Table 4-1 WBS for the SSE Cyber Workflow Process

WBS	Activity	Description	Artifact	OPR/ Supplier	References
Requirements Approving Authority (RAA)	User Requirements	Form High Performance Team (HPT). Provide the Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities and Policy (DOTMLPF-P) changes required to achieve Mission Focused Cyber Hardening (MFCH) for a space and weapon system. Provide tailored Cyber Survivability Attribute (CSA) requirements per each critical space and weapon system function in accordance with the Cyber Survivability Implementation Guide.	• IS-ICD/IS-CDD/ AF Form 1067/ Acquisition Decision Memorandum	• User (MAJCOM) • Program Office • SSE	• Appendix A: USAF SSE Acquisition Guidebook (1.1 IS-ICD, IS-CDD) • Cyber Survivability Endorsement Implementation Guide • DoD AT Desk Reference • DoD AT Technical Implementation Guide (TIG)
1.0	**Acquisition Strategy**				
START	Enter DoD Acquisition Life Cycle	Upon entering the DoD Acquisition Life Cycle for any space and weapon system development, AF Form 1067 or new contract, begin the process laid out in this WBS.			
1.1	**Form Systems Security Working Group (SSWG)**				
1.1.1	Appoint Personnel to SSWG / appropriate IPT	Assemble a team to support the program's protection planning. The size and nature of the project, program, or system will dictate the size and makeup of the protection team. Ensure a lead is appointed to guide and facilitate the SSWG efforts SSWG should include personnel that can cover these functions PM, program protection lead (security management/ information protection), logistics, chief engineer, systems engineer, systems security engineer, information system security manager (ISSM), intelligence, Defense Counter-Intelligence and Security Agency (DCSA), National Security Agency, and representatives from the Cybersecurity Working Group (CyWG), AO, TSN, USAF AT Lead, and IP. **NOTE:** The establishment of the CyWG is recommended within the Program Office and as a sub-group to the Integrated Test Team (ITT). Membership should include, as a minimum, the Chief Developmental Tester (CDT) and cyber representatives from the Operational Test Agency (OTA)/Operational Test Organization (OTO), the Lead Developmental Test Organization (LDTO), and the Functional Management Office (FMO). The CyWG is responsible for integrating and coordinating all Cybersecurity test and evaluation and supporting the Risk Management Framework assessment and authorization process. **NOTE:** It is a best practice for LDTO, OTA/OTO, and participating cyber test agency representatives on the CyWG to also be members of the SSWG.	• PPP Table 1.2-1	• PM	• DoDI 5000.83 • DoDI 5000.90 • DoDI 8510.01 • DoDI 8500.01 • AFI 99-103 • AFMAN 63-119 • AFPAM 63-113 • "Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, p.56155, 4 May 2020. • DoD Cybersecurity Test and Evaluation Guidebook • National Space Traffic Management Policy", Federal Register, Vol. 83, No. 120, Space Policy Directive 3, p. 28969, 21 June 2018. • DASD(SE) "Program Protection Plan Outline & Guidance"
1.1.2	Develop SSWG Charter	Publish a charter with the business rules for SSWG members to ensure Program Protection Planning and documentation is a focused effort based on well-defined objectives.	• SSWG Charter • PPP Section 1.2 and Table 1.2-1	• SSWG	• AFPAM 63-113
1.1.3	Gather Documentation	Collect relevant/available documentation to assist with the subsequent steps in the process. If modifying an existing system, review previously identified vulnerabilities of the system. Information Security Initial Capabilities Document (IS-ICD), Information Security Capability Development Document (IS-CDD), CONOPS, System Requirements Document (SRD), Systems Engineering Plan (SEP), top-level architecture, previous cyber test results/reports, etc.) Transparently share data, to the greatest extent possible, in its native form and require minimal	• PPP Section 1.1	• SSWG	• Appendix B: USAF Combined Process Guide for CPI and CC Identification • Appendix D: Attack Path Analysis (APA) • DoD Cybersecurity Test and Evaluation Guidebook (Phase 1) • AFPD 33-3 • Department of Defense (DoD) Mission Engineering (ME) Guidebook

WBS	Activity	Description	Artifact	OPR/ Supplier	References
		formatting and manipulation. All DoD data will be shared as widely as possible across the Military Services and OSD. Options to prevent data transparency should not be entertained by the Contracting Officer, Engineering Lead and Program Manager.			
1.1.4	Intelligence and Counter-intelligence Documentation	Request the appropriate threat information/products respective to the maturity of the program (i.e. Defense Intelligence Threat Library Threat Module, Technology Targeting Risk Assessment, Validated On-Line Life Cycle Threat (VOLT) Report, Air Force Office of Special Investigations (AFOSI) products, Initial Threat Environment Assessment, and Defense Security Service Threat Assessment).	• PPP Table 5.1-1	• SSWG	• Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA) • Defense Acquisition Guide (DAG) Chapter 7 • AFPD 71-1 • DoDD 5240.02 • DoDI 5000.86, Acquisition Intelligence • DoDI O-5240.24 • AFPAM 63-113 • DoDD 5250.01 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 1)
1.1.5	Conduct Critical Program Information (CPI) Analysis	Conduct the appropriate activities in order to identify, understand, and protect information about the program and information residing in the system being acquired. This includes the identification, classification, and marking of program and system information. Programs identified as having International Acquisition and Exportability (IA&E) content are to be classified, marked, and handled in according to the program SCG. It also provides the basis for a program to understand what information is associated with the program and system, as well as, the importance of that information. Information identified provides the basis for decisions on protections (or other requirements) that must be implemented for the program and the system. Refer to the DAG for additional detail.	• PPP Section 5.3.6 & Table 5.3.6-1 • Statement of Work (SOW) • DD Form 254	• SSWG	• DAG Chapter 9 • DoDM 5200.01 V1-V3 • DoDI 5220.22 CH-2 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 1)
1.2	**Characterize the System**				
1.2.1	User/Stakeholder Requirements and Information	Review and understand what the customer requirements, capabilities, desired effects are. (IS-ICD [CSAs], IS-CDD [CSAs], CONOPS/CONEMP, SRD, etc.). During the JCIDS document approval cycle, ensure that SSWG representation and High Performance Team (HPT) are supporting one another. The HPT provides User inputs to the Safety Critical Functions (SCFs), Mission Critical Functions (MCFs), and functions associated with CPI to inform the top-level architecture and the System Survivability Key Performance Parameter (KPP)/CSAs (Cyber Survivability Attributes) appropriately. **NOTE:** If the program is Pre- Milestone B, this step will generate information to be documented in the IS-CDD **NOTE:** The requirements need to be testable and measurable. This review is also the first step to beginning the MBCRA for test and evaluation.	• Acquisition Strategy (AS) • IS-CDD • Survivability and Vulnerability Program Plan (SVPP) [applicable to Space systems]	• User • SSWG • Survivability Working Group (SWG)	• Appendix A: USAF SSE Acquisition Guidebook (1.1 IS-ICD, IS-CDD) • CJCSI 5123.01H • Cyber Survivability Endorsement Implementation Guide • DAG Chapter 3 Section 4.2.1 • AFI 99-103 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 1). • "Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, Section 4, p.56157, 4 May 2020 • SMC-S-014 (2010), AFSC Standard: Survivability Program Management for Space
1.2.2	Develop System Description	Provide a high-level description of the system and the technology of which it is comprised. Describe the system (including system boundaries and interconnections). For all interconnections, determine requirements	• PPP Section 1.0 and Appendix E, Cybersecurity Strategy (CS)	• SSWG	• DoDI 8510.01 • AFPAM 63-113 • NIST SP800-37 Risk Management Framework for Information Systems and Organizations: A

WBS	Activity	Description	Artifact	OPR/ Supplier	References
		needed to achieve Authorization to Operate (ATO).			System Life Cycle Approach for Security and Privacy • Appendix B: USAF Combined Process Guide for CPI and CC Identification, paragraph 5.5.1 • Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA) • Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, Section 4, p.56157, 4 May 2020 • DoD Cybersecurity Test and Evaluation Guidebook (Phases 1 and 2)
1.2.3	ID Mission Environment(s)	Identify the environments the system is planned to be operated and maintained in, to include geographical areas for deployment/operations and applicable kinetic and cyber threat environments. ME (Mission Engineering) and MIM (Mission Integration Management) activities will be performed as part of concept and system development to inform developmental decisions and ensure the department is systematically investing in the appropriate capabilities, in an integrated and cost effective manner, to meet mission needs. Include system-unique maintenance/test equipment and training systems if applicable.	• PPP Section 1.1	• SSWG	• United States Code (USC) Title 10, § 133a, 133b • DoDI 5000.88 • DoDI 5000.90 • AFI 99-103 • Appendix B: USAF Combined Process Guide for CPI and CC Identification • DoD Cybersecurity Test and Evaluation Guidebook (Phases 1 and 2) • DoD Mission Engineering Guidebook
1.2.4	Bound the System/ID System Boundary	Identify the system boundaries, interconnections/interfaces, and dependencies to include what systems are internal/external to the system boundary. Identify mission dependence that are affected by either connectivity into or out from the space and weapon system. When identifying internal and external dependencies, seek to identify content and connectivity dependencies that can adversely affect system mission, system content, or connectivity that can adversely affect the mission of a connected system. **NOTE:** Based on maturity of program, details of the internal and external boundaries may or may not be known. If unknown, ensure bounding the system is started no later than System Functional Review (SFR). System boundaries should be updated as more information becomes available.	• PPP Section 1.1 and Appendix E	• SSWG	• Appendix B: USAF Combined Process Guide for CPI and CC Identification • Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA) • DoD Cybersecurity Test and Evaluation Guidebook (Phases 1 and 2)

WBS	Activity	Description	Artifact	OPR/ Supplier	References
1.2.5	Conduct CPI Identification/ Analysis	CPI should be identified early and reassessed throughout the life cycle of the program, to include: • Prior to each acquisition milestone • Prior to each system's engineering technical review • Prior to each phase of Cybersecurity and Cyber Resiliency testing (e.g., Phases 3 – 6) • Throughout operations and sustainment • During software/hardware technology updates. • Use applicable CPI tools, Subject Matter Expert (SME), functional decomposition, and data flows to identify candidate and final CPI, as well as, its location. Use the functional decomposition, identified boundaries and system interfaces to develop the list of critical components and determine its criticality. • Classifying CPI COC as per the AT FOUO SCG, Table Entry VI.13. • **NOTE:** PO should follow internal PEO Directorate level coordination process to request final MDA approval. *Programs without CPI are still required to do a PPP*. **NOTE:** CPI protection should commence soon after the CPI has been identified, and, like CPI identification, CPI protection should continue throughout the life cycle of the program. The PO should work with the AT office early to avoid compromised components.	• PPP Section 2.2, Table 2.2-1, Section 3.0 and Section 4.0 • Anti-Tamper Plan	• SSWG	• DoDI 5200.39 • AFPAM 63-113 • DAG Chapter 9 • DoD Critical Program Information (CPI) Horizontal Protection Guidance (HPG) • DoD Anti-Tamper Desk Reference • Appendix B: USAF Combined Process Guide for CPI and CC Identification • Appendix C: Functional Thread Analysis (FTA) • DoD Program Protection Plan Outline & Guidance • DoD Cybersecurity Test and Evaluation Guidebook (Phases 1 and 2)
1.2.6	Functional Thread Analysis	Conduct the functional decomposition, criticality analysis, Vulnerability Analysis (VA) and generate Attack Path Vignettes (APV).	• Criticality Analysis Input, PPP, Appendix C • MBCRA Input	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (1.1 IS-ICD, IS-CDD, and 1.10 Risk Management) • Appendix C: Functional Thread Analysis • ISO 17666: 2016, Space Systems – Risk Management, 1st ed. • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
1.2.6.1	Conduct Functional Decomposition	Decompose the system beginning with the highest-level User requirements. Identify the system-level mission critical functions, safety critical functions, and the functions associated with CPI. **NOTE:** depending on the maturity of the system, the functional decomposition will have higher fidelity. Ultimately, the system should be functionally decomposed to the individual component level.	FTA Report	SSWG	• Appendix D: Attack Path Analysis (APA)
1.2.6.1.1	Conduct Criticality Analysis	An end-to-end functional decomposition performed by systems engineers to identify mission critical functions and components. Includes identification of system missions, decomposition into the functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions. Criticality is assessed in terms of the impact of function or component failure on the ability of the component to complete the system mission(s). Understand the consequence associated with the MCFs, SCFs, and functions associated with CPI in accordance with Section 1.10 of Appendix A: USAF SSE Acquisition Guidebook. Additionally, identify the cyber events, manmade or natural, that will result in the	• Criticality Analysis, PPP Appendix C • MBCRA Input	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (1.1 IS-ICD and IS-CDD, 1.10 Risk Management). • Appendix B: USAF Combined Process Guide for CPI and CC Identification. • Appendix D: Attack Path Analysis (APA). • (U) Anti-Tamper (AT) Security Classification Guide, 30 July 2020 (U//FOUO). • ISO 17666:2016, Space Systems – Risk Management, 1st ed. • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2).

WBS	Activity	Description	Artifact	OPR/ Supplier	References
		system's failure/degradation that affect the mission capabilities as specified by the Requirements Approval Authority (RAA).			• DoDI 5000.83 Tech and PP to Maintain Technological Advantage • DoDI 5000.85 Major Capability Acquisition • DoDI 5200.44 Protection of MCF to Achieve TSN • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2) • Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, Section 4, p.56157, 4 May 2020 • National Space Traffic Management Policy", Federal Register, Vol. 83, No. 120, Space Policy Directive 3, Section 2, p. 28970, 21 June 2018
1.2.6.1.2	Prioritize the Functions	Prioritize the functions based on the User requirements, risk assessments, and intended operational environment (including threats).	• Criticality Analysis Input, PPP Appendix C • FTA Report • MBCRA Input	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (1.1 IS-ICD, IS-CDD, and 1.10 Risk Management) • ISO 17666:2016, Space Systems – Risk Management, 1st ed. • Appendix C: Functional Thread Analysis (FTA) • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2). • Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, Section 4, p.56157, 4 May 2020
1.2.6.2	Deleted.				
1.2.6.3	Conduct Vulnerability Analysis	Analyze inherited vulnerabilities from required system of system connections, including access points and attack paths.	• Vulnerability Analysis	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (1.10 Risk Management) • Appendix C: Functional Thread Analysis (FTA) ISO 17666:2016, Space Systems – Risk Management, 1st ed. • Appendix D: Attack Path Analysis (APA) • (U) Anti-Tamper (AT) Security Classification Guide, 30 July 2020 (U//FOUO) • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2) • Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, Section 4, p.56157, 4 May 2020
1.2.6.3.1	Identify Vulnerabilities	Identify all known and potential vulnerabilities. A vulnerability is any weakness in system design, development, production, or operation that can be exploited to defeat a system's mission objectives or significantly degrade its performance (including exfiltration of data, which can be used to negatively impact mission effectiveness of the targeted system or other mission systems). All aspects must be considered to include the development, production, test, and operational environments; this includes both industry and Government locations.	• PPP Section 5.2, Table 5.2-1 • Risk Management Framework for DoD IT Plan • Inputs to Cybersecurity Risk assessment	• SSWG	• Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA). • DoDI 8500.01 • DoDI 8510.01 • AFI 17-101 • DoD Trusted Systems and Networks (TSN) Analysis • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2) • Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, Section 4, p.56157, 4 May 2020

WBS	Activity	Description	Artifact	OPR/ Supplier	References
1.2.6.3.2	Analyze Entry Access Points and Attack Path Vulnerabilities	Analyze cyber Entry Access Points (EAPs) and Attack Paths. Analyze EAPs and potential cyber vulnerabilities that would allow threats to gain access to the system's CPI or CCs, or to trigger a component malfunction, failure, or inability for the system to perform its intended function. Identify potential weaknesses in the component design, architecture, or code that could be potentially exploited to negatively impact the integrity, confidentiality, and availability of system data. Identify the supply chain, development, production, and test environments and processes that would allow adversaries to exfiltrate/gain access to CPI or introduce components (hardware, software, and firmware) that could cause the system to fail at some later time. Identify potential mission impacts if identified data is compromised. Complete / update the Functional Thread Analysis per Appendix C: Functional Thread Analysis.	• Risk Management Framework for DoD IT Plan. • Inputs to Cybersecurity risk assessment. • FTA Input. • APA Input.	• SSWG • CyWG	• Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA) • DoD Trusted Systems and Networks (TSN) Analysis • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2) • Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, Section 4, p.56157, 4 May 2020
1.2.6.3.3	Generate Attack Path Vignettes	Develop cyber-attack scenarios (i.e., Attack Path Vignettes) that combine identified potential cyber vulnerabilities into operationally representative cyber-attack paths. The Attack Path Vignettes should identify attack path nodes, methodologies, anticipated mission impacts, risk ratings, and potential test methodologies/resources.	• APA Input	• SSWG	• Appendix D: Attack Path Analysis (APA)
1.2.7	DELETED				
1.2.8	DELETED				
1.2.9	Conduct Threat Analysis	Provide supporting Acquisition Intelligence unit the known information developed in WBS 1.2. Acquisition Intelligence unit performs an updated likelihood for the overall risk assessment based on known threat data. **NOTE:** The higher the fidelity of the information provided to the Intelligence Community (e.g., component part numbers if available), the higher the fidelity and relevance of the information the Intelligence Community can provide.	• Inputs to Risk Assessment	• SSWG	• ISO 17666:2016, Space Systems – Risk Management • Appendix A: USAF SSE Acquisition Guidebook (Risk Management). • Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA) • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
1.2.9.1	Determine Scope of Threat Assessment	Consult with SSWG to establish scope and depth of threat assessment to be performed. Identify operational scenarios and threat actors relevant to the system.	• Documentation on bounds of threat analysis to include hardware and software listings, system boundary diagrams, systems engineering drawings/ DoDAFs	• Supporting Acq Intel unit • AFOSI	• United States Code (USC) Title 10, § 133a, 133b • DoDI 5000.88 • DoDI 5000.90 • DoD Mission Engineering Guidebook • AFI 99-103 • Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA) • WBS 1.2.3 (operational environment, deployment locations/scenarios, Acquisition Intelligence Guidebook (AIG))

WBS	Activity	Description	Artifact	OPR/ Supplier	References
					• NIST SP800-30 r1.0 Tasks 1-2 and 1-5 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
1.2.9.2	ID Threat Sources	Determine threat sources to be incorporated into analysis (e.g. adversary nation state, hacker community, insider, supply chain, etc.). Determine threat information sources (e.g. mine existing intelligence/counterintelligence, develop new production requirements, and identify appropriate Production Centers for each threat type).	• Documentation of threats to be considered and sources for intelligence on each threat type • PPP Sections 5.0, 5.1, Table 5.1-2 • Risk Management Framework for DoD IT Plan • Operations Security (OPSEC) Plan	• SSWG • Supporting Acq. Intel Unit • AFOSI	• DoDI 5000.88 • DoDI 5000.90 • DoDI 8510.01 • DoDI 8500.01 • DoD Mission Engineering Guidebook • AFMAN 14-401 • AFI 17-203 • AFMC Acquisition Intelligence Guidebook (AIG) • NIST SP800-30 r1.0 Tasks 1-2 and 1-5
1.2.9.3	ID Threat Events	List possible ways threat sources could exploit potential and known vulnerabilities (of analogous systems).	• Risk Management Framework for DoD IT Plan • OPSEC Plan	• SSWG • Supporting Acq Intel unit • AFOSI • Defense Intelligence Agency (DIA) • National Air & Space Intelligence Center (NASIC)	• Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA) • DoDI 5000.86 • DoDI 5000.90 • DoDI 8510.01 • DoDI 8500.01 • AFI 63-101/20-101 • AFMAN 14-401 • NIST SP800-30 r1.0 • Adversary Cyber Threat Analysis (ACTA) Process • DoD Trusted Systems and Networks (TSN) Analysis • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
1.2.9.4	Conduct System Research	Research the system's operation to include its capabilities, functions, external interactions and key dependencies, CONOPS, combat environment, KPPs, etc. Determine system's cyber dependencies. Identify existing intelligence relevant to the system, its capabilities, and the cyber operational environment, taking into account adversary cyber strategy and doctrine and relevant operational scenarios. Review analysis with SSWG and refine/adjust as required. **NOTE:** Program will provide artifacts to supporting Acquisition Intelligence Unit.	• Production Requirements (PR) Record Copy	• Supporting Acq Intel Unit	• DoDI 5000.83 • DoDI 5000.90 • DoDI 8510.01 • DoDI 8500.01 • Adversary Cyber Threat Assessment (ACTA) step #15 • AFMC Acquisition Intelligence Guidebook (AIG) • NIST SP800-30 r1.0 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
1.2.9.5	Critical Intelligence Parameter (CIP) Breach Review	Assess the impact of changes to adversary capabilities related to the CIP and determines if the breach compromises mission effectiveness of current or future capability solution(s).	• Cyber threat risk matrices	• Supporting • Acq Intel Unit SSWG	CJCSI 5123.01H
1.2.9.6	Translate Intelligence/ Counterintelligence Risk	Use established methodologies, such as Classified Information Compromise Assessment (CICA) and its associated Damage Assessment Report (DAR) to translate Intelligence Community threat rankings to RMF-compatible risk matrices.	• Cyber threat risk matrices	• Supporting Acq Intel Unit • AFOSI	• DoDI 5000.86 • DoDI 5000.90 • DoDI 8500.01 • DoDI 8510.01 • Adversary Cyber Threat Assessment (ACTA) step #16 • AFMC Acquisition Intelligence Guidebook (AIG) • NIST SP800-30 r1.0
1.2.9.7	Deliver Threat Assessment to SSWG	Provide completed forms, associated narrative, and risk transition product to the SSWG.	• Threat Assessment documentation (as required): - Cyber threat risk matrices	• Supporting Acq Intel Unit • AFOSI	• Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA) • DoDI 5000.88 • DoDI 5000.90

WBS	Activity	Description	Artifact	OPR/ Supplier	References
			- Overlays of cyber threats on program design documents - Cyber threat register - Production Center narrative cyber threat analyses - Associated briefings		• DoDI 8510.01 • DoDI 8500.01 • AFI 99-103 • Adversary Cyber Threat Assessment (ACTA) step #16 • AFMC Acquisition Intelligence Guidebook (AIG) • NIST SP800-30 r1.0 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
1.2.10	Unmitigated Initial Risk Assessment	The unmitigated risk assessment is necessary to allow the SSWG to examine the initial risks within the system. The depth of the unmitigated risk assessment will rely on the fidelity of program information. Identify SSE risks by pairing threat events and vulnerabilities; consider all risks to include CPI/CC/TSN/Cybersecurity and Security Management/Information Protection. Document SSE risks in the Program's Risk Register, and capture the resultant risk assessment in the MBCRA products. **NOTE:** This initial risk assessment is titled "unmitigated" because the SSWG has not established any SSE requirements or mitigations based off the known information at this given point in development. Some SSE considerations may be documented in the User requirements, and those will be further decomposed to mitigate any risks identified in this step and hereafter.	• Risk Assessment	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (1.10 Risk Management) • ISO 17666:2016, Space Systems – Risk Management, 1st ed. • Appendix C: Functional Thread Analysis (FTA) • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2) • Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, Section 4, p.56157, 4 May 2020
1.2.10.1	Develop Initial Recommendations	Develop initial set of recommendations that address identified potential cyber vulnerabilities. Evaluate and provide recommendations for the De-Identification of data, drawings and information through a series of effective approaches, algorithms, and tools. Recommendations should include design remediations, exploitation mitigations, test support, and other assessment team recommendations that could help drive a more survivable system.	• Risk Assessment	• SSWG	• Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA) • Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, Section 4, p.56157, 4 May 2020 • NISTIR 8053, De-Identification of Personal Information
1.2.11	Draft Security Classification Guide (SCG)	Conduct appropriate information analysis in order to identify, understand and protect the information about the program that will require classification, and marking considerations. Incorporate the Cybersecurity Security Classification/Declassification Guide for Air Force Weapon Systems. **NOTE:** Ensure SCG addresses functional test plans, cyber test plans, test reports, and vulnerability information/findings, to include potential vulnerability information contained in the MBCRA.	• PPP, Appendix A (SCG)	• SSWG	• DoDI 5200.48 • Cybersecurity Security Classification/Declassification Guide for Air Force Weapon Systems
1.3	**Develop Initial Requirements**				
1.3.1	Conduct Trade Space Analysis	The SSWG conducts a trade space analysis of cost, schedule, and performance for the prioritized MCFs, SCFs, and functions associated with CPI to inform the top-level architecture and the System Survivability KPP/CSAs appropriately.	• Criticality Analysis Input, PPP Appendix C	• SSWG • Survivability Working Group (SWG)	• Appendix A: USAF SSE Acquisition Guidebook (1.1.2 HPT (High Performance Team) Implementation of JCIDS Survivability KPP and CSAs)

WBS	Activity	Description	Artifact	OPR/ Supplier	References
		Trade Space Analysis in: • Producing more complete and robust requirements pre-Milestone A • Making the engineering design process much more efficient and effective • Considering the manufacturability of a proposed design explicitly • Establishing baseline Cyber Resiliency of current capabilities These alternatives are then compared to the Critical Functions of the system to evaluate the risks versus the value of requirement decisions derived from the Trade Space Analysis. These decisions drive the architecture's system boundaries (internal and external) with emphasis on protection of the MCFs, SCFs and functions associated with CPI. These in turn drive the need for repeating a FTA the MCFs and SCFs and their criticality may have changed. **NOTE:** Based on maturity of program, details of the internal and external boundaries may or may not be known.	• Initial Concept Design Review (ICDR) • Survivability and Vulnerability Program Plan (SVPP)		• Appendix B: USAF Combined Process Guide for CPI and CC Identification • Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA) • DASD (SE)/DoD CIO Trusted Systems and Network Analysis • DoDI 5000.02 • DoDI 5000.88 • DoD Cybersecurity Test and Evaluation Guidebook (Phases 1 and 2) • NIST 800-160, Vol. 1 • SMC-S-014 (2010), AFSC Standard: Survivability Program Management for Space, 19 July 2010
1.3.2	Develop Initial Requirements	Develop initial requirements documents (i.e., Statement Of Objectives/ Statement of Work (SOO/SOW) requirements, CDRLs (to include test support deliverables) System Requirements Document (SRD), and System Specifications Requirements). Ensure adequate coverage of SSE requirements and complete traceability to User Requirements / Stakeholder Requirements in WBS 1.2.1. Ensure the Security Management/Information Protection requirements are in the requirements (security clearance requirements, physical security for safeguarding information (Secure Classified Information Facility (SCIF), Special Access Program Facility (SAPF), Open storage facilities, Secret Internet Protocol Router Network (SIPRNet) terminals, storage containers), any additional security features (restricted areas, guns, gates, and guards), training, and start a draft DD 254 to provide. **NOTE:** CyWG representatives within the SSWG should confirm requirements are testable, measurable, and achievable.	• Initial SOO/SOW, SRD/Spec, or equivalent	• SSWG • Survivability Working Group (SWG)	• Appendix A: USAF SSE Acquisition Guidebook (2.2 SRD and System Specification, 2.3 SOO and SOW, and Attachment 1) • NIST 800-160, Vol. 1 • DoD Cybersecurity Test and Evaluation Guidebook (Phases 1 and 2) • SMC-S-014 (2010), AFSC Standard: Survivability Program Management for Space
1.3.2.1	Assess SSE Requirements Implementation	Assess SSE Requirements Implementation using the Excel workbook in Appendix E.	• SSE Requirements Implementation Assessment	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (Attachment 1) • Appendix E: SSE Requirements Implementation Assessment
1.3.3	Submit Production Requirements	Coordinate production requirements (PRs) with supporting Acquisition Intelligence unit. Acquisition Intelligence unit will submit PR to appropriate intelligence/counterintelligence community Production Centers (DIA, NASIC, DIA-TAC, AFOSI, etc.). **NOTE:** Include production requirements for supplier threat information for identified critical components.	• PR Record Copy	• Supporting Acq Intel Unit	• DoDI 5000.83 • DoDI 5000.86 • DoDI 5000.90 • DoDI 8500.01 • DoDI 8510.01 • Adversary Cyber Threat Assessment (ACTA) step #15 • AFMC Acquisition Intelligence Guidebook (AIG) • NIST SP800-30 r1.0
1.4	**Categorize System**				
1.4.1	Identify Critical System Information	Identify and document all the types of information processed, stored, or transmitted by the system and determine their security impact values.	• PPP Appendix E, Cybersecurity Strategy (CS) • Information Technology (IT) Determination or	• PM/Information Security Officer (ISO) • Information System Security	• Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA) • CNSSI No. 1253 • DAG Chapter 9

WBS	Activity	Description	Artifact	OPR/ Supplier	References
			Categorization Document	Manager (ISSM)	• DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
1.4.2	Categorize	Determine and document the confidentiality, integrity and availability (C-I-A) levels. Verify the controls determined, per C-I-A level and AO overlay, are accounted for in the system requirements per Appendix A: SSE AG Attachment 1. Prepare and submit IT Categorization and Selection Checklist for AO approval.	• PPP Appendix E, Cybersecurity Strategy • IT Determination or Categorization Document	• PM • Information Systems Security Officer (ISSO) • ISSM • AO or designee	• Appendix A: USAF SSE Acquisition Guidebook (Attachment 1) • Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA) • AFI 17-101 • CNSSI No. 1253 • NIST SP800-53 v5 • NIST SP800-37 • Federal Information Processing Standards (FIPS) Publication 199 • DoDI 8500.01 • DoDI 8510.01 • DoDI 5000.82 • USC Title 40, Clinger-Cohen Act • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2) • (For AFLCMC Programs) AFLCMC Standard Process for Cybersecurity Assessment and Authorization
1.4.3	Cybersecurity Strategy (CS)	Submit the Cybersecurity Strategy (CS) in accordance with the Clinger-Cohen Act. **NOTE:** The Cyber Test Strategy is captured in the TEMP and summarized in the CS in the "Cybersecurity Testing" Section. The CS shall identify the Testing Integration and Product Evaluation along with the Cryptographic Certification items being incorporated into the system design. The CS also provides the program test ISSP, Number 11 (undated) and the NSA and NIST related certification item testing elements.	• PPP Appendix E, Cybersecurity Strategy	• PM • ISSO • ISSM • AO or designee • CyWG • Test Agencies	• Appendix C: Functional Thread Analysis (FTA) • DoDI 5000.90 • AFI 17-101 • AFMAN 17-1402 • CNSSI No. 1253 • NIST SP800-37 • DoDI 8500.01 • DoDI 8510.01
1.4.4	Register System	Register information systems and Platform Information Technology (PIT) systems, IAW DoDI 8510.01 and AFI 17-101, in Information Technology Investment Portfolio Suite (ITIPS) and Enterprise Mission Assurance Support Service (eMASS).	• eMASS • ITIPS	• PM • ISSO • ISSM	• NIST SP800-37 • DoDI 8510.01 • AFI 17-101 • AFI 17-130
1.5	**Develop Draft Program Documents**				
1.5.1	Intelligence and Counterintelligence Requirements and Documentation	Request, from your program office's assigned Acquisition Intelligence representative, the appropriate threat information/products respective to the maturity of the program, (e.g. Defense Intelligence Threat Library Threat Modules, Technology Targeting Risk Assessment, Validated On-line Life-cycle Threat (VOLT) Report, AFOSI products (as listed in PPP Outline and Guidance V1.0, Section 5.1 and 6.0) and Defense Security Service Threat Assessment).	• PPP Table 5.1-1	• SSWG	• DAG Chapter 7 • DoDI 5000.86 • DoDI 5000.90 • DoDD 5240.02 • DoDI O-5240.24 • AFPAM 63-113 • DoDD 5250.01

WBS	Activity	Description	Artifact	OPR/ Supplier	References
1.5.2	Foreign Participation	Draft Technology Assessment/Control Plan (TA/CP); consider and develop Foreign Military Sales (FMS) strategy with CPI/CC protection decisions moving forward with the Protection Strategy. Consider customization of Defense Exportability Features (DEF) if there is a potential to sell an export variant to a foreign customer in the future.	• PPP Section 8.0 • TA/CP	• PM	• AFI 10-701 • AFI 10-701, AFSC Supplement • AFI 63-101/20-101 • Appendix B: USAF Combined Process Guide for CPI and CC Identification • AT Technical Implementation Guide (TIG) • DoD Anti-Tamper Security Classification Guide (SCG) • DoDI 5200.39 • DoDI 5200.44 • PPP Outline and Guidance V1.0.
1.5.3	MOVED to 1.7.5				
1.5.4	Draft Program Documents	Ensure program artifacts include SSE and cyber test considerations.	• AT Concept Plan • Test and Evaluation Master Plan (TEMP) • SEP • Information Support Plan (ISP) • Life Cycle Sustainment Plan (LCSP) • Draft Program Protection Plan (PPP)	• SSWG • CyWG	• AFI 99-103 • AFLCMC Internal Process Guide for Operational Test & Evaluation (OT&E) Readiness Certification • AFM 99-113 • Appendix A: USAF SSE Acquisition Guidebook (1.0 Programmatic Documents) • AT Plan Template • AT Technical Implementation Guide (TIG) • DAG CH 3-4.3.24 • DOT&E TEMP Guidebook • DoD Cybersecurity Test and Evaluation Guidebook
1.6	**Create/Update LCCE & CARD**	Create/update Life Cycle Cost Estimate (LCCE) & Cost Analysis Requirements Description (CARD) with costs to achieve CPI/CC/TSN/Cybersecurity and Security Management/Information Protection requirements (**WBS 1.3**) for the program.	• PPP Section 11.0, CARD, LCCE, POE	• PM/Chief Engineer/ Financial Mgmt Office	• **Appendix A: USAF SSE Acquisition Guidebook (1.5 Cost Analysis Requirements Description (CARD))** • **DoDI 5000.73, "Cost Analysis Guidance and Procedures", 13 March 2020**
1.7	**Risk Assessment**				
1.7.1	Review Criticality Analysis	Review and update criticality analysis initiated in **WBS 1.2** based on feedback from **WBS 1.3** & **WBS 1.4**, as necessary.	• PPP Appendix C • Updated Criticality Analysis	• SSWG	• Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA) • DAG Chapter 9 • DoDI 5200.44 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
1.7.2	Review Vulnerability Analysis	Review and update the analysis on WBS 1.2.6.3 (vulnerabilities from required system of system connections, including access points and attack paths). **NOTE:** Depending on the maturity of the system, the vulnerability analysis should not be limited to only the system of system connections.	• Updated Vulnerability Analysis	• SSWG	• DoDI 8500.01 • DoDI 8510.01 • DoD Trusted Systems and Networks (TSN) Analysis • ISO 17666:2016, Space Systems – Risk Management, 1st ed. • Appendix A: USAF SSE Acquisition Guidebook (1.10 Risk Management) • Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA) • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2) • Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, Section 4, p.56157, 4 May 2020

WBS	Activity	Description	Artifact	OPR/ Supplier	References
1.7.3	Review Threat Analysis	Review and update threat analysis initiated in WBS 1.2.9, as necessary. Threat information is based on current intelligence and counterintelligence.	• Updated Risk Assessment	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (1.10 Risk Management) • ISO 17666:2016, Space Systems – Risk Management, 1st ed. • Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA) • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
1.7.4	Risk Assessment	Identify SSE risks by pairing threat events and vulnerabilities; consider all risks to include CPI/CC/TSN/Cybersecurity and Security Management/Information Protection. Document SSE risks in the Program's Risk Management Process and System Safety Process. In addition, capture the pairing of threats and vulnerabilities within the MBCRA. Obtain SSE risk approval from the appropriate approving authority (i.e. PM, PEO, SAE, or Chief Information Officer (CIO)). If risk assessment is not approved, return to previous steps necessary to mitigate the unapproved risks. Update SSE Requirements Implementation Assessment.	• Independent Technical Risk Assessment (ITRA). • Risk Assessment • SSE Requirements Implementation Assessment • Hazard Assessment	• IRTA Tea. • SSWG • System Safety Group.	• DoDI 5000.88, Engineering of Defense Systems, Section 3.5 • DoDI 5000.90 • Appendix A: USAF SSE Acquisition Guidebook (1.10 Risk Management) • Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA) • Appendix E: SSE Requirements Implementation Assessment • ISO 17666:2016, Space Systems – Risk Management, 1st ed. • AFI 91-102_AFGM2020-01 • MIL-STD-882E • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2) • AFLCMC Standard Process for Cybersecurity Assessment and Authorization • Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, Section 4, p.56157, 4 May 2020
1.7.4.1	Generate Initial MBCRA Products	Generate FTA & APA Reports documenting identified Entry Access Points, Cyber Boundary, Cyber Attack Paths, potential cyber vulnerabilities, Mission Critical Functions, Safety Critical Functions, and potential operational impacts if the identified potential cyber vulnerabilities are exploited. Update APA for high-risk potential vulnerabilities identified during FTA risk assessment, as needed. Update CTA & cyber test methodology as needed based on any new or changed potential vulnerabilities. **NOTE:** Ensure all resources used, as well as, the analysis processes used, assumptions made, and conclusions reached during the FTA & APA analysis activities are clearly codified in program documents for later reference (particularly during future FTA & APA updates). Resources used for these analyses should be stored in a single resource repository.		• CyWG	• Appendix C: Functional Thread Analysis (FTA) • Appendix D: Attack Path Analysis (APA) • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2) • Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, Section 4, p.56157, 4 May 2020
1.7.5	Risk Management	Integrate risks associated with CPI/CC/TSN/ Cybersecurity and Security Management / Information Protection with the Program Risk Management process. As these risks are identified and managed, they should be included when risks are briefed up the chain of command. **NOTE:** Appropriately classify, mark, and handle security risks.	• Independent Technical Risk Assessment (ITRA). • Program Protection • Acquisition Strategy Panel (ASP) slide (coordination with ACE) • Risk Register	• IRTA Team Lead. • PM.	• Acquisition Center of Excellence (ACE) • DoDI 5000.88, Engineering of Defense Systems, Section 3.5 • ISO 17666:2016, Space Systems – Risk Management, 1st ed. • Appendix A: USAF SSE Acquisition Guidebook (1.2.1 Acquisition Strategy Panel (ASP) and 1.10 Risk Management)

WBS	Activity	Description	Artifact	OPR/ Supplier	References
Acquisition Strategy Decision	Obtain concurrence with the MDA on strategy	If approved, proceed to WBS 2.0 to get RFP approval. If not approved, fix appropriately and go back to Acquisition Strategy.	• ASP CHART	• PM/CE	• Appendix A: USAF SSE Acquisition Guidebook (1.2.1 Acquisition Strategy Panel [ASP])
2.0	**Request for Proposal**				
2.1	**Requirements Analysis**	The Requirements Analysis Process is the method to decompose User needs (usually identified in operational terms at the system level during implementation of the Stakeholder Requirements Definition Process, see DAG Section 4.2.1) into clear, achievable, and verifiable high-level requirements. As the system design evolves, Requirements Analysis activities support allocation and derivation of requirements down to the system elements representing the lowest level of the design. Formal Cyber Survivability requirements allocation for subsystem and box-level specifications are derived by performing an SRA. Various types of SVPP analyses and tests will be performed in support of the SRA. Fundamental to the SRA are the result of trade studies and threat system interaction analyses. This sub-topical area contains information on the Requirements Analysis Process found in the DAG Chapter 3, Section 4.2.2. Generate requirements to mitigate risks and establish protections of CPI, SCF, and MCF.	• Requirements Analysis	• SSWG • Survivability Working Group (SWG)	• Appendix A: USAF SSE Acquisition Guidebook (2.2 SRD and System Specifications, 2.3 SOO and SOW) • MIL-HDBK-520 • DAG Chapter 3 Section 4.2
2.1.1	Finalize Contractor Requirements	Utilizing WBS 1.2, WBS 1.3, and WBS 1.7, finalize contractor requirements (i.e., SOO/SOW to include CDRLs and DIDs). Ensure requirements are included for necessary test support Obtain agreement on the requirements from the AO, TSN, USAF AT Lead, and IP.	• SOO/SOW or equivalent	• SSWG	• DoDI 5000.89 • AFI 99-103 • Appendix A: USAF SSE Acquisition Guidebook (2.3 SOO and SOW)
2.1.2	Finalize System Requirements	Utilizing WBS 1.2, WBS 1.3, and WBS 1.7, finalize system requirements (e.g., SRD/Spec). Allocated Survivability requirements are formally documented (as applicable) in the system and/or segment specifications (Type A specifications), development specifications (Type B specifications), box and/or product specifications (Type C specifications), process specifications (Type D specifications) and material specifications (Type E specifications) Ensure requirements are testable, achievable, and measurable. Obtain agreement on the requirements from the AO, TSN, USAF AT Lead, and IP.	• SRD/Spec or equivalent	• SSWG	• DoDI 5000.89 • AFI 99-103 • Appendix A: USAF SSE Acquisition Guidebook (2.2 SRD and System Specifications)
2.1.3	Alternative Systems Review (ASR)	Conduct ASR, if applicable, per Appendix A: USAF SSE Acquisition Guidebook Section 4.0.	• ASR Meeting minutes	• PM • CE • SSWG	• Appendix A: USAF SSE Acquisition Guidebook (4.1.1 Alternate Systems Review (ASR) or Engineering & Manufacturing Development (EMD) Contract Award)
2.2	**Develop Request for Proposal**	**NOTE:** Recommend having an independent review team assess the RFP for applicability and gaps prior to approval.			
2.2.1	Develop SETR SSE Entry/Exit Criteria	It is a best practice that SETR entrance and exit criteria should be included in the Integrated Master Plan (IMP) in the contract.	• IMP	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (4.1 SETR/IMP)
2.2.2	Select DFARS AFFARS, FAR Clauses	Ensure appropriate clauses are on contract. Contact the contracting officer.	• RFP and Contract	• SSWG • Contracting officer	• DoDI 5000.02 • Appendix A: USAF SSE Acquisition Guidebook (3.1 Request for Proposal (RFP) - Contract Clauses)
2.2.3	Develop Sections L and M Criteria	Section L provides instructions to the Offeror to prepare their proposal. Section M defines Measures of Merit, which includes the factors, sub factors, and elements used to “grade” the Offeror’s proposal.	• Sections L and M	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (3.2 RFP - Section L, 3.3 RFP - Section M)

WBS	Activity	Description	Artifact	OPR/ Supplier	References
2.3	**Programmatic Plans**	Develop/Finalize Information Support Plan (ISP), Life Cycle Sustainment Plan (LCSP), Systems Engineering Plan (SEP), and Test and Evaluation Master Plan (TEMP). Ensure SSE considerations are documented appropriately.	• SEP • TEMP • ISP • LCSP	• SSWG • ITT • CyWG	• DoDI 5000.02 • DoDI 5000.85 • DoDI 5000.88 • DoDI 5000.89 • DoDI 8500.01 • DoD Mission Engineering Guidebook, November 2020 • AFI 99-103 • Appendix A: USAF SSE Acquisition Guidebook (1.7 Information Support Plan (ISP), 1.8 Life Cycle Sustainment Plan (LCSP), 1.11 Systems Engineering Plan (SEP), and 1.12 Test and Evaluation Master Plan (TEMP)) • DoD TEMP Guidebook
2.4	**Risk Assessment**	Update SSE risks in the program's Risk Management Process and System Safety Process. Update SSE Requirements Implementation Assessment. Obtain approval from the appropriate approving authority (e.g. PM, PEO, SAE, or Chief Information Officer (CIO)). If risk assessment is not approved, return to previous steps necessary to appropriately mitigate the unapproved risks.	• Updated Risk Assessment • SSE Requirements Implementation Assessment • Hazard Assessment	• IRTA Team. • SSWG • SWG • PM • CE • System Safety Group	• Appendix A: USAF SSE Acquisition Guidebook (1.10 Risk Management) • Appendix E: SSE Requirements Implementation Assessment • ISO 17666:2016, Space Systems – Risk Management, 1st ed. • AFI 91-102_AFGM2020-01 91-202 • MIL-STD-882E • AFLCMC Standard Process for Cybersecurity Assessment and Authorization (For AFLCMC Programs) • Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, Section 4, p.56157, 4 May 2020
	Approve RFP	If approved, then proceed to WBS 3.0. If not approved, adjudicate comments appropriately.			
3.0	**Contract Award**				
3.1	**Ensure Proposal Includes Requirements & Deliverables**				
3.1.1	Establish Proposal Review Team	Ensure the proposal team has SSE representation. Appoint an SSE Sub-Factor Chief under the SE Factor Chief with evaluators from the SSWG.		• Source Selection Evaluation Board Chair • SSE • SSWG	• See Acquisition Center of Excellence (ACE) for more information
3.1.2	Proposal Review	During source selection and proposal review, ensure proposal meets requirements & deliverables from WBS 2.2. If applicable, evaluate basis of estimates for appropriate costing.	• Contract • SRD	• PM • Contracts • SSWG	• See ACE for more information
Contract Award		If contract is awarded, proceed to WBS 4.0. If contract not awarded, the PM will coordinate with the MDA for next steps.			
4.0	**Program Execution, Program Reviews & Technical Reviews**				
4.1	**Update/Align Program Protection Artifacts**				
4.1.1	Update Systems Security Working Group (SSWG) to include contractor	Update and expand the SSWG membership, roles, and charter to include the contractor team. Reference WBS 1.1 **NOTE:** CyWG membership should also be expanded to include any newly identified participating cyber test agencies.	• Updated Charter • Program Protection Implementation Plan (PPIP)	• PM • SSWG • CyWG	

WBS	Activity	Description	Artifact	OPR/ Supplier	References
4.1.2	CPI Horizontal Identification & Protection	Use CPI identification subject matter experts and technologists, security classification guidance, and DoD policy (e.g., DoDI S-5230.28). Consult the Acquisition Security Database (ASDB) and the DoD CPI HPG, including the list of example CPI, to help identify the same or similar CPI associated with other programs. For more information about the ASDB, please contact your DoD Component ASDB representative or email OSD.ASDBHelpdesk@mail.mil ASDB available via SIPRNet at https://www.dodtechipedia.smil.mil/ASDB **NOTE:** Work with the USAF Anti-Tamper Service Lead early and often for guidance.	• PPP Section 4.0, ATP	• SSWG	• DoDI 5000.83 • DoDI 5200.39 • DoDD 5200.47E • DAG Chapter 8 • DoD Critical Program Information (CPI) Horizontal Protection Guidance, v2.0 • ASDB • Appendix B: USAF Combined Process Guide for CPI and CC Identification • AT Technical Implementation Guide (TIG)
4.1.3	Update Security Classification Guide (SCG) and DD254	Update SCG and DD254 (e.g., security clearance requirements, physical security requirements for safeguarding information (SCIF, SAPF, Open storage facilities, SIPRNet terminals, storage containers) and the potential for additional security features (restricted areas/gates/guns/guards)). Reference WBS 1.2.11.	• PPP Section 5.3.6 & Table 5.3.6-1 • SOW • DD Form 254	• SSWG	• DAG Chapter 9 • DoDM 5200.01, Vol. 1 • DoDI 5220.22, CH-2 • AFI 31-101 (restricted access) • AFI 63-101/20-101 • DoDI 5200.48
4.1.4	Update Programmatic Plans	Update documents in WBS 2.3, if required.	• SEP • TEMP • ISP • LCSP	• SSWG • ITT • CyWG	• DoDI 5000.02 • DoDI 5000.82 • DoDI 5000.85 • DoDI 8500.01 • AFI 99-103 • Appendix A: USAF SSE Acquisition Guidebook (1.7 Information Support Plan (ISP), 1.8 Life Cycle Sustainment Plan (LCSP), 1.11 Systems Engineering Plan (SEP), and 1.12 Test and Evaluation Master Plan (TEMP)) • DoD TEMP Guidebook
4.2	**Conduct SSE through SE**	Conduct Program Reviews/Milestone Reviews & Technical Reviews through integrated lifecycle management with access to tech data/info needed to make risk-based informed decisions. Ensure program protection activities and system design are on track.	• PPP • LCSP • SEP	• PM • CE • SSWG	• DoDI 5000.02 • DoDI 5000.83 • DoDI 5000.88 • AFI 63-101/20-101 • DAG Chapter 3 • Appendix A: USAF SSE Acquisition Guidebook (4.1 Systems Engineering Technical Reviews (SETRs) and Integrated Master Plan (IMP)) • Appendix A: USAF SSE Acquisition Guidebook (1.11 Systems Engineering Plan (SEP)) • Appendix E: SSE Requirements Implementation Assessment
4.2.1	System Requirements Review (SRR)	Conduct SRR in accordance with the entrance criteria specified in Appendix A: USAF SSE Acquisition Guidebook Section 4.0. Verify the top-level system / performance requirements are adequate to support further requirements analysis, architecture, design, and test activities. In addition, verify the requirements adequately address the Cybersecurity and Cyber Resiliency requirements. Obtain Defense Intelligence Agency – Threat Assessment Center (DIA-TAC) reports for known critical components and evaluate risk to determine proper design. Complete/update the Functional Thread Analysis per Appendix C: Functional Thread Analysis, and the Attack Path Analysis per	• SRR Meeting minutes and Action Items • SVPP • DIA-TAC reports • SSE Requirements Implementation Assessment	• PM • CE • SWG • SSWG • CyWG	• DoDI 5000.02 • DoDI 5000.88 • DoD Mission Engineering Guidebook, November 2020 • AFI 99-103 • IEEE 15288.2 • Appendix A: USAF SSE Acquisition Guidebook (4.1.2 System Requirements Review (SRR)) • Appendix E: SSE Requirements Implementation Assessment • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)

WBS	Activity	Description	Artifact	OPR/ Supplier	References
		Appendix D: Attack Path Analysis. Based on findings, add/modify requirements. **Prerequisite:** Complete Requirements Analysis in WBS 2.1. If applicable, update requirements analysis in support of SRR.			
4.2.2	Develop Architecture Design	The Architecture Design Process is a trade and synthesis method to allow the Program Manager and Systems Engineer to translate the outputs of the Stakeholder Requirements Definition and Requirements Analysis processes into alternative design solutions and establishes the architectural design of candidate solutions that may be found in a system model. The Architecture Design Process, combined with Stakeholder Requirements Definition and Requirements Analysis, provides key insights into technical risks early in the acquisition life cycle, allowing for early development of mitigation strategies. This sub-topical area contains information on the Architecture Design Process found in the DAG Chapter 3, Section 4.2.3. Architecture Design Process. Identify system security related system elements and corresponding boundaries/ interconnects/interfaces. Design the architecture's boundaries/interconnects/ interfaces to be cyber secure and resilient. Attempt to identify requirements which will remediate (i.e., design out) weaknesses/vulnerabilities identified during the SSE risk assessment process. Complete a traceability of the architecture to the requirements.	• Architecture Requirements (DoDAF Views)	• SSWG	• DAG Chapter 3, Section 4.2.3. Architecture Design Process • NIST 800-160, Vol. 2 • DoDI 5000.02
4.2.3	System Functional Review (SFR)	Conduct SFR in accordance with the entrance criteria specified in Appendix A: USAF SSE Acquisition Guidebook Section 4.0. Verify the Functional Baseline (requirements and verification methods) are established and under formal configuration control. System functions in the system performance specification are decomposed and defined in specification for lower level elements (system segments and major subsystems). Verify the requirements adequately address the Cybersecurity and Cyber Resiliency requirements. In addition, ensure verifiable test requirements are documented. Update system boundaries from WBS 1.2.4. Functional Thread Analysis completed for SCFs, MCFs, and CPI. Submit DIA-TAC reports for known critical components and evaluate risk to determine proper design.	• SFR Meeting minutes and Action Items • DIA-TAC reports • Updated Risk Assessment • Updated Functional Thread Analysis Report • SSE Requirements Implementation Assessment	• PM, • CE • SSWG	• Appendix A: USAF SSE Acquisition Guidebook (4.1.3 System Functional Review (SFR)) • Appendix E: SSE Requirements Implementation Assessment • IEEE 15288.2 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
4.2.4	Design / Requirements Decomposition	Complete a decomposition of the architecture and Cybersecurity and Cyber Resiliency requirements to ensure all MCF, SCF, and Functions associated with CPI are allocated. This decomposition is based on risk to obtain a cyber-secure and cyber resilient system.	• System / Subsystem requirements and architecture	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (Section 2.2 and Attachment 1) • NIST 800-160, Vol. 2 • DoDI 5000.02 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
4.2.5	Preliminary Design Review (PDR)	Conduct PDR in accordance with the entrance criteria specified in Appendix A: USAF SSE Acquisition Guidebook Section 4.0. Verify the Allocated baseline is established and the design provides sufficient confidence to proceed with detailed design. In addition, verify the design adequately addresses the Cybersecurity and Cyber Resiliency requirements.	• PDR Meeting minutes and Action Items • DIA-TAC reports • Functional Thread Analysis • Updated Risk Assessment • Attack Path Analysis	• PM • CE • SSWG • SWG	• Appendix A: USAF SSE Acquisition Guidebook (2.2 System Requirements Document (SRD), 4.1.4 Preliminary Design Review (PDR) • Appendix C: Functional Thread Analysis • DoDI 5000.02 • Appendix D: Attack Path Analysis • Appendix E: SSE Requirements Implementation Assessment

WBS	Activity	Description	Artifact	OPR/ Supplier	References
		Complete an attack path analysis per Appendix D: Attack Path Analysis, ensuring boundaries are evaluated. Based on findings, add/modify requirements based on their risk re-assessments, and adjust the test strategy and plans to reflect these new requirements and their design vulnerabilities. Obtain agreement on the security requirements from the AO, TSN, USAF AT Lead, and IP. **NOTE:** PDR for Space and Missile System Center (SMC) programs could have the same detail as both PDR and CDR listed in this document, due to the unique lifecycle of space systems. Submit DIA-TAC reports for known critical components and evaluate risk to determine proper design.	• SSE Requirements Implementation Assessment • SVPP		• IEEE 15288.2 • DoD Cybersecurity Test and Evaluation Guidebook (Phase-2)
4.2.6	Finalize Design / Requirements	Finalize the architecture, Cybersecurity, and Cyber Resiliency requirements allocation for all MCFs, SCFs, and functions associated with CPI. This decomposition/ allocation is based on risk to obtain a cyber-secure and resilient system.	• Final System / Subsystem requirements and architecture	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (2.2 System Requirements Document (SRD) and System Specifications, and Attachment 1 – System Level and Lower Level Requirements Excel Workbook) • NIST 800-160, Vol. 2 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2)
4.2.7	Critical Design Review (CDR)	Conduct CDR in accordance with the entrance criteria specified in Appendix A: USAF SSE Acquisition Guidebook Section 4.0. Verify the product baseline is stable and the initial product baseline is established. Verify the design embodies the requirements and adequately satisfies the Cybersecurity and Cyber Resiliency requirements. Update the attack path analysis per Appendix D: Attack Path Analysis, ensuring boundaries and identified potential vulnerabilities are evaluated. Also, ensure that the information flow through actual architecture components has been identified. Based on findings, add/modify requirements and adjust cyber test strategy/scope. Obtain agreement on the requirements from the AO, TSN, USAF AT Lead, and IP. Final Functional Thread Analysis completed for SCFs, MCFs, and CPI. Submit any remaining DIA-TAC reports and evaluate risk to determine proper design.	• CDR Meeting minutes and Action Items • DIA-TAC reports • Final Functional Thread Analysis • Updated Attack Path Analysis • Updated Risk Assessment • Updated SSE Requirements Implementation Assessment • SVPP	• PM • CE • SSWG • SWG	• Appendix A: USAF SSE Acquisition Guidebook (4.1.5 Critical Design Review (CDR)) • Appendix A: USAF SSE Acquisition Guidebook (2.2 System Requirements Document (SRD) and System Specifications, and Attachment 1 – System Level and Lower Level Requirements Excel Workbook) • Appendix C: Functional Thread Analysis. • Appendix D: Attack Path Analysis. • Appendix E: SSE Requirements Implementation Assessment • IEEE 15288.2 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 2) • DoDI 5000.02
4.2.8	Test Readiness Review (TRR)	Conduct TRR in accordance with the entrance criteria specified in Appendix A: USAF SSE Acquisition Guidebook Section 4.0. Component and system testing (i.e., Phase 3 Cyber Vulnerability Identification testing – WBS 5.2.2.1) should be initiated as early as possible (typically in a laboratory or development environment) in order to identify deficiencies and potential vulnerabilities early enough to effect system changes prior to deployment. Verify the test plans, procedures, and verification methods will adequately satisfy the test and system verification requirements. Specifically, verify the cyber test plan will test the potential cyber vulnerabilities identified during the Attack Path Analysis (or at least the high priority potential vulnerabilities). TRRs should be conducted prior to “For Score” testing for Laboratory, Ground and Flight. In	• TRR Meeting minutes and Action Items • Updated Risk Assessment • Test Plans and Procedures • Updated SSE Requirements Implementation Assessment	• PM • CE • SSWG	• USC Title 10, § 133a, 133b • DoDD 5000.01 • DoDI 5000.02 • DoDI 5000.89 • AFI 99-103 • AFPD 17-1 • IEEE 15288.2 • Appendix A: USAF SSE Acquisition Guidebook (4.1.6 Test Readiness Review (TRR)) • Appendix C: Functional Thread Analysis. • Appendix D: Attack Path Analysis. • Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, Section 4, p.56157, 4 May 2020.

WBS	Activity	Description	Artifact	OPR/ Supplier	References
		addition, verify the configuration and any delta configurations as going through the testing phase. Finally, verify all test plans and procedures are completed prior to any test execution (Laboratory, Ground, and Flight) to ensure appropriate and sufficient testing is planned. **NOTE:** Obtain an Interim Authorization to Test (IATT) prior to testing.			
4.2.9	Functional Configuration Audit/System Verification Review (FCA/SVR)	Conduct FCA/SVR in accordance with the entrance criteria specified in Appendix A: USAF SSE Acquisition Guidebook Section 4.0. Verify the system design is verified to conform to the requirements through analysis, demonstration, inspection, and test. In addition, verify the configuration of all verification methods has been reviewed and understood. Review Developmental Test & Evaluation (DT&E) reports. Obtain agreement on the requirements from the AO, TSN, USAF AT Lead, and IP. Submit DIA-TAC reports for any updated critical components and evaluate risk to determine proper design.	• FCA/SVR Meeting minutes and Action Items • DIA-TAC reports • Updated Risk Assessment • Updated SSE Requirements Implementation Assessment • AT Plan	• PM • CE • SSWG	• Appendix A: USAF SSE Acquisition Guidebook (2.2 System Requirements Document (SRD) and System Specifications, 4.1.7 Functional Configuration Audit (FCA), 4.1.8 System Verification Review (SVR) • IEEE 15288.2 • Appendix E: SSE Requirements Implementation Assessment
4.2.10	Production Readiness Review (PRR)	Conduct PRR in accordance with the entrance criteria specified in Appendix A: USAF SSE Acquisition Guidebook Section 4.0. Verify the manufacturing and SCRM processes can support production. Verify that the Design for Manufacturing, concerning not only data and drawings, but also their Manufacturing Bill of Materials (BOM) have not introduced AT and SCRM risks, issues or concerns; and that could affect the System-Under Design's MCFs and SCFs. Obtain agreement on the requirements from the AO, TSN, USAF AT Lead, and IP. Update the Functional Thread Analysis and the Attack Path Analysis as necessary.	• PRR Meeting minutes and Action Items • Updated Risk Assessment • SVPP • Updated SSE Requirements Implementation Assessment • AT Plan • Parts, Materials and Processes Selection List (PMPSL) • As-Designed Parts, Materials and Processes List (ADPMPL) • As-Built Parts, Materials and Processes List (ABPMPL)	• PM • CE • SSWG • SWG • USAF Space Parts Working Group (SPWG)	• DoDI 5000.88 • IEEE 15288.2 • Appendix A: USAF SSE Acquisition Guidebook (4.1.9 Physical Configuration Audit (PRR)) • Appendix E: SSE Requirements Implementation Assessment
4.2.11	Physical Configuration Audit (PCA)	Conduct PCA in accordance with the entrance criteria specified in Appendix A: USAF SSE Acquisition Guidebook Section 4.0. Verify the product baseline is established as verified in the FCA/SVR. Verify the design and manufacturing documentation matches to the physical configuration. Obtain agreement on the requirements from the AO, TSN, USAF AT Lead, and IP.	• PCA Meeting minutes and Action Items • SVPP • Updated Risk Assessment • Updated SSE Requirements Implementation Assessment • AT Plan	• PM • CE • SSWG • SWG	• IEEE 15288.2 • Appendix A: USAF SSE Acquisition Guidebook (4.1.10 Physical Configuration Audit (PCA)) • Appendix E: SSE Requirements Implementation Assessment
4.3	**Update Program Protection Analysis and Programmatic Plans**	Reassess and update program protection analysis. This process is iterative and must be revisited again and throughout the life cycle of the program, to include: prior to each acquisition milestone; prior to each system's engineering technical review; throughout operations and sustainment; and specifically during software/hardware technology updates.	• PPP, Section 2.2, Table 2.2-1, Section 3.0, Section 4.0 and Appendix C (Criticality Analysis)	• SSWG	• DoDI 5000.02 • DoDI 5000.83 • DoDI 5000.88 • DoDI 5000.39 • DoDI 5000.44 • DoDI 8510.01 • DoDI 8500.01 • AFMAN 14-401

WBS	Activity	Description	Artifact	OPR/ Supplier	References
					• DoD Trusted Systems and Networks (TSN) Analysis • Appendix B: USAF Combined Process Guide for CPI and CC Identification
4.3.1	Develop/Update Plan of Action and Milestones (POA&M)	Develop/Update POA&M as required. Develop design remediations to reduce the probability or consequence of vulnerability exploitation. If unable to design out the vulnerability, develop and select mitigation options to limit the impact of vulnerability exploitation.	• POA&M • Security Plan	• PM/SCA	• NIST SP800-37
4.3.2	Update PPP and Applicable Appendices	Conduct appropriate information analysis in order to identify, understand, and protect the information about the program that will require classification, handling, and marking considerations. **NOTE:** It is recommended to update the Program Protection Plan for each SETR, and as often, as required after the updated analyses have been conducted to support submission at milestone decisions.	• PPP Appendices A (SCG), C (Criticality Analysis), D (Anti-Tamper Plan), E (Cybersecurity Strategy)	• SSWG	• DoDI 5200.48 • DoDM 5200.01, Vol. 1 • Cybersecurity Security Classification/Declassification Guide for Air Force Weapon Systems • Appendix A: USAF SSE Acquisition Guidebook (2.3 SOO and SOW, Attachment 2 CDRL 54) • Appendix C: Functional Thread Analysis. • Appendix D: Attack Path Analysis. • (For AFLCMC Programs) AFLCMC Standard Process for Cybersecurity Assessment and Authorization
4.3.3	Monitor Protection Activities	Monitor CPI and CC throughout the life cycle of the program. Monitoring includes determining if an event has occurred that requires the program to reassess CPI or its associated protections. Events may include, but are not limited to, the following: • *Operational Environment*: A change in the physical location of the system with CPI other than that for which it was originally designed. • *Protection Effectiveness:* A change in the ability of the CPI protections to deter, delay, detect, and respond to attempts to compromise CPI (e.g., presumed effectiveness of system requirements invalidated through cyber test). • *Security Classification*: A change to a relevant SCG, and thus the classification thresholds. • *System Modification*: A change to the system architecture and/or designs. • *Capability Maturation*: A change in the state-of-the-art for a particular capability and thus the thresholds used for CPI identification. • *Cyber Test Strategy*: A change in the cyber test and evaluation strategy.	• SEP • TEMP • LCSP • PPP, Section 2.2, Table 2.2-1, Section 3.0, and Section 4.0	• SSWG • PM • CE • CyWG	• DoDI 5200.39, CH-3 • AFPAM 63-113 • DAG Chapter 9 • Appendix A: USAF SSE Acquisition Guidebook (1.8 Life Cycle Sustainment Plan (LCSP), 1.11 Systems Engineering Plan (SEP), and 1.12 Test and Evaluation Master Plan (TEMP)) • Appendix B: USAF Combined Process Guide for CPI and CC Identification • Appendix C: Functional Thread Analysis • Appendix D: Attack Path Analysis • DoD Program Protection Plan Outline & Guidance
4.3.4	Update Programmatic Plans	Update SEP, TEMP, and LCSP as needed.	• SEP • TEMP • LCSP	• SSWG • PM • CE • CyWG	• DoDI 5200.39, CH-3 • AFPAM 63-113 • DAG Chapter 9 • Appendix A: USAF SSE Acquisition Guidebook (1.8 Life Cycle Sustainment Plan (LCSP), 1.11 Systems Engineering Plan (SEP), and 1.12 Test and Evaluation Master Plan (TEMP))
4.4	**Risk Assessment**	Update SSE risks in the Program's Risk Management Process and System Safety Process. In addition, incorporate risks from test reports.	• Updated Risk Assessment • SSE Requirements	• SSWG • PM • CE	• Appendix A: USAF SSE Acquisition Guidebook (1.10 Risk Management) • Appendix E: SSE Requirements Implementation Assessment

WBS	Activity	Description	Artifact	OPR/ Supplier	References
		Update SSE Requirements Implementation Assessment. Obtain approval from the appropriate approving authority (e.g. PM, PEO, SAE, or Chief Information Officer (CIO)) If risk assessment is not approved, return to previous steps necessary to appropriately mitigate the unapproved risks.	• Implementation Assessment • Hazard Assessment • MBCRA Report • SWG	• System Safety Group	• ISO 17666:2016, Space Systems – Risk Management, 1st ed. • AFI91-202_AFGM2021-01 • MIL-STD-882 • AFLCMC Standard Process for Cybersecurity Assessment and Authorization (For AFLCMC Programs) • Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, Section 4, p.56157, 4 May 2020
4.5	**Review/Approve PPP**	The PPP will be submitted for MDA approval at each milestone review, beginning with Milestone A. **NOTE:** Program Management, to include program planning and execution, is vested in the Program Management chain of command	• PPP	• SSWG • PM • MDA • PEO	• DoDI 5000.02 • DoDI 5000.83 • AFI 63-101/20-101 • AFPAM 63-113 • DAG Chapter 9 • OSD PPP Outline and Guidance, PPP example, and OSD Evaluation Criteria
	Milestone Decision/ Decision Point	The Acquisition Strategy will define the criteria for the Milestone Decisions and Decision Points (e.g., PDR, CDR, TRR). The "Milestone Decision / Decision Point" after WBS 4.5 leads to the next program phase, as well as, verification/validation. At this point, the program should reevaluate the acquisition strategy, ensure appropriate expertise is included in the Systems Security Working Group, and continue progressing through the process again.	• Milestone Decision/ Decision Point • Updated ASP	• MDA	• DoDI 5000.02 • DoDI 5000.85 • Appendix A: USAF SSE Acquisition Guidebook (1.2 Acquisition Strategy)
5.0	**Verification / Validation**				
5.1	**Interim Authorization to Test (IATT) / Authorization to Operate (ATO)**	Assemble and submit the Security Authorization Package to receive ATO or IATT	• IATT • ATO	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (2.3 SOO and SOW, and Attachment 2 – Contract Data Requirements Lists (CDRLs) Associated with SSE) • AFI 17-101 • (For AFLCMC Programs) AFLCMC Standard Process for Cybersecurity Assessment and Authorization • DoDI 8510.01
5.1.1	Submit Authorization Package	Assemble the Security Authorization Package for Cybersecurity, review it with the Security Controls Assessor (SCA), and submit package for approval.	• Security Authorization Package	• SSE • SSWG • PM	• AFI 17-101 • (For AFLCMC Programs) AFLCMC Standard Process for Cybersecurity Assessment and Authorization • DoDI 8510.01
5.1.2	Risk Acceptance (Authorization)	The AO weighs the operational need against the overall risk of operation of the system and determines if the risk is acceptable. **NOTE:** The AO may issue conditions along with the authorization decision. These authorization conditions must be met for the authorization to remain valid. **NOTE:** The AO may also determine immediate remediation is required prior to issuing an authorization decision.	• Signed Authorization (IATT/ATO)	• AO	• NIST SP800-37 • AFI 17-101 • (For AFLCMC Programs) AFLCMC Standard Process for Cybersecurity Assessment and Authorization • DoDI 8510.01
5.2	**Developmental Test and Evaluation (DT&E) /Operational Test and Evaluation (OT&E)**				
5.2.1	Review Cyber Test Planning Artifacts	Ensure MBCRA reflects most recent system updates and test results. Review the test planning artifacts from CDR, TRR, and FCA. (WBS 4.2.7, WBS 4.2.8, and WBS 4.2.9). Update test	• Updated test plans, TEMP	• SSWG • CyWG	• USC Title 10, § 133a, 133b • Appendix C: Functional Thread Analysis

WBS	Activity	Description	Artifact	OPR/ Supplier	References
		plans, as necessary. Ensure test plan(s) match the test strategy outlined in the CS and TEMP. Review the FTA and APA for any required changes and their resultant risks as associated with the MBCRA results.			• Appendix D: Attack Path Analysis. • DoDD 5000.01 • DoDI 5000.89 • AFI 99-103 • AFPD 17-1 • DoD Cybersecurity Test and Evaluation Guidebook
5.2.2	Conduct Cyber DT&E	Conduct DT&E to verify SSE requirements and to provide knowledge to measure progress, identify problems, to characterize system capabilities and limitations, and manage technical and programmatic risks. DT&E results are used as exit criteria to ensure adequate progress prior to investment commitments or initiation of phases of the program.	• Updated Risk Assessment • Cooperative Vulnerability Identification (CVI) test report(s) • Updated cyber test portions of CS and TEMP • Vulnerability Reports • ACD test report(s) • DT&E artifacts	• SSWG • CyWG • cyber test agency	• DoDI 5000.02 • USC Title 10, § 133a, 133b • DoDD 5000.01 • AFI 99-103 • AFPD 17-1 • DoD Cybersecurity Test and Evaluation Guidebook (Phases 3 and 4)
5.2.2.1	Cooperative Vulnerability Identification (CVI)	Conduct CVI activities (Phase 3 cyber T&E activities) in a lab / developmental test environment. This testing and analysis is performed to identify cyber vulnerabilities early in the development / test process to effect system design (to include supporting and providing feedback to the Critical Design Review (CDR) if not already conducted), to inform follow-on Adversarial Cybersecurity Developmental Test and Evaluation (ACD), Cooperative Vulnerability and Penetration Assessment (CVPA), and Adversarial Assessment (AA) cyber test activities, and to help inform the Operational Test Readiness Review (OTRR). Test and verify system controls, Cybersecurity functionality, Cybersecurity posture, and validate earlier cyber vulnerabilities analysis through penetration testing. The CVI process includes detailed test planning and execution of vulnerability, controls, system misuse/abuse, and penetration testing based upon MBCRA and CVI activities conducted to date. Update requirements as necessary. **NOTE:** CVI testing typically consists of multiple incremental test events (beginning with individual sub-components / components and increasing to end-to-end system testing) spanning the developmental test period and occasionally into operational test if system modifications occur during operational test. Whenever possible, CVI activities should begin during system development and may include integrated contractor/Government cyber test activities.	• Updated Risk Assessment • CVI test report(s) • Updated cyber test portions of CS and TEMP	• SSWG • CyWG • cyber test agency • SWG	• USC Title 10, § 133a, 133b • AFI 99-103 • AFPD 17-1 • ISO 17666:2016, Space Systems - Risk Management, 1st ed... • DoDD 5000.01 • DoDI 5000.90 • DoDI 5000.02 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 3). • DoD PM Guidebook for Integrating the Cybersecurity Risk Management Framework into System Acq Lifecycle • Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, Section 4, p.56157, 4 May 2020
5.2.2.2	Adversarial Cybersecurity Developmental Test and Evaluation (ACD)	Conduct Adversarial Cybersecurity DT&E upon completion of the CVI activities and vulnerability remediation/mitigation implementation (ideally on the completed system). The ACD includes an evaluation of the system's Cybersecurity using realistic tactics, techniques, and procedures while in a representative operating environment. Evaluate the system's Cyber Resiliency (i.e., capability to perform its mission while subjected to and following a cyber-attack) through	• Vulnerability Report • ACD test report(s) • DT&E artifacts • Updated cyber test portions of CS and TEMP	• SSWG • CyWG • cyber test agency	• USC Title 10, § 133a, 133b • DoDD 5000.01 • DoDI 5000.90 • AFI 99-103 • AFPD 17-1 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 4)

WBS	Activity	Description	Artifact	OPR/ Supplier	References
		penetration testing with the intent of causing mission effects.			
5.2.3	Conduct Cyber OT&E	Determine the operational effectiveness, operational suitability, and survivability or lethality of a system when operated under realistic operational conditions, including Joint combat operations and system-of-systems concept of employment. Evaluate whether threshold requirements in the approved requirements documents and critical operational issues have been satisfied. Assess impacts to combat operations and provide additional information on the system's operational capabilities, limitations, and deficiencies.	• Test and Evaluation Reports • CVPA test report(s) • Updated Risk Assessment • Updated cyber test portions of CS and TEMP (if required) • Survivability and Vulnerability Program Plan (SVPP)	• SSWG • CyWG • cyber test agency • Survivability Working Group (SWG)	• DAG Chap 8, 3.2 Operational T&E • USC Title 10, § 133a, 133b • ISO 17666:2016, Space Systems – Risk Management, 1st ed. • DoDD 5000.01 • DoDI 5000.89 • AFI 99-103 • AFPD 17-1 • DoD Cybersecurity Test and Evaluation Guidebook (Phases 5 and 6) • SMC-S-014 (2010), AFSC Standard: Survivability Program Management for Space, 19 July 2010
5.2.3.1	Cooperative Vulnerability and Penetration Assessment (CVPA)	The purpose of the CVPA is to provide a comprehensive characterization of the Cybersecurity status of a system in a fully operational context and to substitute for reconnaissance activities in support of adversarial testing when necessary. This is an OT&E event performed by a Cyber Blue Team, which is completed either before or following MS C (as appropriate) and after the SUT has received an authority to operate or an interim authority to test in an operationally representative network(s). This testing may be integrated with DT&E activities if conducted AMCI99-101 18 JUNE 2018 11 in a realistic operational environment and in a realistic operational environment and approved in advance by the OSD Director, Operational Test and Evaluation (DOT&E). Cooperative Vulnerability and Penetration Assessment (CVPA). **NOTE:** The CVPA should be conducted after previously identified vulnerabilities are remediated or mitigated.	• Test and Evaluation Reports • CVPA test report(s) • Updated Risk Assessment • Updated cyber test portions of CS and TEMP (if required)	• SSWG • CyWG • cyber test agency • SWG	• USC Title 10, § 133a, 133b • DoDD 5000.01 • DoDI 5000.89 • DoDI 5000.90 • AFI 99-103 • AFPD 17-1 • AMCI 99-101 • ISO 17666:2016, Space Systems – Risk Management, 1st ed. • DoD Cybersecurity Test and Evaluation Guidebook (Phase 5) • DoD PM Guidebook for Integrating the Cybersecurity Risk. Management Framework into System Acq. Lifecycle • DOT&E Memo: Procedures for Operational Test & Evaluation of Cybersecurity in Acquisition Programs
5.2.3.2	Adversarial Assessment (AA)	Conduct an Adversarial Assessment following the completion of the CVPA and subsequent remediation activities. The AA assesses the capability of a unit equipped with a system to support its missions while subjected to validated and representative cyber threat activity (i.e., Cybersecurity and Cyber Resiliency testing of a system in an operationally representative environment). The OTA shall evaluate the system's capability to: • Prevent cyber intrusions from negatively impacting mission effectiveness/mission functions • Mitigate the effects of cyber-attacks, enabling the system to complete critical mission tasks • Recover from cyber-attacks and restore mission capability degraded or lost due to threat activity	• Test and Evaluation Reports • AA test report(s) • Updated Risk Assessment • Updated cyber test portions of CS and TEMP (if required)	• SSWG • CyWG • cyber test agency • SWG	• USC Title 10, § 133a, 133bDoDD 5000.01 • DoDI 5000.90 • AFI 99-103 • AFPD 17-1 • DoD Cybersecurity Test and Evaluation Guidebook (Phase 6) • DoD PM Guidebook for Integrating the Cybersecurity Risk Management Framework into System Acq Lifecycle • DOT&E Memo: Procedures for Operational Test & Evaluation of Cybersecurity in Acquisition Programs • ISO 17666:2016, Space Systems – Risk Management, 1st ed.
5.3	**Generate Test Report(s)**	Capture the results of cyber DT&E and OT&E in required test report artifacts in accordance with supporting test plans. Test results will demonstrate execution of test plans, which verified and validated requirements. Upon completion of each cyber test and evaluation phase (i.e., CVI, ACD, CVPA, and AA), generate a cyber-vulnerability report.	• DT&E and OT&E reports • Updated cyber test portions of the CS and TEMP (if required)	• SSWG • CyWG	• USC Title 10, § 133a, 133b • DoDD 5000.01 • DoDI 5000.89 • AFI 99-103, Section 5.19, 5.20 • AFPD 17-1 • Appendix C: FTA. • DoD Cybersecurity Test and Evaluation Guidebook

WBS	Activity	Description	Artifact	OPR/ Supplier	References
		Review the FTA for any required changes and their resultant risks as associated with the Test Reports results. Any identified test failures/vulnerabilities during DT&E and OT&E should be resolved by reverting to WBS 4.2 and WBS 4.4, respectively. The CyWG shares the report and all supporting documentation with SE, the Program Office, CDT, Cybersecurity testers, and stakeholder. Capture any vulnerabilities or deficiencies in Joint Deficiency Reporting System (JDRS). Deficiencies should be linked to requirements. **NOTE:** Apply Security Classification Guide to deficiency reporting.			
6.0	**Operation & Support**				
6.1	**Authorization To Operate (ATO)**	See WBS 5.1. Submit final ATO package to AO for approval, if necessary.	• ATO	• SSWG	• AFI 17-101 • DoDI 8510.01 • (For AFLCMC Programs) AFLCMC Standard Process for Cybersecurity Assessment and Authorization
6.2	**System Sustainment**	Maintain the same system security posture during the operation & sustainment phase as during the design phase. Ensure the correct DFARS clauses, security requirements, etc., are on the sustainment contract. Ensure that the Users deliver and follow an operational security plan. For any major modifications, return to the start of the WBS. For minor modifications, ensure monitoring is maintained and considered (need to follow the technical orders and have a Security Plan).	• LCSP • PPP	• Product Support Manager	• Appendix A: USAF SSE Acquisition Guidebook (3.1.2 Recommended List of DFARS Clauses)
6.3	**Monitoring**	Determine the security impact of proposed or actual changes to the system, environment, threats, and vulnerabilities.	• Plan of Actions & Milestones (POA&M) • PPP Section 9.1 & Appendix E (Cybersecurity Strategy)	• PM	• NIST SP800-37 • AFPAM 63-113 • NIST SP800-137 • Cybersecurity Principles for Space Systems", Federal Register, Vol. 85, No. 176, Title 3, Space Policy Directive 5, Section 4, p.56157, 4 May 2020
6.3.1	Ongoing Security Assessments	Assess a selected subset of the technical, management, and operational security controls employed within and inherited by the system in accordance with the organization-defined monitoring strategy, or at minimum annually.	• POA&M	• SCA	• DoDI 8510.01 • NIST SP800-37
6.3.2	Ongoing Remediation Actions	Conduct remediation actions based on the results of ongoing monitoring activities, assessment of risk.	• POA&M	• ISSO/ Common Control Provider	• NIST SP800-37
6.3.3	Security Status Reporting	Report changes to the risk posture of the system to the Authorizing Official in accordance with the monitoring strategy.	• PPP Section 9.0	• ISSO/ Common Control Provider	• AFI 17-101 • NIST SP800-37
6.3.4	System Removal & Decommissioning	Implement a system decommissioning strategy, when needed, which executes required actions when a system is removed from service.	• LCSP • PPP	• ISSO/ Common Control Provider	• NIST SP800-37 • Appendix A: USAF SSE Acquisition Guidebook (1.8 Life Cycle Sustainment Plan (LCSP))
6.3.5	Program Protection Surveys	Conduct surveys on the contractor and sub-contractor facilities at least once during each integrated life cycle phase and at contract renewal.	• SOW • Performance Work Statement (PWS) • PPP Section 9.0	• SSWG	• Appendix A: USAF SSE Acquisition Guidebook (2.1 Performance Work Statement (PWS), 2.3 Statement of Objectives (SOO) and Statement of Work (SOW)
6.3.6	Schedule & Conduct CPI/CC Reviews	Reassess CPI and CCs throughout the life cycle of the program at least every two years throughout operations and sustainment and specifically during software/hardware technology updates.	• PPP, Section 3.0	• PM/SSWG	• DoDI 5000.39 • DoDI 5000.44 • AFI 63-101/20-101 • AFPAM 63-113

WBS	Activity	Description	Artifact	OPR/ Supplier	References
					• Appendix B: USAF Combined Process Guide for CPI and CC Identification
6.3.7	Update the PPP as Required	Review and update the PPP at minimum every five years or as threat changes.	• PPP	• SSWG	• AFI 63-101/20-101
6.3.8	Deficiency Reporting	Review Deficiency Reports (DRs) and complete root cause analysis reporting as necessary. Cyber incident response begins with the submittal of an OPREP-3B, Rule 6C report or a CCIR and includes those actions taken to respond, coordinate, analyze, and report any event or cyber Incident for the purpose of mitigating any adverse operational or technical impact. For further instructions, reference CROWS CICC IRT CONOPS, Section 7. Cyber Incident Response Process Flow. **NOTE:** Upon an incident and/or deficiency, update risk assessment.	• DR • Updated risk assessment	• SSWG • SWG	• Appendix A: USAF SSE Acquisition Guidebook (2.3.2 Program Protection) • Air Force Cyber Resiliency Office for Weapon Systems (CROWS) Cyber Incident Coordination Cell (CICC) and Cyber Incident Response Team (IRT) for Weapon Systems Concept of Operations • ISO 17666:2016, Space Systems – Risk Management, 1st ed.
6.3.9	Continuous Monitoring	Continuously monitor Cybersecurity and Cyber Resiliency activities annually, or as needed. Continuous monitoring includes the effectiveness of SSE requirements and changes to the environment for both Government and contractors.	• USAF Contractor Security Plan	• SSWG	• CDRL 19 (Appendix A: USAF SSE Acquisition Guidebook Attachment 2, and Appendix A Section 2.3.3 Cybersecurity and Trusted Systems and Networks)
6.4	**Update Risk Assessment**	Update SSE risks in the Program's Risk Management Process and System Safety Process. Obtain approval from the appropriate approving authority (e.g. PM, PEO, Service Acquisition Executive (SAE), or Chief Information Officer (CIO)). If risk assessment is not approved, return to previous steps necessary to appropriately mitigate the unapproved risks. **NOTE:** If current risks are elevated or new medium/high-risks are identified, then approval of those risks should be obtained.	• Updated risk assessment • Hazard Assessment	• SSWG • PM • CE • System Safety Group • SWG	• Appendix A: USAF SSE Acquisition Guidebook (1.10 Risk Management) • AFI 17-101 • AFI 91-202 • MIL-STD-882 • (For AFLCMC Programs) AFLCMC Standard Process for Cybersecurity Assessment and Authorization • ISO 17666:2016, Space Systems – Risk Management, 1st ed. Back to Workflow Process Chart
End					