersecurity monitoring and testing capability is available and implemented on systems throughout the life cycle of the fielded system.

2.2.6. Ensures cybersecurity testing and evaluation is conducted throughout the acquisition life cycle and integrated with interoperability and other functional testing; and that a cybersecurity representative participates in planning, execution, and reporting of integrated test and evaluation activities as documented in DoDI 5000.02, *Operation of the Adaptive Acquisition Framework*.

2.2.7. **(Added-SPOC)** Responsible for security, Operations Security (OPSEC), and Sensitive Activities Management Office (SAMO) to assess the vulnerabilities, threats, and/or risks associated with observables of a system/capability terrestrially, at launch, and on orbit. Observables include, but are not limited to, personnel, equipment, physical capabilities, Electromagnetic Spectrum, and associated Cyber/IT. These observables must be fully assessed/coordinated throughout the lifecycle of the program and require inputs from acquisitions, testing, and operations to mitigate potential inadvertent discovery of the program regardless of system classification level.

2.2.8. **(Added-SPOC) HQ SpOC Deputy Commander for Combat Support (S1/4/8).**

2.2.8.1. **(Added-SPOC)** Provides subject matter experts to participate in and support the Combat Force Proponent–Fielding Process (CFP-FP) as part of an Integrated Capability Team (ICT). ICT members are responsible for providing expertise and ensuring the completion of deliverables within their respective areas including, but not limited to human capital, logistics and mission sustainment, infrastructure resilience, resource management and special programs.

2.2.8.2. **(Added-SPOC) HQ SpOC Director, Human Capital (S1).**

2.2.8.2.1. **(Added-SPOC)** In coordination with mission owners, assists in the development and validation of human capital requirements and organizational constructs.

2.2.8.2.2. **(Added-SPOC)** Provides subject matter experts to participate in and support the CFP-FP as part of an ICT. ICT members are responsible for providing expertise and ensuring the completion of deliverables within their respective areas.

2.2.8.2.3. **(Added-SPOC)** Executes assigned responsibilities as documented in approved operational acceptance plans.

2.2.8.2.4. **(Added-SPOC)** Confirms there are no unmitigated human capital impacts, or that remaining unmitigated risks are acceptable at operational acceptance.

2.2.8.3. **(Added-SPOC) HQ SpOC Director, Mission Sustainment (S4).**

2.2.8.3.1. **(Added-SPOC)** Serves as HQ SpOC focal point for life cycle logistics management.

2.2.8.3.2. **(Added-SPOC)** Coordinates system/program materiel fielding plans; ensures all aspects of materiel fielding are considered and documented to support operational acceptance.

2.2.8.3.3. **(Added-SPOC)** Provides subject matter experts to participate in and support the CFP-FP as part of an ICT. ICT members are responsible for providing expertise and ensuring the completion of deliverables within their respective areas.

2.2.8.3.4. **(Added-SPOC)** Executes assigned responsibilities as documented in approved operational acceptance plans.

2.2.8.3.5. **(Added-SPOC)** Confirms there are no unmitigated logistics or mission sustainment impacts, or that remaining unmitigated risks are acceptable at operational acceptance.

2.2.8.3.6. **(Added-SPOC)** Co-chairs the Configuration Review Board with the respective operational division representative.

2.2.8.4. **(Added-SPOC) HQ SpOC Director, Resource Management & Special Programs (S8).**

2.2.8.4.1. **(Added-SPOC)** Provides subject matter experts to participate in and support the CFP-FP as part of an ICT. ICT members are responsible for providing expertise and ensuring the completion of deliverables within their respective areas.

2.2.8.4.2. **(Added-SPOC)** Executes assigned responsibilities as documented in approved operational acceptance plans.

2.2.8.4.3. **(Added-SPOC)** For SAP/Special Access Required (SAR) programs, reviews cybersecurity packages for risk determination, authorization consideration, and computer resources. Reviews Program Protection Plans to ensure compliance with applicable Department of Defense (DoD), Joint Staff, DAF, and USSF program guidance for applicable systems. Also reviews cross-domain and cryptologic concerns and information technology documents, as required.

2.2.8.4.4. **(Added-SPOC)** Provides program baseline funding levels and status of Program Objective Memorandum and President's Budget submissions so SpOC Divisions, Deltas, and program offices can assess risk based on program funding levels throughout the Future Years Defense Plan (FYDP).

2.2.9. **(Added-SPOC) HQ SpOC Director, Intelligence (S2).**

2.2.9.1. **(Added-SPOC)** Provides subject matter experts to participate in and support the CFP-FP as part of an ICT. ICT members are responsible for providing expertise and ensuring the completion of deliverables within their respective areas.

2.2.9.2. **(Added-SPOC)** Executes the system acceptance process and serves as approval authority as identified in **Table 2.1.**

2.2.9.3. **(Added-SPOC)** Executes assigned responsibilities as documented in approved operational acceptance plans.

2.2.9.4. **(Added-SPOC)** Confirms there are no unmitigated intelligence, surveillance, and reconnaissance (ISR) issues.

2.2.9.5. **(Added-SPOC)** Presents Directorate-level weapon system capability status at weapon system updates.

2.2.10. **(Added-SPOC) HQ SpOC Deputy Commander for Operations, Plans, Training & Force Development (S3/5/7).**

2.2.10.1. **(Added-SPOC)** Responsible for all operational capabilities generated, presented, and sustained by SpOC while supporting combat force generation, service force provider, and force proponency.

2.2.10.2. **(Added-SPOC)** Executes the system acceptance process and serves as approval authority as identified in **Table 2.1.**

2.2.10.3. **(Added-SPOC)** Utilizes the CFP-FP to shepherd new systems and major upgrades of existing systems to operational acceptance delivering fully burdened space warfighter capabilities ensuring all DOTMLPF-P elements required to support sustained operations are in place. For more information refer to SPOCMAN 13-626, *Combat Force Proponent–Fielding Process.*

2.2.10.3.1. **(Added-SPOC)** Space Command and Control (C2) software pilot program capabilities will adhere to the Responsive Operational Acceptance Plan (ROAP) as opposed to the CFP-FP.

2.2.10.4. **(Added-SPOC)** Provides updates to the SpOC/CC on the status of new systems and significant capability modifications to existing systems as they progress through the system acceptance process towards operational acceptance.

2.2.10.5. **(Added-SPOC) HQ SpOC Director, Current Operations (CUOPS) (S33).**

2.2.10.5.1. **(Added-SPOC)** Assists with the coordination and assessment of observables associated with a system in support of the CFP-FP as part of an ICT.

2.2.10.5.2. **(Added-SPOC)** Provides astrodynamics and space domain awareness sensor assessments in support of the CFP-FP as part of an ICT, and in support of the system acceptance process.

2.2.10.6. **(Added-SPOC) HQ SpOC Director, Future Operations (FUOPS) (S35).**

2.2.10.6.1. **(Added-SPOC)** Executes the system acceptance process and serves as approval authority as identified in **Table 2.1.**

2.2.10.6.2. **(Added-SPOC)** Oversees implementation of CFP-FP to track development activities ensuring new systems and major upgrades to existing systems are ready for operational acceptance.

2.2.10.6.3. **(Added-SPOC)** Ensures an appropriate level of ICT partnership with all external SpOC agencies representing FGEs outside of SpOC's authority.

2.2.10.6.4. **(Added-SPOC)** Executes assigned responsibilities as documented in approved operational acceptance plans.

2.2.10.6.5. **(Added-SPOC)** Presents Directorate-level weapon system capability status at weapon system updates.

2.2.10.7. **(Added-SPOC) HQ SpOC S35 Divisions.**

2.2.10.7.1. **(Added-SPOC)** Executes and/or assists Mission Deltas as applicable in the system acceptance process.

2.2.10.7.2. **(Added-SPOC)** Implements the CFP-FP across their portfolio to track development activities ensuring new systems and major upgrades to existing systems are ready for operational acceptance.

2.2.10.7.2.1. **(Added-SPOC)** Space C2 software pilot program capabilities will adhere to the ROAP as opposed to the CFP-FP.

2.2.10.7.3. **(Added-SPOC)** Appoints a Weapon System Lead (WSL) for each assigned weapon system to execute CFP-FP functions guiding new weapon systems and major upgrades through the CFP-FP. The WSL will establish and lead an ICT comprised of Force Generation Element (FGE) subject matter experts from HQ SpOC Staff, Mission Deltas, program offices, and other external agencies as required to execute all relevant FGEs. ICT members are responsible for providing expertise and ensuring the completion of deliverables within their respective areas. For more information refer to the SPOCMAN13-626.

2.2.10.7.4. **(Added-SPOC)** Responsible for the development and coordination of an operational acceptance plan to include fielding and operational acceptance criteria. Fielding criteria are assessed at materiel release by the MDA IAW DAFPAM 63-128.

2.2.10.7.5. **(Added-SPOC)** Responsible for the development and coordination of trial period and documentation supporting trial period and operational acceptance (e.g., Trial Period Review Panel, briefs, trial period entry/exit/operational acceptance memorandums, etc.) for systems/capabilities where the OA Authority is at HQ SpOC or higher.

2.2.10.7.6. **(Added-SPOC)** Co-chairs the Configuration Review Board with SpOC/S4 representative for modification requests within their mission area.

2.2.10.7.7. **(Added-SPOC)** HQ SpOC/S35D is the office of primary responsibility for the Space C2 System software pilot program and Space C2 system acceptance processes. Responsible for coordinating Space C2 system early use and rapid deployment approvals in coordination with the operational Mission Delta Commander (Delta/CC) and HQ SpOC/S35.

2.2.10.7.8. **(Added-SPOC)** HQ SpOC/S35D is responsible for the development, revision, and implementation of the Space C2 system ROAP.

2.2.10.8. **(Added-SPOC) HQ SpOC Director, Strategic Plans, Policy, & Integration (S55).**

2.2.10.8.1. **(Added-SPOC)** Process owner for system acceptance within SpOC providing oversight and support as needed. Primary interface with USSF OPR for the system acceptance process.

2.2.10.8.2. **(Added-SPOC)** Manages the overall SpOC CFP-FP and serves in an advisory role to WSL and ICT.

2.2.10.9. **(Added-SPOC) HQ SpOC Director, Training & Force Generation (S73).**

2.2.10.9.1. **(Added-SPOC)** Provides subject matter experts to participate in and support the CFP-FP as part of an ICT. ICT members are responsible for providing expertise and ensuring the completion of deliverables within their respective areas.

2.2.10.9.2. **(Added-SPOC)** Executes assigned responsibilities as documented in approved operational acceptance plans.

2.2.10.9.3. **(Added-SPOC)** Responsible for the oversight and coordination of training documentation of new systems and major upgrades of existing systems.

2.2.10.9.4. **(Added-SPOC)** Confirms there are no unmitigated training impacts at operational acceptance, or that remaining unmitigated risks are accepted at the appropriate level.

2.2.11. **(Added-SPOC) HQ SpOC Director, Mission Communication & Data Integration (S6).**

2.2.11.1. **(Added-SPOC)** Executes the system acceptance process and serves as approval authority as identified in **Table 2.1.**

2.2.11.2. **(Added-SPOC)** Provides subject matter experts to participate in and support the CFP-FP as part of an ICT. ICT members are responsible for providing expertise and ensuring the completion of deliverables within their respective areas.

2.2.11.3. **(Added-SPOC)** Executes assigned responsibilities as documented in approved operational acceptance plans.

2.2.11.4. **(Added-SPOC)** Confirms there are no unmitigated cybersecurity risk impacts at operational acceptance, or that remaining unmitigated risks are accepted at the appropriate level.

2.2.12. **(Added-SPOC) HQ SpOC Director, Nuclear Command, Control, and Communications (NC3) Enterprise (S10).**

2.2.12.1. **(Added-SPOC)** Executes the system acceptance process and serves as approval authority as identified in **Table 2.1.**

2.2.12.2. **(Added-SPOC)** Executes assigned responsibilities as documented in approved operational acceptance plans.

2.2.13. **(Added-SPOC) HQ SpOC Judge Advocate.**

2.2.13.1. **(Added-SPOC)** Provides subject matter experts to participate in and support the CFP-FP as part of an ICT. ICT members are responsible for providing expertise and ensuring the completion of deliverables within their respective areas.

2.2.13.2. **(Added-SPOC)** Executes assigned responsibilities as documented in approved operational acceptance plans.

2.2.13.3. **(Added-SPOC)** Confirms there are no unmitigated legal issues at operational acceptance, or that remaining unmitigated risks are accepted at the appropriate level.

2.2.14. **(Added-SPOC) HQ SpOC Public Affairs.**

2.2.14.1. **(Added-SPOC)** Provides subject matter experts to participate in and support the CFP-FP as part of an ICT. ICT members are responsible for providing expertise and ensuring the completion of deliverables within their respective areas.

2.2.14.2. **(Added-SPOC)** Executes assigned responsibilities as documented in approved operational acceptance plans.

2.2.15. **(Added-SPOC) HQ SpOC Safety.**

2.2.15.1. **(Added-SPOC)** Provides subject matter experts to participate in and support the CFP-FP as part of an ICT. ICT members are responsible for providing expertise and ensuring the completion of deliverables within their respective areas.

2.2.15.2. **(Added-SPOC)** Executes assigned responsibilities as documented in approved operational acceptance plans.

2.2.15.3. **(Added-SPOC)** Confirms there are no unmitigated safety impacts at operational acceptance, or that remaining unmitigated risks are accepted at the appropriate level.

2.3. Acquisition Organization Leadership.

2.3.1. The Program Executive Officer and Program Manager execute integrated life cycle management responsibilities for space systems, as documented in DoDI 5000.02 and AFI 63-101/20-101, *Integrated Life Cycle Management*, and related issuances. Ensures appropriate resources and funding to support activities required for operational acceptance and maintains the ability to address deficiencies found during deliberate readiness development.

2.3.2. The Program Manager, in conjunction with STARCOM, defines test and evaluation strategy for engineering and developmental testing. The MDA and Program Manager participate in the fielding criteria, test, and evaluation strategy discussions to ensure systems meet operational requirements.

2.3.3. The MDA (or Service Acquisition Executive [SAE] for Acquisition Categories [ACAT] ID, IB, IC, IAC, and special interest programs) issues a Materiel Fielding Decision Memorandum, following a Materiel Release Review, documenting the decision to authorize the materiel to be fielded. The Program Manager, consistent with DAFPAM 63-128, *Integrated Life Cycle Management*, certifies there are no unmitigated operational risks or deficiencies over the lifecycle affecting the performance or fielding of the system, or remaining unmitigated risks or deficiencies are accepted by the appropriate authority. The Program Manager also ensures a safety release has been completed IAW DAFI 91-202, *The US Air Force Mishap Prevention Program*, or applicable safety guidance.

2.3.4. The Program Manager delivers the new or modified systems to the operational user(s).

2.4. Space Training and Readiness Command Commander.

2.4.1. Conducts independent integrated test and evaluation of appropriate USSF systems and delivery of timely, accurate, and expert information in support of system development, fielding, and operational acceptance IAW DoDI 5000.89, *Test and Evaluation*, and DoDI 5000.89_DAFI 99-103, *Capabilities-Based Test and Evaluation*. The independent testing and evaluations will include Blue Team vulnerability evaluations and intrusion assessments (e.g., cooperative vulnerability identification and cooperative vulnerability & penetration assessment, cybersecurity inspection/assessments, and red team operations [e.g., adversarial assessment]). **(T-1)**

2.4.1. **(SPOC)** Cyber vulnerability testing must incorporate effective assessment of known adversary capabilities and their ability to penetrate U.S. networks associated with our systems. To accomplish this, a current Intelligence Community (IC) approved Adversary Cyber Threat Assessment (ACTA) may be requested by the acquisition organization's integrated intelligence professionals in conjunction with STARCOM. The ACTA will outline known adversary cyber

techniques used in other forums to defeat U.S. cybersecurity defenses and is used to set up network penetration testing. **(T-2)**

2.4.2. Analyzes collected test data against an objective evaluation framework and delivers timely and accurate decision-quality results.

2.4.3. Provides recommendations via results briefings or written reports to inform the fielding and operational acceptance authority decision-makers.

2.4.4. Provides environment and infrastructure (e.g., range) to conduct tests and evaluations.

2.5. Space Delta Commander.

2.5.1. Reviews technical data in system acceptance documentation for accuracy and completeness and provides feedback.

2.5.2. Provides recommended changes to initial and critical sparing plans in system acceptance documentation for accuracy and completeness.

2.5.3. Utilizes Delta internal processes to address system acceptance support, including providing feedback to the program office during development, test support, scheduling and schedule deconfliction, deployment support, required training provided by other FLDCOMs, required manning, additional required resourcing, and other programmatic issues.

2.5.4. Supports the conduct of the appropriate deployment and employment reviews for operational systems in coordination with service component leads or institutional stakeholders as appropriate, ensuring deficiencies are identified to the appropriate acquisition program office for resolution.

2.5.5. Participates in system acceptance planning/strategy for space systems to clearly identify operational acceptance requirements, testing strategy, and system delivery expectations.

2.5.5.1. **(Added-SPOC)** SpOC Mission Deltas participate in SpOC's CFP-FP to track development activities ensuring new weapon systems and major upgrades to existing weapon systems are ready for operational acceptance. Provide personnel support to the SpOC-led ICT to coordinate system acceptance process actions.

2.5.6. Supports definition and coordination of operational acceptance criteria.

2.5.6. **(SPOC)** Supports development of operational acceptance plans and executes assigned responsibilities as documented in approved operational acceptance plans.

2.5.7. Ensures units are ready to assume day-to-day responsibilities for the system upon fielding decision.

2.5.8. Provides operational acceptance approval recommendation for the operational acceptance decision authority's consideration.

2.5.8. **(SPOC)** Provides fielding decision recommendation for the fielding decision authority's consideration.

2.5.8.1. **(Added-SPOC)** Executes the system acceptance process and serves as approval authority as identified in **Table 2.1.**

2.5.8.2. **(Added-SPOC)** Signatory on the Transition Support Plan (TSP) between the appropriate losing and gaining authorities (e.g. Delta-equivalent commanders).

2.5.8.3. **(Added-SPOC)** Responsible for the development and coordination of trial period and documentation supporting trial period and operational acceptance (e.g., Trial Period Review Panel, briefs, trial period entry/exit/operational acceptance memorandums, etc.) when Mission Delta Commander is OA Authority.

2.5.9. Responsible for managing assigned weapon systems and cannot delegate the responsibility. Unit commanders must approve changes to system operations, within the approved configuration, to manage resources and assure the preservation of system baseline characteristics. **(T-2)** If change impacts currency of the operations technical order, the commander should work with the applicable program office to ensure the update is appropriately documented.

2.6. Space Force Test & Evaluation Director.

2.6.1. Provides oversight of the Space Force Test & Evaluation (T&E) enterprise, to include the Integrated Test Force (ITF), the Integrated Test process, and T&E resourcing.

2.6.2. Reviews Test & Evaluation plans for all USSF systems and provides recommendations for required T&E activities.

2.6.3. Provides recommendations, based on T&E activity results, for system acceptance and/or residual use capability, to the FLDCOM Commander.

Chapter 3

SYSTEM ACCEPTANCE PROCESS

3.1. System Acceptance Process Overview. The system acceptance process is the formal process by which USSF, through FLDCOMs, accepts delivery of a new system or permanent modifications to existing systems. The program office retains overall responsibility for the life cycle management of the system throughout the system life cycle, regardless of operational alignment, transfer, or transition, unless responsibility is agreed to in writing by Chief Operations Officer. The process is intended to be rigid in its structure, but offers flexibility within each step (e.g., tailored test) depending on the entry parameters.

3.1.1. This instruction does not provide guidance regarding Initial Operational Capability (IOC) or Full Operational Capability (FOC) criteria or milestone declarations.

3.1.2. The system acceptance process may be applied more than once during the lifecycle of an acquisition program. The process uses data gathered during acquisition, technical evaluations, and operational evaluations to support a final acceptance decision. The steps within the system acceptance process must be flexible and may be tailored based upon unique requirements of a program. At a minimum, the Program Management Office (PMO), test agencies, Deltas, operational units, and FLDCOM must be fully engaged during this process. **(T-1)**

3.2. System Development. The responsible PMO leads the development of the system and will weigh operational, sustainment, and cybersecurity factors as early and as often as possible throughout the development of a system to minimize risk, cost and performance issues to operators and sustaining organizations. **(T-1)** Systems that collect, process, produce, or consume intelligence data should have intelligence supportability plans, risks, and cost drivers (to include workforce development) identified as outlined in DoDI 5000.86, *Acquisition Intelligence*.

3.3. Entry. This process allows the USSF to receive multiple categories of systems from disparate sources.

3.3.1. The first category of systems to enter the system acceptance process are those that follow the pathways defined in DoDI 5000.02, *The Adaptive Acquisition Framework*. This includes systems acquired by Space Systems Command (SSC) and the Space Development Agency (SDA). Systems in this category are developed to fulfill an operational or institutional need."

3.3.2. The second category of systems to enter this process includes interdepartmental, interagency, commercial, or international transfers. It also includes systems developed and operated by DAF sources external to USSF FLDCOMs or PMOs (e.g., Air Force Research Laboratory, Space Rapid Capabilities Office [SpRCO], and the Missile Defense Agency). Once these systems have met the objectives of the prototype development, experimentation, pathfinder, or operations and they still have utility and usable lifespan, then they may be considered for operational use and system acceptance.

3.3.3. The third category of system to enter this process is the transfer of a previously operationally accepted system to the Institutional Force with the intent to utilize any residual system capabilities (e.g., the transfer of an operationally accepted system from SpOC to STARCOM that is no longer force presented and has residual capabilities for training).

3.3.4. Program managers for systems entering the acceptance process from the first or second category will notify the Future Operations Division (SF/COO/X) workflow at SF.COOX.Workflow@spaceforce.mil upon entry. **(T-1)**

3.3.5. **(Added-SPOC)** For the first and second categories of systems entering the system acceptance process, SpOC will employ CFP-FP to ensure new systems and major upgrades to existing systems are ready for operational acceptance. Space C2 software pilot program capabilities will adhere to the ROAP as opposed to CFP-FP to ensure readiness for operational acceptance. Sustainment modifications to existing systems are not subject to CFP-FP and will be assessed using standard criteria, see paragraph **A4.2.2.** **(T-2)**

3.4. Integrated Test. After entry into the systems acceptance process, each system will undergo test and evaluation IAW Department of Defense guidance for the appropriate acquisition model. **(T-1)** This is to ensure the system meets the design requirements and is effective, suitable, and survivable. Proper evaluation and system development adjudication is required for systems described in paragraphs **3.3.2** **and** **3.3.3** with residual use to be integrated to the USSF.

3.4.1. Integrated test is an essential step for all systems to include cases of interdepartmental, interagency, international, commercial, and residual use systems. This process may be expedited in the case of interagency systems and residual use cases because system development has already been accomplished and the system was operational for the current user.

3.4.2. If the gaining FLDCOM Commander deems that formal test and evaluation is not required, then a commander's estimate shall be required from the gaining unit. **(T-2)** This estimate is required to ensure the gaining unit meets readiness requirements to receive the system or upgrade.

3.5. System Fielding Decision. The fielding decision is the point at which the system and day-to-day responsibility is transitioned from the current owner (e.g., PMO, SpRCO, commercial, or FLDCOM) to the FLDCOM responsible for operating the system. The fielding decision should not be made until the FLDCOM responsible for operating the system has the necessary resources available to begin deliberate readiness development, if required.

3.5. (SPOC) System Fielding Decision. Day-to-day responsibility implies a unit's responsibility to utilize and maintain the system during the current stage in the system acceptance process (e.g., SSC is responsible during capability development, at the fielding decision SpOC is responsible for operations and Satellite Control Authority (SCA) while SSC maintains responsibility for maintenance until operational acceptance). An approved Transition Support Plan (TSP), signed by the appropriate losing and gaining authorities (e.g. Delta-equivalent commanders), should be in place within sufficient time to enable implementation of successful transition prior to fielding to document the actions, responsibilities, and timelines necessary to transfer workload. The TSP should consider elements such as system financial support (Planning, Programming, Budgeting, and Execution), contract scope/management, system configuration management, personnel transfer (either matrixed or Unit Manning Document [UMD] changes), Level 1 and 2 maintenance authorities, crytpo/communications security (COMSEC) management, and cybersecurity/system vulnerability management (Information System Security Manager).

3.5.1. System fielding alone does not constitute full operational capability and should not be used for CCMD-driven operations until formal operational acceptance. The current owner

must plan appropriate resources and funding to support activities to address deficiencies found during deliberate readiness development in a timely manner. **(T-2)** Systems that have been fielded but do not constitute operational capability can be used for test, training, or other institutional activities. Further, for enterprise-wide capabilities/subsystems that support multiple operational programs/systems across an enterprise, operational acceptance criteria will be jointly determined by the user and development communities and documented in an approved operational acceptance plan. **(T-2)**

3.5.2. If the system entered the system acceptance process IAW **paragraph 3.3.1**, collaboration between the FLDCOM and the acquisition MDA is required for a successful fielding. The MDA or SAE authorizes the system for fielding and the FLDCOM Commander retains decision authority to accept the system.

3.5.2.1. **(Added-SPOC)** Fielding-related requirements and fielding acceptance criteria are to be documented in the materiel fielding plan or fielding strategy as well as the transition support plan and operational acceptance plan. For more information on materiel fielding, see DAFI 63-101/20-101, *Integrated Life Cycle Management.*

3.5.2.2. **(Added-SPOC)** The acquisition organization authorizing the system for fielding and SpOC as the gaining operational FLDCOM will collaboratively assess readiness for fielding. The acquisition organization will confirm fielding readiness and SpOC will assess against fielding criteria and either accept or reject the system. If accepted, day-to-day responsibility for the system transitions to SpOC and it enters the deliberate readiness development phase. If rejected, the rationale for not accepting fielding is provided and both the acquisition organization and SpOC determine how to resolve whatever issues prevented fielding. Participants in the fielding decision include the fielding decision authority, the appropriate acquisition organization representative, the SpOC Division, the Mission Delta, appropriate test organization(s) and other stakeholders as appropriate. The Mission Delta Commander has a key role in the fielding decision as the operational commander assumes operational risk. Therefore, the Mission Delta Commander or designated representative will provide a concur/non-concur recommendation on the fielding decision. **(T-2)**

3.5.3. Systems developed to be used for test, training, research and development, and experimental forces are considered fielded once it is determined that they meet development criteria.

3.5.3. **(SPOC)** For systems fielded to SpOC, see **Attachment 4** for information on developing fielding criteria.

3.6. Deliberate Readiness Development. Upon fielding, systems intended to conduct CCMD operations transition to a period of deliberate readiness development. The gaining FLDCOM is responsible for the specific readiness criteria and timelines. Distinguishing between a fielding and an acceptance decision allots a time period for an operational unit to attain proficiency and for the CCMD to increase their employment confidence. This ensures that all parties are ready and able to employ the system when the capability is presented to a CCMD. Deliberate readiness development does not apply to systems fielded with the purpose to fulfill USSF institutional requirements.

3.6.1. A component of deliberate readiness development is the trial period. The trial period provides the operating unit an opportunity to exercise the system using operational techniques and procedures. It ensures the unit is able to perform continued day-to-day operations and all associated support activities. The system will be employed in an operational configuration with sufficient operational safeguards in place to mitigate risk. **(T-2)** Trial period length is determined by the operational acceptance approval authority and is documented in the operational acceptance plan.

3.6.1.1. **(Added-SPOC)** Trial Period Review Panel (TPRP). The responsible SpOC Division, or Mission Delta if OA Authority resides with the Mission Delta Commander, convenes a TPRP to ensure the system or modification is ready to enter or exit trial period. It is chaired by the operational acceptance approval authority unless delegated. Membership should include applicable stakeholders from, but not limited to, HQ SpOC, Mission Delta, operational unit(s), SSC or other acquisition organization, and STARCOM Operational Test Organization. May also consider for membership CCMD representatives, other Services, international partners, and other organizations as applicable.

3.6.1.1.1. **(Added-SPOC)** Trial Period Entry. A TPRP is held prior to trial period entry to ensure the system or modification is ready to enter trial period. If a system or modification is ready to enter trial period at fielding, the fielding decision can occur at the TPRP entry. Ideally, the TPRP entry will occur once all trial period entry criteria have been satisfied. This provides the approval authority the information necessary to make a trial period entry decision. There are instances when certain criteria are not complete, for example, functional checks on the operational system following a software load. In these cases, a conditional trial period entry approval may be granted and the trial period entry memo will clearly state the conditions that must be met prior to the unit entering trial period. The TPRP, with input from stakeholders, results in a trial period entry decision. Trial period entry approval will be documented in a memorandum signed by the appropriate approval authority.

3.6.1.1.2. **(Added-SPOC)** Trial Period Exit. A TPRP is also conducted prior to trial period exit to review how the system or modification performed during trial period and ensure exit criteria are met. This TPRP, with input from stakeholders, results in a trial period exit decision and operational acceptance of the system or modification. For low-risk modifications with a short trial period (e.g., 72 hours) the TPRP exit may be waived by the OA Authority, in which case the conditions for trial period exit will be established at the TPRP entry and documented in the entry memorandum. The operational unit will inform the OA Authority that the conditions for exit were met and the date/time group of exit which will be documented in the operational acceptance memorandum.

3.6.2. In addition to the trial period, the deliberate readiness development phase includes: live training, live fire exercises, mission rehearsals, and tactics development. Each of these activities are used to demonstrate the tactics, techniques, and procedures (TTPs), command and control, intelligence, force protection, logistical, and interoperability elements available to enable mission accomplishment, as well as the full DOTMLPF-P elements required to support sustained operational activities.

3.6.3. The unit gaining a system will require readiness training during deliberate readiness development. **(T-2)** Interdepartmental, interagency, or international transfer authorities have a significant role during this period and are required to provide all necessary documents and procedures to enable a seamless transfer (e.g., TTPs, safety information, technical and operations manuals).

3.6.4. While a system operates in its operational environment with the operations unit, no CCMD-directed operations are authorized at this point without coordination consistent with processes described in paragraphs **3.8.3.1 or 3.8.3.2**. For SpOC systems, exceptions may be granted by SpOC/S3 when fielding of a system requires that CCMD-directed operations must be executed during trial period to accomplish required fielding and operational testing activities (e.g., the use of a ground system in trial period to control operationally accepted satellites that are broadcasting operational signals supporting CCMD-directed operations).

3.7. Operational Acceptance Decision . The final significant decision point in the system acceptance process is the operational acceptance decision. When operational acceptance criteria are met, DOTMLPF-P elements required to support sustained operational activities are in place, risks are deemed acceptable for employment in an operational capacity through coordination with service component leads or institutional stakeholders, and the approval authority declares the new system or modification able to support its operational mission. The operational acceptance approval authority could: 1) accept, 2) accept with liens, or 3) reject a system for operational use. A lien is placed on the operational acceptance decision when a criterion is not met. The lien will be documented in the operational acceptance memorandum along with a designated responsible party to resource and execute the remedy. **(T-1)** Operational acceptance decisions may be executed multiple times within a program's life cycle depending on the unique delivery schedule of capabilities or modifications to a fielded system. For example, the launch of an additional satellite into an existing constellation (e.g., Global Positioning System) may drive an operational acceptance decision for use of that particular asset.

3.7.1. The operational acceptance approval authority declares the new system able to perform its operational mission and is ready for presentation to the CCMD. The approval authority takes recommendations from stakeholders into consideration and is the final approval authority. If the approval authority makes the decision to reject the system for operational use and determines fix actions are necessary, the program office is responsible to lead the effort to rectify the identified issue and/or resource changes needed to meet operational acceptance criteria. By rare exception all Category 1 deficiencies discovered in testing will be addressed by the program office and cleared by the Integrated Test Team IAW T.O. 00-35D-54, *USAF Deficiency Reporting, Investigation, and Resolution,* prior to operational acceptance. **(T-1)** The operational acceptance decision is documented with an operational acceptance memorandum signed by the approval authority, or their delegated representative. The rationale supporting the operational acceptance decision will be documented in the memorandum (e.g., why it was accepted, accepted with lien(s), or rejected a system for operational use). **(T-2)**

3.7.2. The operational acceptance approval authority determines if new systems have: 1) achieved documented operational objectives, 2) demonstrated required levels of reliability and dependability, and 3) accounted for the resources necessary to support sustained operations as defined within the operational acceptance plan.

3.7.3. The operational acceptance plan is a tailored plan that documents the specific actions, timelines, criteria, and organizational responsibilities for operational acceptance of a new system. It is focused from operational testing through deliberate readiness development to operational acceptance and addresses key decision points with corresponding criteria for success.

3.7.4. Operational acceptance plans are developed for new systems and new capabilities to existing systems. Because operational acceptance criteria, decision parameters, risk tolerances and delivery timelines are unique for each program capability, the operational acceptance plan may be a tailorable document to address the unique parameters of each capability delivery. At a minimum, the operational acceptance plan must address the criteria required for an operational acceptance decision. **(T-1)** An initial operational acceptance plan must be approved before Milestone B for major capability acquisition or within two years of start for middle tier acquisition. **(T-1)**

3.7.4. **(SPOC)** If not a major capability acquisition or middle tier of acquisition, the OA Plan must be complete within two years of receiving initial funding. This does not apply to the Space C2 software pilot program which follows the software acquisition pathway, remains in development, and not required to complete within two years of initial funding.

3.7.4.1. Responsibility for developing the operational acceptance plan resides with the FLDCOM that has, or will have, overall operational responsibility for the system. The designated FLDCOM will update the operational acceptance plan when a significant change to the development, fielding, or sustainment of the program or system impacts the ability to execute the plan. The operational acceptance plan is coordinated with identified stakeholders at the level commensurate with the operational acceptance approval authority. Coordination will include the MDA, PM, appropriate FLDCOM directorates, the test unit, the gaining operational unit, and other organizations as required. **(T-2)** Stakeholder meetings may be used to address issues on operational acceptance criteria and other important aspects of the operational acceptance plan. The operational acceptance decision authority is the final approval authority for operational acceptance.

3.7.4.2. **(Added-SPOC)** See **Attachment 3** for an operational acceptance plan template. See the SpOC ROAP for Space C2 pilot program templates (OPR: SpOC/S35D).

3.7.5. Modifications are changes to hardware or software to satisfy an operational mission requirement by removing or adding a capability or function, enhancing technical performance or suitability, or changing the form, fit, function, or interface of an in-service, configuration-managed DAF asset as documented in DAFPAM 63-128. Modifications require an operational acceptance decision, unless the modification includes only operation and maintenance funded actions which preserve a previously established performance through routine, recurring maintenance actions to address product quality or identified vulnerabilities (e.g., software version patching). The PM, FLDCOM directorate, and operational unit coordinate on the level of modification and required decision.

3.8. Force Presentation . Following operational acceptance, the system is ready to be presented to a CCMD. The operational acceptance authority will notify the Force Management Division (SF/COO/S7O) that a system may be included in the Global Force Management processes IAW CJCSI 3100.01E. **(T-0)**

3.8.1. The Chief Operations Officer recommends if a system to be presented to a CCMD for operations adequately supports warfighter requirements. If a system is incorporated into a USSF unit that is not currently assigned to a CCMD, per the Forces For table, then that system will be service retained IAW CJCSI 3100.01E. **(T-0)**

3.8.2. Integrated Joint Special Technical Operations (IJSTO) is the process used by CCMDs and components to plan, task, and employ SAP capabilities. The USSF will apportion SAP capabilities into IJSTO at the earliest opportunity IAW CJCSI 3120.08D, Integrated Joint Special Technical Operations. **(T-0)**

3.8.3. Systems that do not complete the full system acceptance process may still be requested for use by a CCMD. These could be systems that meet an urgent need, and the operational acceptance process cannot be completed in a timely manner. These systems will use the following deviations from the system acceptance process.

3.8.3.1. *Early Use.* Early use is the operational use of a system while it is still in development. Operational users may consider early use of an asset if there is a CCMD-driven operational need and it is deemed necessary and advantageous to deploy the asset to increase military utility with the understanding the asset is still in development. The requesting agency and gaining FLDCOM will coordinate the early use request with the acquiring organization to determine capabilities, limitations, risks, interim procedures, resource requirements and readiness levels. The responsible FLDCOM in conjunction with the gaining command and operations community assesses the feasibility of early use for a system. Users may conduct early use operations in parallel with development and testing activities. The providing program office and gaining FLDCOM will resolve conflicts between operational and developmental priorities on a case-by-case basis. Systems that meet the criteria of early use require Chief Operations Officer approval informed by the FLDCOM responsible for operating the system and the acquisition organization. Early use does not negate the requirement to adhere to the system acceptance process, which still applies to gain an operational acceptance decision.

3.8.3.2. *Rapid Deployment.* Capabilities requiring rapid deployment (e.g., Joint Urgent Operational Needs (JUON), Joint Emergent Operational Needs (JEON), Joint Capability Technological Demonstrations (JCTD), and Urgent Operational Needs (UON)) follow rapid acquisition development processes for fielding. These processes follow tailored acquisition and test activities requiring the execution of the system acceptance process in a compressed/modified timeline to ensure systems can be successfully fielded with required support and acceptable risk. Systems that meet the criteria of rapid deployment systems require Chief Operations Officer approval informed by the gaining FLDCOM responsible for operating the system and the acquisition organization.

DEANNA M. BURT
Lieutenant General, USSF
Chief Operations Officer

(SPOC)

DAVID N. MILLER JR.
Lieutenant General, USSF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

(Added-SPOC) 32 CFR Part 989, *Environmental Impact Analysis Process (EIAP)*, Current Edition

(Added-SPOC) AFI 10-701, *Operations Security (OPSEC)*, 24 July 2019

(Added-SPOC) AFI 17-140, *Architecting*, 29 June 2018

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

AFI 63-101/20-101, *Integrated Life Cycle Management*, 30 June 2022

AFPD 13-6, *Space Policy,* 13 August 2013

CJCSI 3100.01E, *Joint Strategic Planning System,* 21 May 2021

CJCSI 3120.08D, *Joint Special Technical Operations*, 28 January 2013

(Added-SPOC) CJCSM 3130.06D, *Global Force Management Allocation Policies and Procedures*, 20 June 2024

(Added-SPOC) DAFI 17-220, *Spectrum Management*, 8 June 2021

DAFI 90-161, *Publishing Processes and Procedures*

(Added-SPOC) DAFI 91-202, *The Department of the Air Force (DAF) Mishap Prevention Program*, 20 March 2020

(Added-SPOC) DAFMAN 13-201, *Airspace Management*, 10 December 2020

DAFPAM 63-128, *Integrated Life Cycle Management,* 3 February 2021

(Added-SPOC) DoD Manual 5200.45, *Original Classification Authority and Writing a Security Classification Guide*, 17 January 2025

(Added-SPOC) DoDD 3200.15, *Sustaining Access to the Live Training and Test Domain*, 18 December 2013

(Added-SPOC) DoDD 5030.19, *DoD Responsibilities on Federal Aviation,* 6 March 2023

(Added-SPOC) DoDI 4650.01*, Policy and Procedures for Management and Use of the Electromagnetic Spectrum*, 9 January 2009

DoDI 5000.02, *Operation of the Adaptive Acquisition System,* 8 June 2022

(Added-SPOC) DoDI 5000.83_DAFI63-113, *Technology and Program Protection to Maintain Technological Advantage*, 8 March 2022

DoDI 5000.86, *Acquisition Intelligence*, 11 September 2020

DoDI 5000.89, *Capabilities-Based Test and Evaluation*, 13 July 2022

(Added-SPOC) DoDI 5000.91, *Product Support Management for the Adaptive Acquisition Framework*, 4 November 2021

(Added-SPOC) DoDI 8510.01, *Risk Management Framework for DoD Systems*, 19 July 2022

(Added-SPOC) DoDM 5200.01V2, *DoD Information Security Program: Marking of Information*, 24 February 2012

(Added-SPOC) DoDM 5200.01V3, *DoD Information Security Program: Protection of Classified Information*, 24 February 2012

(Added-SPOC) SPFI 10-201, *Force Readiness Reporting*, 27 April 2023

(Added-SPOC) SPOCMAN 13-626, *Combat Force Proponent – Fielding Process*, 2 May 2025

T.O. 00-35D-54, *USAF Deficiency Reporting, Investigation, and Resolution*, 1 September 2015

(Added-SPOC) TO 00-20-2, *Maintenance Data Documentation*, 15 March 2016

(Added-SPOC) TO 00-5-16, *Computer Program Identification Number (CPIN) Management*, 16 September 2019

Prescribed Forms

None

Adopted Forms

DAF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

(Added-SPOC) ACAT—Acquisition Category

(Added-SPOC) ACTA—Adversary Cyber Threat Assessment

(Added-SPOC) APA—Additional performance attribute

(Added-SPOC) ATO—Authorization to Operate

(Added-SPOC) C2—Command and Control

CCMD—Combatant Command

(Added-SPOC) CDD—Capability Development Document

(Added-SPOC) CFP-FP—Combat Force Proponent – Fielding Process (previously OIMD – Operations Integration and Mission Delivery)

(Added-SPOC) CIO—Chief Information Officer

CJCSI—Chairman of the Joint Chiefs of Staff Instruction

(Added-SPOC) CNS—Capability Needs Statement

(Added-SPOC) COMSEC—Communications security

(Added-SPOC) CONEMP—Concept of employment

(Added-SPOC) CONOPS—Concept of operations

(Added-SPOC) COO—Chief Operations Officer

(Added-SPOC) CPIN—Computer Program Identification Number

CSO—Chief of Space Operations

DAF—Department of the Air Force

(Added-SPOC) DAFMAN—Department of the Air Force Manual

(Added-SPOC) DoD—Department of Defense

DOTMLPF-P—Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities, and Policy

(Added-SPOC) DRRS—Defense Readiness Reporting System

(Added-SPOC) DT—Developmental Test

(Added-SPOC) E2E—End to end

(Added-SPOC) eMASS—Enterprise Mission Assurance Support Services

(Added-SPOC) FD—Fielding Decision

(Added-SPOC) FGE—Force Generation Element

(Added-SPOC) FISMA—Federal Information Security Management Act

FLDCOM—Field Command

(Added-SPOC) FYDP—Future Years Defense Plan

(Added-SPOC) HQ—Headquarters

IAW—In Accordance With

(Added-SPOC) ICD—Initial Capabilities Document

(Added-SPOC) IC—Intelligence Community

(Added-SPOC) ICT—Integrated Capability Team

IJSTO—Integrated Joint Special Technical Operations

(Added-SPOC) IMDS—Integrated Maintenance Data System

(Added-SPOC) IS-CDD—Information Systems CDD

(Added-SPOC) IS-ICD—Information Systems ICD

(Added-SPOC) ISR—Intelligence, Reconnaissance, Surveillance

(Added-SPOC) ISSM—Information System Security Manager

(Added-SPOC) IT—Information Technology

(Added-SPOC) ITIPS—Information Technology Investment Portfolio Suite

JCTD—Joint Capability Technical Demonstrations

JEON—Joint Emergency Operational Need

JUON—Joint Urgent Operational Needs

(Added-SPOC) KPP—Key performance parameter

(Added-SPOC) KSA—Key systems attribute

(Added-SPOC) LDTO—Lead Developmental Test and Evaluation Organization

MDA—Milestone Decision Authority

(Added-SPOC) MET—Mission Essential Task

(Added-SPOC) MOE—Measure of effectiveness

(Added-SPOC) MOP—Measure of performance

(Added-SPOC) MTA—Middle Tier of Acquisition

(Added-SPOC) NC3—Nuclear Command, Control, and Communications

(Added-SPOC) NEPA—National Environmental Policy Act

(Added-SPOC) NSA—National Security Agency

O&M—Operations and Maintenance

(Added-SPOC) OA—Operational Acceptance

(Added-SPOC) OPR—Office of Primary Responsibility

(Added-SPOC) OPSEC—Operations Security

(Added-SPOC) OTA—Operational Test Agency

(Added-SPOC) OTO—Operational Test Organization

(Added-SPOC) OT—Operational Test

(Added-SPOC) OV—Operational Viewpoint

PMO—Program Management Office

(Added-SPOC) PM—Program Manager

(Added-SPOC) PNVC—Presidential and National Voice Conferencing

(Added-SPOC) RDT&E—Research, Development, Test, and Evaluation

(Added-SPOC) ROAP—Responsive Operational Acceptance Plan

(Added-SPOC) SAMO—Sensitive Activities Management Office

SAP—Special Access Program

(Added-SPOC) SAR—Special Access Required

(Added-SPOC) SCA—Satellite Control Authority

(Added-SPOC) SCI—Sensitive Compartmented Information

(Added-SPOC) SOI—Space Object Identification

SpOC—Space Operations Command

(Added-SPOC) SpRCO—Space Rapid Capabilities Office

SSC—Space Systems Command

STARCOM—Space Training and Readiness Command

(Added-SPOC) SW-ICD—Software ICD

(Added-SPOC) T&E—Test and Evaluation

(Added-SPOC) TEMP—Test and Evaluation Master Plan

(Added-SPOC) TPRP—Trial Period Review Panel

(Added-SPOC) TSP—Transition Support Plan

TTPs—Tactics, Techniques, and Procedures

(Added-SPOC) UMD—Unit Manning Document

UON—Urgent Operational Needs

USAF—United States Air Force

USSF—United States Space Force

(Added-SPOC) UTC—Unit Type Code

(Added-SPOC) WSL—Weapon System Lead

(Added-SPOC) WSS—Weapon System Sustainment

Terms

(Added-SPOC) Baseline & Monitor Systems and Detect Anomalies—System shall implement and maintain a cybersecurity configuration baseline, to detect and report system anomalies indicative of a cyber-event. System shall monitor the cybersecurity configuration baseline of system functions, and report health status and anomalies to system operators based on system CONOPS.

Category 1 Deficiency—Those deficiencies which may cause death, severe injury, or severe occupational illness; may cause loss or major damage to a weapon system; critically restrict the combat readiness capabilities of the using organization; or which would result in a production line stoppage, and for which there is no viable workaround.

(Added-SPOC) Control Access—System shall only allow identified, authenticated, and authorized persons and non-person entities access or interconnection to system or sub-system elements. The capability shall enforce a validation mechanism to protect the C, I, & A of system resources (e.g., memory, files, interfaces, logical networks).

(Added-SPOC) Ensure Critical Functions and Mission Performance Levels—System partitioning shall implement technical/logical mitigations including logical and physical segmentation. The system shall be able to maintain mission critical functions at minimum performance thresholds identified within the system's concept of operations (CONOPS). Compromise of non-critical functions shall not significantly impact system mission capability.

(Added-SPOC) Institutional Force—Service institutional forces are intended to perform the Service functions described in title 10, U.S. Code, sections 7013(b), 8013(b), and 9013(b), e.g., recruit, organize, supply, equip, train, service, mobilize, demobilize, etc. Operational forces not assigned to CCMDs are "Service-retained." Institutional forces and Service-retained forces remain assigned to the Secretary of the Military Department with an administrative control relationship with their Military Department or Service unless allocated. (CJCSM 3130.06D)

(Added-SPOC) Manage System Performance in Cyber Degraded Situations—Upon anomaly detection or cyber degradation events, the system shall be sufficiently resilient to mitigate cyber-event effects through orderly, structured, and prioritized system responses in order to ensure minimum mission functionality requirements to complete the current mission or return for recovery. Mission commander shall be able to selectively disconnect/disable subsystems that are not critical as well as isolate the system from integrated platform systems.

(Added-SPOC) Minimize & Harden Attack Surfaces—System shall automatically disable all unauthorized ports, protocols, and services (PPS), including access points, by default. Any deviations from PPS baselines shall be approved and documented by a configuration management board. System shall support automated monitoring and logging of system attack surface and associated cyber events.

(Added-SPOC) Protect Information from Exploitation—System shall ensure all data 'at rest' is protected commensurate with its confidentiality and integrity requirements. System shall prevent unauthorized access, use, modification, and transfer/removal of data, including attempted exfiltration, from the system to unauthorized person and non-person entities throughout the system's lifecycle (including development).

(Added-SPOC) Recover System Capabilities—After a cyber-event, the system shall be capable of being restored to a known-good configuration from a trusted source within a specified duration, as determined by the PMO, FLDCOM Commander, and FD/OA/EU Approval Authority (refer to Table 2.1). System recovery shall prioritize critical functions.

(Added-SPOC) Reduce Cyber Detectability—Ensure signaling and communications (both wired and wireless) implemented by the system (or state "supported by system/capability") shall not enable an adversary to monitor and/or target system and/or supported DoD weapon systems through its emanations.

(Added-SPOC) Secure Transmission and Communications—System shall ensure all transmissions and communications of data 'in transit' are protected commensurate with its confidentiality and integrity requirements. System shall only use National Security Agency (NSA) certified cryptographic capabilities.

System—a weapon system intended for operational employment as part of the joint force, institutional capabilities, service-retained capabilities, software, permanent modifications to existing systems, training, and test and evaluation systems.

Vulnerability Assessment—Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

Attachment 2

SUMMARY OF SYSTEMS ACCEPTANCE CONDITIONS AND CRITERIA

A2.1. Entry of system from PMO to be force presented to support CCMD activities.

A2.1.1. IAW **paragraph 3.3.1**, the system will go through the entire six-step process of: (1) Entry, (2) Integrated Test, (3) Fielding Decision, (4) Deliberate Readiness Development, (5) Operational Acceptance, and (6) Force Presentation.

A2.1.2. The system is an operationally accepted system which is available for CCMD activities.

A2.2. Entry of system from PMO for use by an Institutional Force.

A2.2.1. IAW **paragraph 3.3.1**., The system will go through steps one and three of the six-step process: (1) Entry, (3) Fielding Decision.

A2.2.2. The system undergoes a fielding decision by an Institutional Force and will be used for USSF activities.

A2.3. Entry of system from an external agency to be force presented to support CCMD activities.

A2.3.1. IAW **paragraph 3.3.2**, the system will go through the entire six-step process of: (1) Entry, (2) Integrated Test, (3) Fielding Decision, (4) Deliberate Readiness Development, (5) Operational Acceptance, and (6) Force Presentation.

A2.3.2. A commander's estimate is required to ensure the gaining unit is properly postured to receive the system IAW **paragraph 3.4.1**.

A2.3.3. This system is an operationally accepted system which is available for CCMD activities.

A2.4. Entry of system from an external agency for use by an Institutional Force.

A2.4.1. IAW **paragraph 3.3.2**, the system will go through steps one through three of the six-step process of: (1) Entry, (2) Integrated Test, (3) Fielding Decision.

A2.4.2. A commander's estimate is required if integrated test is expedited or not required IAW **paragraph 3.4.1**.

A2.4.3. The system undergoes a fielding decision by an Institutional Force and will be used for USSF activities.

A2.5. Return of system from CCMD operations to an Institutional Force.

A2.5.1. IAW **paragraph 3.3.3**, the system will go through steps one through three of the six-step process of: (1) Entry, (2) Integrated Test (3) Fielding Decision.

A2.5.2. The system will be recommended to be no longer assigned or allocated to CCMDs IAW **paragraph 2.1.2**.

A2.5.3. A commander's estimate is required if integrated test is not required IAW **paragraph 3.4.1**.

A2.5.4. This system is available to be used for USSF activities.

Attachment 3 (Added-SPOC)

OPERATIONAL ACCEPTANCE PLAN TEMPLATE

A3.1. (Added-SPOC) Purpose. The operational acceptance plan documents the specific actions, milestones, criteria, and organizational responsibilities necessary to operationally accept a new system and employ it as an operational capability. It spans from operational testing through deliberate readiness development, including trial period, to operational acceptance. It addresses key decision points with corresponding criteria for success and is tailored for the specific system/capability. The plan includes the fielding decision criteria necessary for SpOC to accept the system from the current owner (e.g., SSC, SDA, SpRCO, Missile Defense Agency, commercial). The plan also contains the criteria required to operationally accept the system. The following template is provided as a guide to developing an operational acceptance plan. It should be tailored for the specific system and may be expanded to include additional sections or information or delete information that does not apply.

Table A3.1. (Added-SPOC) OA Plan Template.

Note: Italicized text describes what information should be included in that section, replace italicized text with appropriate information. Non-italicized text (i.e. Trial Period, Operational Acceptance, Presentation sections) describes those respective events and can be included in the OA plan and expanded on if necessary.

TITLE PAGE. *Name of the system being delivered (e.g., Presidential and National Voice Conferencing (PNVC) End-to-End (E2E) Operational Acceptance (OA) Plan. Include SpOC emblem, date, distribution statement and releasability information. Include overall classification markings on top/bottom of page. Classification markings (if required) will comply with DoDI 5200.48 for Controlled Unclassified Information (CUI) and DoDM 5200.01, Vol 2 for classified information.*

SIGNATURE PAGE. *Include signature blocks for "Submitted by" and "Approval". Approval is the OA Authority. It may be submitted by the respective SpOC Division Chief or Director.*

REVISION HISTORY. *Include a table indicating history of revisions (e.g., Version #, Description of Change, Date, Revised by).*

TABLE OF CONTENTS. *Insert a table of contents showing main and subparagraphs. Include list of enclosures, appendices, tables, and figures as appropriate.*

EXECUTIVE SUMMARY. *A high-level synopsis of the system and how it will progress to operational acceptance. Consider identifying key organizations and their roles (e.g., acquisition organization, operational test organization, SpOC Directorate/Division, Mission Delta, and operational unit). Goal is one half to one page providing enough of an explanation that if it is the only part of the document that is read, the reader knows what is being operationally accepted, why, and how.*

1. INTRODUCTION. *Provide a short explanation of why the system is being delivered (e.g., next generation, fulfills capability gap).*

1.1 Mission Description. *Describe the mission of the system and how it will accomplish it.*

1.2 System Description. *Describe the system to include all aspects as applicable (e.g., space segment, ground segment, control segment). Include key capabilities of the system.*

Figure 1. Operational Viewpoint (OV-1). *Insert an OV-1 either following the mission or system description, wherever is more appropriate.*

2. PROGRAM BACKGROUND. *Consider providing historical context to the system being delivered if beneficial to "how we got here". This should be a brief, high level view.*

3. ROLES AND RESPONSIBILITIES. *List stakeholder organizations and their roles and responsibilities as applicable. Recommend using a Table.*

OFFICE	**ROLES/RESPONSIBILITIES**
HQ SpOC/S35	• OA Authority/chairs TPRPs • etc

4. TESTING

4.1. Test Organizations. *Identify the Operational Test Agency (OTA) and/or Operational Test Organization(s) (OTO), as applicable, designated to perform the day-to-day execution of OTA responsibilities. Also identify the Lead Developmental Test and Evaluation Organization (LDTO).*

4.2. Test and Evaluation (T&E) Management. *Provide a short synopsis of the Test and Evaluation Master Plan (TEMP) or test strategy. Include the level of test and what will be tested (e.g., system under test). Cite the applicable TEMP/Test Plan. Note: intent is not to restate the TEMP/Test Plan, but to provide an understanding of what and how the system will be tested as those test results will support the operational acceptance decision.*

4.3. Cybersecurity testing/assessments. *Provide a short synopsis of cybersecurity testing/assessments, such as a Cybersecurity Vulnerability Assessment which identifies, quantifies, and prioritizes the vulnerabilities in a system using a combination of automated and manual tools to include penetration testing performed by credentialed security professionals. For Top Secret/Collateral and below, as well as SAP mission systems, the Space Authorizing Official (DoD Designated AO) approves the Interim Authority to Test prior to operational testing and the Authority to Operate prior to trial period entry, or a Continuous Authority to Operate, if applicable. For SCI mission systems, the Air Force Intelligence Community Authorizing Official (DoD Designated AO) approves the Interim Authority to Test prior to operational testing and the Authority to Operate prior to trial period entry, or a Continuous Authority to Operate, if applicable. Refer to Attachment 4, paragraph A4.2.1.16.3 for the list of testable cybersecurity criteria or consult HQ SpOC/S66 (collateral systems) or HQ SpOC/S8ZY (SAP/SAR systems) for additional guidance.*

5. FIELDING DECISION. *The fielding decision is the point at which the system and day-to-day responsibility is transitioned from the current owner to SpOC as the FLDCOM responsible for operating and sustaining the system. Identify the organization that will transition the system to SpOC and how it will occur (e.g., what acquisition authority authorizes the system for fielding, what SpOC authority accepts the system, how will this occur). Provide the criteria necessary for SpOC to accept the system from the current acquisition organization. Cite applicable Transition Support Plan.*

6. DELIBERATE READINESS DEVELOPMENT. *Provides time for the operational unit to gain proficiency and increase employment confidence. It may include live training, live fire exercises, mission rehearsals, and/or tactics techniques and procedure development. If any of these activities are planned, describe what will occur and the purpose. Also, identify any measures that must be attained before moving forward (e.g., TTPs in place prior to entering trial period, etc.).*

6.1. Trial Period. A component of deliberate readiness development is the trial period. Trial period provides the operating unit an opportunity to exercise the system using operational techniques and procedures ensuring the unit can perform continued day-to-day operations and associated support activities. The system is employed in an operational configuration performing its operational mission with sufficient safeguards in place to mitigate risk. A Trial Period Review Panel (TPRP) will convene to ensure the system is ready to enter or exit trial period. Trial period length is determined by the operational acceptance approval authority and is documented in the operational acceptance plan.

6.2. Trial Period Length. *Provide the anticipated length of trial period. Describe any unique circumstances regarding how the trial period will be conducted, (e.g., start at main operating center for some extent of time, transfer operations to a backup center for an additional extent of time.)*

6.3. Trial Period Entry Criteria. *Provide the criteria that must be achieved to enter trial period. One technique is to use the OA criteria providing a status at trial period entry. If this technique is used, recommend identifying which criteria must be met prior to entering trial period (e.g., authorization to operate (ATO) in place). Another technique is to list only the essential criteria that must be met to enter trial period. This would be a subset of OA criteria (e.g., all operational test objectives met, favorable operational test (OT) assessment supporting TP entry, successful cutovers, ATCs/ATOs granted, trained/certified operators in place, verified/validated technical data available, fallback procedures established).*

6.4. Fallback Procedures. *Fallback procedures are established to mitigate risk. In the event of a catastrophic failure that may cause death, severe injury, or may cause loss or major damage to a weapon system or critically restricts the combat readiness capabilities of the using organization, it may be necessary to pull the system from trial period (e.g., fallback). These procedures must be established, agreed upon by stakeholders, and clearly understood by operators. While the OA Authority can always direct fallback, consideration should be given to delegating fallback authority to the appropriate operational level (e.g., Commander, Director of Operations, Crew Commander, etc.). Fallback procedures and time necessary to fallback,*

known as fallback time, are annotated in the trial period entry memorandum. If classified, provide point of contact information for who can provide fallback information.

6.5. Trial Period Exit Criteria. *Provide the criteria that must be achieved to exit trial period. Most likely this will be the OA criteria since OA occurs with trial period exit. If OA criteria are listed in an attachment to the OA plan, can refer to that.*

7. OPERATIONAL ACCEPTANCE. Operational Acceptance is the final significant decision point in the system acceptance process. With OA, the OA Authority declares the system/capability can support its operational mission and is ready for presentation to the combatant commands. Stakeholders will confirm readiness for OA within their respective area and make a recommendation to the Approval Authority on whether to OA, OA with a lien(s), or not to OA. OA is documented with an OA memorandum signed by OA Authority or their delegated representative. The rationale supporting the OA decision will be documented in the OA memorandum (e.g., why it was accepted, accepted with lien(s), or not accepted).

8. PRESENTATION. Following operational acceptance, the system is ready to be force presented to a CCMD. The operational acceptance authority will notify the Force Management Division (SF/COO/S7O) that a system may be included in the Global Force Management processes IAW CJCSI 3100.01E.

Enclosure 1: Fielding Criteria

Enclosure 2: OA Criteria

Attachment A: Acronyms

Attachment B: Referenced Documents

Attachment 4 (Added-SPOC)

FIELDING DECISION AND OPERATIONAL ACCEPTANCE CRITERIA

A4.1. (Added-SPOC) Fielding Decision Criteria. The fielding decision is based on fielding criteria. The respective SpOC Division develops and coordinates fielding criteria with the acquiring organization and other applicable stakeholders. The fielding decision should not be made until the FLDCOM responsible for operating and sustaining the system has the necessary resources and support available to begin deliberate readiness development, understanding that more than likely it will not be mature enough for operational acceptance at the time of fielding. The fielding decision follows integrated testing; therefore, those results provide a measure of the operational effectiveness, operational suitability, and survivability (including cybersecurity) of the system, capability, or modification. Consider the following when developing fielding criteria:

A4.1.1. **(Added-SPOC) Major Capability Acquisitions.** For major defense acquisition programs, major systems, and other complex acquisitions, fielding criteria may be the same as operational acceptance criteria, but that criteria would be at a lesser degree of completion at the fielding decision than at OA.

A4.1.2. **(Added-SPOC) Middle Tier of Acquisition (MTA).** For rapidly developed prototypes, fielding criteria may either be the same as operational acceptance criteria (but that criteria would be at a lesser degree of completion at the fielding decision than at OA), or establish fielding criteria that outlines the transitioning of successful prototypes/programs to operations and sustainment, to include:

A4.1.2.1. **(Added-SPOC)** Minimum number of trained personnel.

A4.1.2.2. **(Added-SPOC)** Completion of Developmental Test (DT) and Operational Test (OT).

A4.1.2.3. **(Added-SPOC)** Receipt of DT and OT reports.

A4.1.2.4. **(Added-SPOC)** System has shown that it can meet OA criteria with further maturation during the deliberate readiness development phase.

A4.1.2.5. **(Added-SPOC)** All Category I deficiencies have been resolved or have an acceptable mitigation strategy.

A4.1.2.6. **(Added-SPOC)** A mutually agreed to transition/sustainment plan developed by the acquisition organization.

A4.1.2.7. **(Added-SPOC)** Other criteria as documented in the OA plan.

A4.1.3. **(Added-SPOC) Software Acquisition.** Intended for the timely acquisition of custom software capabilities developed for the DoD and iterates at least annually.

A4.1.3.1 **(Added-SPOC)** For software acquisition programs using the applications path, an initial operational acceptance plan must be approved within one year of entering the execution phase that identifies criteria developed from relevant FGEs within the CFP-FP. Subsequent operational acceptance plans and fielding decisions must be approved for the iterative software releases by meeting user acceptance criteria satisfying operational needs in an operationally representative environment. This does not apply to the Space

C2 software pilot program; refer to the ROAP for operational acceptance plan guidance.

A4.1.3.2 **(Added-SPOC)** For software acquisition programs using the embedded software path, an initial operational acceptance plan and subsequent operational acceptance plans will follow the associated system's schedule.

A4.2. (Added-SPOC) Operational Acceptance Criteria. The operational acceptance decision for a new system or permanent modification to an existing system is based on meeting operational acceptance criteria tailored for the specific system or capability. When determining operational acceptance criteria, start with the applicable requirement document(s) (e.g., Initial Capabilities Document (ICD), Information Systems ICD (IS-ICD), Software ICD (SW-ICD), Capability Development Document (CDD), Information Systems CDD (IS-CDD), Capability Needs Statement (CNS), or AF Form 1067). This is to ensure that the operational acceptance criteria capture the critical elements that a system or capability was developed to satisfy. Operational acceptance criteria should consider Key Performance Parameters (KPP), Key System Attributes (KSA), and Additional Performance Attributes (APA) with regard to Measures of Performance (MOP) and Measures of Effectiveness (MOE). SpOC Divisions are responsible for developing and coordinating operational acceptance criteria with the acquiring organization and key stakeholders.

A4.2.1. **(Added-SPOC) New System/Major Upgrade Criteria.** In SpOC's commitment to deliver fully burdened space warfighter capabilities ensuring all DOTMLPF-P elements required to support sustained operational activities are in place, SpOC Divisions utilize the CFP-FP to shepherd new systems/capabilities to successful operational acceptance. During progression through the CFP-FP, the FGEs can inform the development of operational acceptance criteria. Operational acceptance criteria development is a collaborative effort between the respective SpOC Division, PMO, Mission Delta/operators, operational test organization, and other stakeholders within the ICT to develop realistic and practical operational parameters for assessing system viability. Consider the following when tailoring operational acceptance criteria for a new system or major upgrade to an existing system. It may not be all-inclusive, nor may all apply. Offices listed in parentheses have responsibility for or contribute to the product.

A4.2.1.1. **(Added-SPOC)** System Requirements: Capture system requirements (e.g., KPP, KSA, APA) and acceptable MOP and MOE from applicable requirement documents. (USSF/CSRO)

A4.2.1.2. **(Added-SPOC)** Concept of Employment (CONEMP): A CONEMP is a tactically focused plan which outlines the presentation, employment, and operation of a singular capability (i.e., weapon system). It is informed by DOTMLPF-P requirements. CONEMPS evolve throughout the development of a capability. (SpOC S35 Division/Mission Delta)

A4.2.1.3. **(Added-SPOC)** Security Classification Guide: DoD Manual 5200.01, Volume 3, *DoD Information Security Program: Protection of Classified Information,* DoD Manual 5200.45, *Original Classification Authority and Writing a Security Classification Guide.*

A4.2.1.4. **(Added-SPOC)** International Support Agreements: (HQ SpOC/S559)

A4.2.1.5. **(Added-SPOC)** OPSEC Plan: IAW DAFI 63-101/20-101, *Integrated Life*

Cycle Management, AFI 10-701, *Operations Security (OPSEC)* (HQ SpOC/S339)

A4.2.1.6. **(Added-SPOC)** Information Support Plan: IAW AFI 17-140, *Architecting*

A4.2.1.7. **(Added-SPOC)** Program Protection Plan: IAW DoDI 5000.83_DAFI 63-113, *Technology and Program Protection to Maintain Technological Advantage*, DAFI 63-101/20-101, *Integrated Life Cycle Management* (PMO)

A4.2.1.8. **(Added-SPOC)** Transition Support Plan: IAW DAFPAM 63-128, *Integrated Life Cycle Management* (PMO, SpOC)

A4.2.1.9. **(Added-SPOC)** Life Cycle Sustainment Plan: IAW DAFI 63-101/20-101, *Integrated Life Cycle Management* (PMO)

A4.2.1.10. **(Added-SPOC)** Technical Data Package: IAW DoDI 5000.91, *Product Support Management for the Adaptive Acquisition Framework*, November 4, 2021; MIL-STD-31000, *Technical Data Packages* (PMO)

A4.2.1.11. **(Added-SPOC)** Safety plan in place when applicable; all known mishap risks have been accepted by the mishap risk acceptance authority with concurrence from the system's user prior to approval for operations (HQ SpOC/SE) IAW DAFI 91-202.

A4.2.1.12. **(Added-SPOC)** Funding Levels: Sufficient funding (weapon system sustainment [WSS] & O&M) in the Future Years Defense Program (SSC/S4W; HQ SpOC/S8)

A4.2.1.13. **(Added-SPOC)** Human Capital: Ensure the required human capital (organization, manpower, personnel) is identified, accessed, and trained to meet operational need requirements. (HQ SpOC/S1)

A4.2.1.14. **(Added-SPOC)** Facilities & Infrastructure: Mission systems fielded with resilient and redundant critical infrastructure and facilities capable of operating in all environments. (PMO; HQ SpOC/S4/S8)

A4.2.1.15. **(Added-SPOC)** Computer Program Identification Numbers (CPIN): Assigned to all software requiring or using Mission Critical Software for National Security Systems IAW T.O. 00-5-16, *Computer Program Identification Number (CPIN) Management*. (HQ SpOC/S4)

A4.2.1.16. **(Added-SPOC)** AF Equipment loaded in the Integrated Maintenance Data System (IMDS) as required IAW T.O. 00-20-2, *Maintenance Data Documentation.* (HQ SpOC/S4)

A4.2.1.17. **(Added-SPOC)** Risk Management Framework: Ensure compliance with Federal Information Security Management Act (FISMA) IAW DoDI 8510.01, *Risk Management Framework for DoD Systems (*HQ SpOC/S66 for collateral systems; HQ SpOC/S8ZY for SAP/SAR systems)

A4.2.1.17.1. **(Added-SPOC)** Enterprise Mission Assurance Support Services (eMASS): Assess system specific cybersecurity criteria information to provide tracking and system approval status; current authorization to operate (ATO) (HQ SpOC/S66)

A4.2.1.17.2. **(Added-SPOC)** Registered in the Information Technology Investment

Portfolio Suite (ITIPS) (HQ SF/CTIO)

A4.2.1.17.3. **(Added-SPOC)** The minimum required cybersecurity criteria for monitoring, testing, and evaluating systems include control access, reduce cyber detectability, secure transmission and communications, protect information from exploitation, ensure critical functions and mission performance levels, minimize and harden attack surfaces, baseline and monitor systems and detect anomalies, manage system performance in cyber degraded situations, and recover system capabilities. For more information on these cybersecurity criteria, refer to the terms section in **Attachment 1**. (HQ SpOC/S66 for collateral systems; HQ SpOC/S8ZY for SAP/SAR systems)

A4.2.1.18. **(Added-SPOC)** SAP Information Technology (IT) Integration/Interoperability: SAP IT components of the system must be integrated into or be interoperable with the primary USSF SAP enterprise IT system. Additionally, all information flows into and out of the system should be identified to reduce/eliminate instances of non-optimal means of transferring information (e.g. burning CDs). (HQ SpOC/S8ZY)

A4.2.1.19. **(Added-SPOC)** Equipment/Spares: Sufficient equipment/spares on hand (PMO; HQ SpOC/S4)

A4.2.1.20. **(Added-SPOC)** Training: Training systems with advanced training capability/exercise support; Master Task List; System Training Plan; established Training Planning Team (HQ SpOC/S735)

A4.2.1.21. **(Added-SPOC)** Procedures/TOs: Procedures developed and fully documented technical orders delivered. (PMO, HQ SpOC/S4)

A4.2.1.22. **(Added-SPOC)** Defense Readiness Reporting System (DRRS): Identify Mission Essential Tasks (METs); identify training measurement criteria for personnel, equipment, and training (HQ SpOC/S735) SPFI 10-201, *Force Readiness Reporting*

A4.2.1.22.1. **(Added-SPOC)** Operators/crews: Trained and certified operators/crews and support personnel IAW applicable Resource Readiness C-Level reporting. (Mission Delta) SPFI 10-201, *Force Readiness Reporting*

A4.2.1.23. **(Added-SPOC)** Approved unit type code(s) (UTCs) (HQ SpOC/S1R)

A4.2.1.24. **(Added-SPOC)** Deficiency Resolution: All Category I deficiencies have been resolved or have an acceptable mitigation strategy. Unresolved deficiencies are of acceptable risk and have acceptable risk mitigation and deficiency resolution strategies agreed to by HQ SpOC, Mission Delta, acquisition organization and the operational test organization. (PMO; OTO; HQ SpOC; Mission Delta)

A4.2.1.25. **(Added-SPOC)** Test Results: Demonstrates measures of effectiveness and suitability and that the system and personnel can perform the assigned mission (OTO)

A4.2.1.26. **(Added-SPOC)** Operational Risk: Identify operational risks to allow decision authority to make informed decisions (respective HQ SpOC Division/Directorate; Mission Delta)

A4.2.1.27. **(Added-SPOC)** Spectrum Supportability: For spectrum dependent systems,

all applicable Chief Information Officer (CIO) reviewed Spectrum Supportability Risk Assessments, frequency assignments, spectrum certifications, International Telecommunication Union satellite registrations and disposition of identified discrepancies IAW DoDI 4650.01*, Policy and Procedures for Management and Use of the Electromagnetic Spectrum*, & DAFI 17-220, *Spectrum Management*. (HQ SpOC/S63)

A4.2.1.28. **(Added-SPOC)** Airspace Supportability: For airspace dependent systems, all applicable SAF/IE, HQ FAA, and DoD approved Airspace Proposals, Cooperating Agency Agreements, Records of Decision, National Environmental Policy Act (NEPA) approved implementing and approval documents, inter and intra agency operating/support agreements, and DoD and Federal Safety Risk Management Assessments and mitigations IAW DoDDs 5030.19, *DoD Responsibilities on Federal Aviation,* & 3200.15, Title 32 Code of Federal Regulations, Part 989, *Environmental Impact Analysis Process (EIAP)*, and DAFMAN 13-201, *Airspace Management*. (HQ SpOC/S733A)

A4.2.1.29. **(Added-SPOC)** Deployment Strategy (PMO; respective HQ SpOC/S35 Division; Mission Delta)

A4.2.1.30. **(Added-SPOC)** Disposal/End-of-Life Plan (PMO)

A4.2.2. **(Added-SPOC) Sustainment Modification Criteria.** Instead of developing unique criteria for each modification to an existing system, the following criteria may be used for OA of modifications to an existing system. These criteria are not as extensive as the criteria for a new system or capability since the system has already been operationally accepted. Additional criteria can be added if necessary or annotated as "not applicable" if any don't apply.

A4.2.2.1. **(Added-SPOC)** Data Quality/Effects: Whatever appropriate data quality or effects apply to the weapon system, e.g., metric observations, Space Object Identification (SOI) data, timeliness, etc.

A4.2.2.2. **(Added-SPOC)** Documentation: Identify any updates to documentation (e.g., procedures/technical orders) for operators, maintainers, and/or system administrators necessary due to the modification, and the status of the updated documentation.

A4.2.2.3. **(Added-SPOC)** Training/Evaluation: Identify any training for operators, maintainers, and/or system administrators necessary due to the modification, and the status of the training.

A4.2.2.4. **(Added-SPOC)** Equipment/Spares: Identify changes to equipment/sparing levels required due to the modification, and status of equipment/spares.

A4.2.2.5. **(Added-SPOC)** Cybersecurity: 1) Does the system have a valid Authorization to Operate (ATO), and 2) Have changes to the system (i.e., the modification) been assessed by the system's Information System Security Manager (ISSM) to ascertain if the change has a security impact and coordinated with the Security Control Assessor for the system.

A4.2.2.6. **(Added-SPOC)** Test Results: Demonstrates acceptable levels of effectiveness, suitability, and performance.

A4.2.2.7. **(Added-SPOC)** Deficiencies: That the modification did not cause any

Category I deficiencies, and/or that any deficiencies caused by the modification are of acceptable risk and have acceptable risk mitigation and deficiency resolution strategies.

A4.2.2.8. **(Added-SPOC)** Overall Confidence: That the modification performs as intended and causes no degradation to the system/mission.