INTEGRATED DEFENSIVE CYBERSPACE SYSTEM (IDCS) SECURE PLATFORM ARCHITECTURE FOR REAL-TIME THREAT ANALYSIS AND NETWORK DEFENSE (SPARTAN) STATEMENT OF OBJECTIVES (SOO)

SOO Title: IDCS Secure Platform Architecture for Real-Time Threat Analysis and Network Defense (SPARTAN)

Date: 28 August 2025

Agency/Organization: United States Air Force/Air Force Life Cycle Management Center (AFLCMC)/Defensive Cyber (HNCD)

Contracting Activity: AFLCMC/Defensive Cyber Branch (HNCKC)

Table of Contents

1. BACKGROUND

In an era defined by increasingly sophisticated and persistent cyber threats, the Department of the Air Force (DAF) recognizes the critical need for a modernized and unified cyber defense capability. Current cyber defense operations are hampered by siloed weapon systems, limited synchronization, and slow response times, hindering the DAF's ability to effectively defend against these evolving threats, particularly in the Pacific region. To address these critical capability gaps and align with the evolving demands of modern warfare, the DAF is implementing the Integrated Defensive Cyberspace System (IDCS), a fully funded program of record designed to revolutionize its approach to cyber defense and situational awareness. At the heart of IDCS lies the Big Data Platform (BDP), providing strategic Defensive Cyber Operations (DCO) analytics and data storage within a centralized cloud environment. Complementing the BDP is a caching Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) system for operational DCO analytics, alerting, and incident response, with global access for mission partners. The IDCS architecture further leverages a Sensor Platform, available in both fixed and mobile configurations for tactical detection, analysis, response, and transport. This platform, partly realized through enterprise hardware and mobile acquisition efforts, supports Denied, Degraded, Intermittent, and Limited (DDIL) environments, enabling cyber protection even with partial communications, and is centrally managed through a Cloud environment. By integrating these components, IDCS aims to deliver a common data architecture, enabling seamless coordination, rapid decision-making, and decisive action against adversaries across Air Force networks and critical infrastructure.

2. SCOPE

The Air Force's IDCS program is a strategic, enterprise-wide initiative to modernize and unify its DCO capabilities. IDCS will provide enterprise-scale situational awareness and cyber defense across business, mission, and industrial control systems, protecting the DAF and Department of Defense (DoD) network enclaves, systems, and sensitive operational information from cyber threats. The SPARTAN Multi-Award Contract (MAC) Indefinite-Quantity Indefinite-Delivery (IDIQ) will guide the acquisition, development, deployment, sustainment, and enhancement of IDCS capabilities. As a System of Systems (SoS), a collection of independent systems that integrate to achieve a capability that none of the constituent systems could accomplish individually, the IDCS requires coordinated integration across multiple platforms, leveraging existing systems and incorporating new solutions with open standards and a hybrid cloud architecture. The program will integrate and absorb the functions of existing Air Force cyber weapon systems that perform defensive cyberspace operations, enhancing HNCD capabilities. Interoperability Platforms (IOPs) will be sustained until their tasks are fully absorbed by IDCS. IDCS employs agile software development, using modern tools and techniques, to support the DAF. This Statement of Objectives (SOO) defines the requirements for providing comprehensive services to support the IDCS SPARTAN. These services will support the design, development, deployment, integration, testing, sustainment, and continuous enhancement of IDCS capabilities that will be utilized to execute the DCO missions. The Government will serve as the system integrator and product owner, directing, prioritizing, and modifying the system based on evolving mission requirements.

3. STRATEGIC OBJECTIVES

The objective of this SOO is to acquire contractor services that enable the IDCS program to deliver enhanced situational awareness, proactive threat detection, accelerated incident response, and effective cyber defense across the DAF enterprise. Contractor performance shall align with strategic objectives and performance requirements (identified in Section 4) ensuring interoperability, scalability, and security across the IDCS SoS, and contributing to unified war-fighting capabilities for cyberspace operations forces. Below are the strategic objectives of the IDCS (NOTE: the Government reserves the right to modify, add or remove strategic objectives throughout the duration of this contract to account for possible technological advances made):

3.1. To sustain major components: the current common sensor platform and a situational awareness platform, the DAF BDP.

3.2. To enable DAF DCO to host, integrate, and feed defensive cyber-related data, informing both operational and strategic analysis and contributing to enhanced situational awareness for senior leaders.

3.3. To serve as an important cyber defense modernization effort supporting the Department's initiatives regarding the DAF strategic DCO operational objectives, leveraging streamlined processes, balancing operational and acquisition risks. To provide an integrated set of cyberspace capabilities that will enable the DAF to rapidly identify vulnerabilities, understand their impact, and expeditiously mitigate them utilizing a synchronized suite of cyberspace capabilities.

3.4. To unify the mission systems of network defense and cyber protection teams currently supported by cyber weapon systems, allowing them to conduct cyber missions from the same system with shared, mission-relevant data.

3.5. To provide situational awareness and cyber defense across mission and industrial control systems.

3.6. To integrate Commercial-Off-The-Shelf (COTS), Government-Off-The-Shelf (GOTS), and open-source software capabilities to achieve an effective and efficient mission capability.

3.7. To employ an agile development process and a Continuous Integration/Continuous Delivery (CI/CD) pipeline to deliver incremental capabilities at the speed required to counter emerging and persistent cyber threats.

3.8. Modernize the cyber weapon systems by consolidating existing DCO weapon systems with enhanced capabilities, thereby strengthening DAF cyber defense posture.

3.9. To identify vulnerabilities and provide commanders with a comprehensive risk assessment of existing vulnerabilities on critical mission networks.

3.10. To focus its mission on the capability to find, fix, track, target, engage, and assess the advanced persistent threat.

4. PERFORMANCE REQUIREMENTS

This section outlines key capability areas derived from the Information Systems Initial Capabilities Document (IS-ICD), which will guide the development and implementation of the IDCS SoS. The objectives in Section 3, grouped within Capability Areas (CAs) as detailed in Appendix A, define the operational goals of IDCS. As technology evolves, the Government reserves the right to add, modify, or remove objectives based on operational needs. Future Task Orders (TOs) will focus on objectives within one or more CAs based on government priorities and requirements.

4.1. ***Collaboration:*** Vendors shall collaborate with other government-identified vendors, stakeholders, and other support contractors as part of an integrated team. The Government will define the scope of collaboration required to achieve IDCS objectives. Vendors unwilling to collaborate will not receive an award.

4.2. ***Work Decomposition and Traceability:*** The Contractor shall use an Agile framework (e.g., Scrum, Kanban) to manage the execution of tasks within the Government's environment and documents in Jira or similar government provided agile management suite.

4.3. ***Operating Constraints:*** Offerors shall adhere to specific constraints related to open standards and interoperability. Examples of additional constraints are identified below.

4.3.1. Open Standards & Interoperability: Mandatory use of defined open standards, demonstrated interoperability with legacy, existing, and planned DAF and DoD systems (via government testing), and adherence to specified data formats and schemas. Proprietary formats are prohibited.

4.3.2. Interface & Architecture: Strict compliance with government-provided Information Systems Initial Capabilities Document (IS- ICD)/ Requirements Definition Packages (RDP) (deviations require approval), limited and justified use of proprietary technologies, and contribution to a modular, open architecture supporting component substitution. Solutions must be containerized using industry's best practices and supporting automated builds and deployments for CI/CD pipeline implementation.

4.3.3. General Compliance: Adherence to DAF and DoD policies (Appendix C. References), budgetary limitations, program schedule, FAR, and DFARS regulations.

4.4. ***Technical Expertise:*** The Contractor shall propose qualified personnel (FTEs, labor categories, skillsets) meeting objectives. Anticipated expertise includes cloud engineering, software development, cybersecurity, data science, systems integration, enterprise architecture, test and evaluation, service management, and program management.

4.5. ***Capabilities:*** The Government will work directly with vendors to ensure solution compatibility and integration with the IDCS SoS. TOs will include Performance Standards, Acceptance Criteria, and Surveillance Methods for assessing execution (for example, see Section 4.5.1 CA 1 below). Appendix A is the *IDCS Capability Areas & Objectives Matrix*, which details all Capability Areas (CAs), each linked to specific

Capability Requirements (CRs) aligned with the IS-ICD. The government will provide CRs through the RDPs via a defined process at a later date. Future awards will focus on tasks related to these CAs, ensuring effective development and implementation of the IDCS SoS to meet mission needs.

4.5.1. CA 1: Cloud Services and Infrastructure Management

4.5.1.1. ***General:*** This capability encompasses the design, implementation, security, management, and sustainment of all underlying cloud and on-premises infrastructure necessary to support IDCS. This includes computing, storage, networking, and the physical platforms for garrison, deployable, mobile, and sensor systems.

4.5.1.2. ***Task Description:*** Contractor shall design, build, and maintain a secure, resilient, and scalable hybrid cloud infrastructure by government authorized environments. Manage and sustain on-premises hardware. Implement and manage robust network infrastructure.

4.5.1.3. ***Performance Standards:*** Infrastructure provisioning shall be deployed in accordance with the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) requirements, government-established local policies, and organizational procedures. Patching will be accomplished based on vulnerability severity ratings, guidance from Cyber TOs (or equivalent directive documentation), and assessed impact to the user community. The Contractor shall maintain infrastructure level uptime of 99.9%.

4.5.1.4. ***Acceptance Criteria: Availability*** will be measured using system monitoring tools and reported monthly. Patching times will be tracked by using a ticketing system and reported monthly. Compliance with DISA STIGs will be verified through security scans and audits.

4.5.1.5. ***Surveillance Method:*** The Government will monitor infrastructure performance through system monitoring tools, review monthly reports, and conduct periodic security audits.

4.5.2. CA 2: Agile Software Engineering and DevSecOps

4.5.2.1. ***General:*** This capability focuses on the full lifecycle of software development, from requirements analysis and design through development, testing, deployment, and sustainment, utilizing agile methodologies and DevSecOps principles.

4.5.2.2. ***Task Description:*** Contractor shall design, develop, and maintain high-quality, secure, and modular software applications and services for the IDCS SoS. Implement and manage a robust DevSecOps framework, integrating security best practices and automated security testing throughout the development lifecycle. This includes leveraging Hardware-in-the-Loop (HIL) simulation environments to rigorously test and validate software components interacting with physical hardware elements of the IDCS SoS. HIL testing will

ensure real-time performance, security, and reliability under realistic operating conditions before deployment. Develop and maintain containerized applications. This includes utilizing tools and services within the container ecosystem for deployment, monitoring, and automated scaling, ensuring optimal resource utilization and system performance.

4.5.2.3. ***Performance Standards:*** The quality levels of DevSecOps can be assessed through various metrics that track the effectiveness of security practices throughout the software development lifecycle. The minimum standards required to meet will be identified within their associated TOs. Here are some key metrics that will be considered:

4.5.2.3.1. ***Number of Security Vulnerabilities:*** This metric tracks the volume of security vulnerabilities identified in a system or software project over time, indicating the effectiveness of vulnerability management initiatives.

4.5.2.3.2. ***Compliance with Security Policies:*** This metric verifies consistent adherence to established security requirements and best practices, promoting a unified approach to software development.

4.5.2.3.3. ***Mean Time to Detect (MTTD):*** These metrics measure the average time taken to detect security incidents or vulnerabilities, highlighting the efficiency of security monitoring and incident response processes.

4.5.2.3.4. ***Code Quality Metrics:*** These metrics assess the overall quality of the code being developed, including coding standards compliance, code complexity, and code coverage.

4.5.2.3.5. ***Deployment Frequency:*** This metric measures how often new code changes are deployed to production, a key indicator of a successful DevSecOps process.

4.5.2.3.6. ***Mean time to resolution (MTTR):*** This metric tracks the average time it takes to remediate and resolve issues or incidents occurring in production or during development, indicating the efficiency of incident response and vulnerability management practices.

4.5.3. CA 3: Cybersecurity Operations and Compliance

4.5.3.1. ***General:*** This capability ensures the confidentiality, integrity, and availability of the IDCS SoS and its data through comprehensive cybersecurity measures, adherence to compliance mandates, and proactive defense against cyber threats.

4.5.3.2. ***Task Description:*** Contractor shall implement and maintain a multi-layered security architecture. Achieve and maintain Authority to Operate (ATO) for all IDCS components. Ensure compliance with all applicable Cyber Survivability Attributes (CSAs). Conduct continuous security monitoring, intrusion detection, and threat hunting activities.

4.5.4. CA 4: Data Management, Analytics, Advanced Analytics and Intelligent Automation Integration

4.5.4.1. ***General:*** This capability focuses on harnessing data as a strategic asset for DCO by managing the full data lifecycle and leveraging advanced analytics, Artificial Intelligence (AI), and Machine Learning (ML) to provide actionable insights.

4.5.4.2. ***Task Description:*** The contractor shall develop and implement an integrated defensive cyberspace system with configurable log collection capabilities supporting compliance, data storage, analysis, and alert procedures, with performance thresholds including global data processing large volumes of data. The solution shall provide packet capture and analysis capabilities, visualization of large amounts of raw data and Intellectual Property (IP) data trends over time and maintain sufficient cyber resilience to mitigate cyber event effects through orderly, structured, and prioritized system responses that ensure minimum mission functionality. All development activities will be executed through a dynamic backlog of prioritized operational needs managed by the delegated lower-level requirements authority, with cost estimates and program affordability assessments conducted using rough order of magnitude cost tables suitable for the dynamic characteristics of integrated DCO capabilities, with detailed costing and key performance parameters to be refined in follow-on TOs.

4.5.5. CA 5: System and Enterprise Integration Services

4.5.5.1. ***General:*** The IDCS SoS integrates all components, external systems, and vendor solutions to achieve seamless interoperability and mission objectives. This materiel development solution aligns the defensive cyberspace weapon systems into a single, configurable capability that supports cloud integration, securely forwards data to a BDP, and integrates with both on-premises hunt capabilities and garrison DCO capabilities to enable operator correlation across cloud. The Government directs vendor integration through TOs, and capability drops within an Agile framework, ensuring standardized interfaces and data exchange that deliver the ability to sense, make sense, and act with speed, precision, and common data while mitigating DCO capability gaps.

4.5.5.2. ***Task Description:*** The contractor shall enable or deliver system integration capabilities that deliver a unified IDCS, meeting DoD requirements through seamless interface management, COTS/GOTS integration, and Application Programming Interface (API) development. The contractor must achieve full interoperability with existing DCO weapon systems that will enable the DAF's contribution to unified cyberspace operations forces. The solution shall implement and continuously maintain cyber survivability configuration baselines for all hardware, software, firmware, and open-source modules by version number, incorporate a machine-readable Software Bill of Materials (SBoM) for supply chain risk assessment and achieve an operationally acceptable cyber risk posture 24/7. The Contractor shall develop scalable integration capabilities that support correlation across cloud, and operational domain activity through centralized environments capable of interactive queries, automated workflows, algorithms, and ML, while ensuring

all data transmissions utilize only certified cryptographic capabilities and maintain protection commensurate with confidentiality requirements. All deliverables shall support an Agile framework development process, with configuration management processes that can achieve and maintain operationally-relevant risk posture within a period defined by the government dependent on threat, possible mitigation factors and the identification of degraded cyber risk posture, ultimately enabling operators utilizing separate systems to work on a common platform while providing enhanced cyberspace security, mission assurance, and defense, weapon systems, and critical infrastructure.

4.5.6. CA 6: Command, Control, Communications, Computers and Cyber Intelligence (C5I) Support

4.5.6.1. ***General:*** This capability provides the tools, systems, and processes for decisive and efficient command and control (C2) of DCO forces through timely cyber intelligence and highly reliable and secure communications. The IDCS aligns three (3) defensive cyberspace weapon systems into a single, configurable platform that enables operators to sense, make sense, and act with speed, precision, and common data. This integrated approach delivers operational and tactical control, while providing standardized data exchange, centralized environments, and common baseline equipment access across the DAF's Security Operations Center (SOCs), Cyber Protection Teams (CPTs), Mission Defense Teams (MDTs), and Cyber Maturity Assessments (CMA) providers. Through dedicated cloud environments and comprehensive tool suites, IDCS ensures resilient enterprise DCO capability for enhanced cyberspace security and defense, weapon systems, and critical infrastructure.

4.5.6.2. ***Task Description:*** Contractor shall develop, assist with integration, and sustain C2 applications. Integrate and manage cyber intelligence platforms that will be identified within future TOs. Support the development and dissemination of operational orders.

4.5.7. CA 7: Enterprise Architecture and Requirements Management

4.5.7.1. ***General:*** This capability involves defining, maintaining, and evolving the overall IDCS enterprise architecture and managing the lifecycle of system requirements to ensure alignment with strategic DCO goals and operational needs.

4.5.7.2. ***Task Description:*** Contractor shall develop, document, and maintain the IDCS enterprise architecture. Establish and manage a comprehensive management process. Ensure IDCS architecture and requirements (as identified by the National Institute of Standards and Technology (NIST) publications, best practices, DoD/DISA policies/directives, and the government policy letters) align with broader DoD and DAF enterprise architecture.

4.5.8. CA 8: Test, Evaluation, and Validation Services

4.5.8.1. ***General:*** This capability encompasses the planning, execution, and reporting of comprehensive test, evaluation, and validation activities to ensure IDCS capabilities are fit for purpose, meet specified requirements, and are operationally effective and suitable.

4.5.8.2. ***Task Description:*** Contractor shall develop and implement a comprehensive Test and Evaluation Master Plan (TEMP). Plan, design, and execute various types of testing. Develop and maintain realistic test environments.

4.5.9. CA 9: Service Management, Training, and Sustainment Operations

4.5.9.1. ***General:*** This capability focuses on providing comprehensive user support, training, and the ongoing sustainment of IDCS capabilities, including legacy system support during transition and the maintenance of new systems.

4.5.9.2. ***Task Description:*** Contractor shall establish and operate a multi-tiered service desk/help desk. Develop and deliver comprehensive training programs and materials. Provide ongoing sustainment for deployed IDCS hardware and software.

4.5.10. CA 10: Program Management, Governance, and Innovation

4.5.10.1. ***General:*** This capability encompasses the overall management and governance of the SPARTAN effort, fostering collaboration, ensuring effective execution, managing risks, and driving continuous innovation and efficiency.

4.5.10.2. ***Task Description:*** Contractor shall provide comprehensive program and project management. Implement and manage a risk management process. Facilitate communication and collaboration.

4.5.10.3. Contractor personnel shall collaborate/integrate with government-led teams. They shall possess required certifications and experience (specified in TOs), security clearances, and receive necessary training (initial and ongoing), staffing plans, transition plans, and retention plans may be requested.

5. GENERAL REQUIREMENTS

5.1. *Place of Performance*

Work may be performed at Contractor facilities, government sites, or other suitable locations, including authorized remote work locations. Primary performance locations include San Antonio, TX, and other locations as designated in individual TOs. Key Personnel Positions (KPPs) shall be local to San Antonio, TX or will commute (at the vendors expense) to San Antonio, TX work performance locations at least 4-5 days per week or as directed by the Government.

5.2. *Hours/Duty Days*

Normal duty hours are 7:30 am to 4:30 pm, Central Standard Time (CST), Monday through Friday (excluding Federal Holidays) including Family/Down Days as published. All reference days are business days unless otherwise identified.

5.3. *Federal Holidays*

Federal offices are closed on New Year's Day, Dr. Martin Luther King, Jr. Birthday, Presidents Day, Memorial Day, Juneteenth, Independence Day, Labor Day, Columbus Day, Veteran's Day, Thanksgiving Day, and Christmas Day.

5.4. *Travel*

The Contractor may be required to travel to various locations within the Continental United States (CONUS) and Outside the Continental United States (OCONUS) in performance of this contract. All travel arrangements shall be pre-approved by the CO or Contracting Officer Representative (COR).

6. CONTRACTOR RESPONSIBILITIES

6.1. *Contractor Furnished Property (CFP)/Services*

6.1.1. The Contractor shall provide all necessary personnel, software licenses, hardware, communication equipment, and training materials to perform the services outlined in this SOO.

6.1.2. Contractors shall provide CFP such as laptops, and Personal Identity Verification (PIV) Card readers for each team member.

6.2. *Contractor/Government Communication*

6.2.1. The Contractor shall designate a Focal Point to be the single point of contact for all Contractor and Government correspondence.

6.2.2. The Focal Point shall provide clear and consistent written and verbal responses to the Government within twelve (12) business hours of Government initiated communication (e.g., return phone calls, emails, or other communication).

6.2.3. The Contractor's Focal Point shall meet in person or virtually with the Government team at least weekly, quarterly, and additional meetings may be requested by the Government or the Contractor as necessary. The Contracting Officer (CO), Contractor Focal Point, CORs and/or other designated representative will provide monthly performance feedback to the Contractor.

6.3. *Key Personnel Positions (KPPs)*

The Contractor shall designate KPPs for IDCS efforts with the specified skills. Contractor personnel filling KPP roles shall remain assigned to the effort for the duration of the contract, unless otherwise approved by the Contracting Officer (CO) or COR.

6.4. *Personnel Administration*

6.4.1. The Contractor shall provide the management and support as required to professionally manage the SOO requirement. The Contractor shall provide for employees during designated Government non-workdays or other periods where Government offices are closed due to weather or security conditions.

6.4.2. The Contractor shall maintain the currency of their employees by providing initial and refresher training as required to meet the SOO requirements and provide a Company Employee Listing that shows the employees that are supporting the program, roles they are executing, if they are remote or on site, under what FTE, and the level of credentials they have (CAC, Security badge).

6.4.3. The Contractor shall maintain the currency of their facility and employees' security clearances as required to meet the SOO requirements. The Contractor shall make necessary travel arrangements for employees to accomplish tasks.

7. SECURITY REQUIREMENTS

7.1. *Contractor Security/Clearance Compliance*

7.1.1. The Contractor shall ensure all personnel meet the required security clearance levels (e.g., TS/SCI for KPPs) and comply with all security in-processing and recurring training requirements. All contractor personnel require minimum SECRET eligibility (TS/SCI for KPPs). KPPs must also be local to San Antonio, TX, and hold relevant cyber certifications in accordance with current DODI 8140.03.

7.1.1.1. The Contractor shall have 20% of staff or higher, in accordance with the TOs (rounded up to nearest Full-time Equivalent (FTE) actively cleared upon award, plus cleared KPPs. Clearance requirements are subject to change (including potential polygraphs).

7.1.2. The Contractor shall possess a Facility Clearance (FCL) at the TS/SCI level upon award. All contractor positions require a Common Access Card (CAC) or External Certificate Authority (ECA) for access to systems like Jira and Confluence.

7.2. *Security Training*

7.2.1. Within 10 business days of onboarding, contractors shall complete the required training, (Initial Security Training (IST), Original Classification Authority (OCA), Operations Security (OPSEC), Controlled Unclassified Information (CUI)), review Security Executive Agent Directive 3 (SEAD 3), and the IDCS Security Policy Memorandum. Quarterly SETA training is also mandatory.

7.2.2. The Contractor shall provide an updated Employee Listing Memorandum (ELM) with training records to the COR and signed Non-Disclosure Agreements (NDA). Subcontractors shall meet the same FCL and personnel security requirements.

7.3. *Operations Security (OPSEC)*

7.3.1. IAW with applicable security classification guidance (SCG) and other applicable Government instructions, the Contractor shall develop and implement physical,

personnel and information security programs necessary to protect against inadvertent disclosure of Controlled Unclassified Information and classified information pertaining to the PMO.

7.3.2. The Contractor shall review its current Operations Security (OPSEC) Plan that provides the Government with guidance on how to protect Critical Information about Contractor-owned proprietary systems under Government control annually, and all products produced for the PMO. If the Contractor does not have an OPSEC Plan, the Contractor shall develop one and submit it to the PMO and PMO Security SME, through the Technical Point of Contact (TPOC) for review, prior to implementation.

7.3.3. If changes to the OPSEC Plan are warranted, the Contractor will provide an updated OPSEC Plan IAW DD Form 1423-1. The revised OPSEC Plan shall be submitted to the PMO and PMO Security SME for review, prior to implementation. If no changes to the OPSEC Plan are warranted, the Contractor shall provide a contracts letter stating the review was completed and no modifications are needed and send the letter to the applicable TPOC. The Contractor shall submit this contracts letter IAW DD Form 1423-1.

7.3.4. The Contractor shall acknowledge the Emergency Action Plan (EAP) and adhere to the Critical Information List (CIL). Reportable events (foreign travel, relationships, etc.) shall be disclosed to the COR and Government Security Office. Security violations shall be reported within 12 hours of occurrence.

7.3.5. The Contractor shall adhere to OPSEC procedures (DoDD 5205.02E, DoDM 5202.02, AFI 10-701), protect CUI per EO 13556, 32 CFR Part 2002, DoDI 5200.48, and NIST SP 800-171, and protect classified information per the DD254, Security Addendum, and SCG.

7.3.6. The Contractor shall develop and maintain a Program Protection Implementation Plan (PPIP) based on the government-provided Program Protection Plan (PPP) (provided after award), submit a draft within 30 days of award and after PPP finalization. Subcontractors are subject to the same security requirements, and their Company Employee List (A042) shall be submitted to the COR.

7.4. *Cybersecurity Requirements*

7.4.1. The IDCS will implement cybersecurity configuration baselines and automated monitoring capabilities to handle sensitive information in compliance with AFI 17-101, Risk Management Framework (RMF) requirements. Offerors shall demonstrate the ability to support RMF artifact creation and meet all applicable security requirements to ensure Confidentiality, Integrity, and Availability. *(ref IDCS IS-ICD, to be released at a later date).*

7.4.2. Cyber Survivability Attributes: Offerors shall address how their solutions will achieve the CSAs defined in the IS-ICD *(ref IDCS IS-ICD, to be released at a later date)*, ensuring the IDCS can operate effectively in contested cyber environments.

7.4.3. *Cost and Software Data Reporting (CSDR): T*he Contractor shall systematically collect and report actual contract costs and technical information to the Cost Assessment Data Enterprise (CADE) and the USG based on the OSD DDCA-

approved CSDR Plan and associated Cost Accounting Standards regulations and directives.

8. CERTIFICATIONS AND AGREEMENTS

8.1. *Privileged User Certification*

8.1.1. Certain Information Assurance (IA) Workforce personnel positions under this effort may be designated as a Privileged User (PU) and must obtain the certifications required for their position category, specialty, and level to fulfill the IA baseline certification requirement in accordance with DODI/M 8140.03 Cyberspace Workforce Qualification and Management Program (or equivalent).

8.1.2. Each PU position identified on this contract shall sign a PU Agreement form, fulfill the security qualifications for systems access.

8.2. *Non-Disclosure Agreements (NDAs)*

8.2.1. The Contractor shall require all employees, prime and subcontractor, to sign an NDA prior to starting work.

8.2.2. The purpose of the NDA is to prevent disclosure of sensitive government information the Contractor may be exposed to throughout performance of this contract. Copies of signed NDAs shall be submitted to the CO.

8.3. *Associate Contractor Agreements (ACAs)*

8.3.1. Throughout the performance of the contract, the Contractor may be required to work with, or within proximity to, other contractors within the Software Environment. The Contractor shall enter an ACA with applicable third-party integrators and other stakeholders after contract award for any portion of the contract requiring joint participation in the accomplishment of the requirement. The agreements shall include the basis for sharing information, data, technical knowledge, expertise and/or resources essential to this effort, which shall ensure the greatest degree of cooperation to meet the terms of the contract. The Government will provide specific names of contractors to the Contractor.

8.3.2. ACAs shall include, but not limited to, the following general information:

8.3.2.1. Identify the associate contractors and their relationships.

8.3.2.2. Identify the program involved and the relevant Government contracts of the associate contractors.

8.3.2.3. Describe the associate contractor interfaces by general subject matter.

8.3.2.4. Specify the categories of information to be exchanged or support to be provided.

8.3.2.5. Include the expiration date (or event) of the ACA.

8.3.2.6. Identify potential conflicts between relevant Government contracts and the ACA, including agreements on protection of proprietary data and restrictions on employees.

8.3.2.7. The Contractor is not relieved of any contract requirements or entitled to any adjustments to the contract terms because of a failure to resolve a disagreement with an associate contractor. Liability for the improper disclosure of any proprietary data contained in or referenced by any ACA shall rest with the parties to the ACA and not the Government. All costs associated with the ACAs are included in the negotiated cost of this contract. ACAs may be amended as required by the Government during the performance of this contract. The Contractor shall submit copies of all ACAs to the CO.

DATA RIGHTS & INTELLECTUAL PROPERTY

8.4. The government will acquire and retain unlimited rights to all technical data and computer software developed specifically for the IDCS under this contract, unless otherwise specified in individual TOs.

8.5. Any modification changes or introductions of new software, modification of established processes/procedures or government directed development resources shall be approved by the Government prior to implementation.

8.6. All work performed and produced in accordance with this contract shall be under the sole ownership of the Government in accordance with DFARs clauses. 252.227-7013, 252.227-7014, 252.227-7018 and 252.227-7025

9. SERVICES SUMMARY

The Contractor's performance will be assessed by a process that measures success towards achieving defined performance objectives. The Contractor performance will be assessed against defined objectives per AFI 63-101, AFI 10-601, and FAR Subpart 37.6. Service acceptance follows the CO-approved Government Performance Plan. Quarterly Program Increment performance will be evaluated per the Quality Assurance Surveillance Plan (QASP). Code quality will be assessed using an Assessment Matrix (released at a later date) by a government-designated assessor. (NOTE: Assessment criteria may change due to evolving mission needs. A QASP will be tailored to and released as part of the supporting TOs.)

10. CONTRACT ADMINISTRATION

10.1. The Contractor shall establish clear organizational lines of authority and responsibility to ensure effective management of the resources assigned to the requirement. The Contractor shall assign one (1) representative as the Task Lead to have full Contractor authority to act in all contracts matters and be responsible and accountable to the CO in representing the Contractor for meeting the performance requirements of this SOO.

10.2. The Task Lead shall be available during normal duty hours, Monday through Friday, except Federal Holidays, to meet with the COR, Program Office (PO) or Government Lead to discuss program and/or technical issues. The Task Lead shall attend scheduled team and/or staff meetings, as requested by the COR, PO, or Government Lead.

10.3. The Contractor shall develop, maintain, and provide a Responsible, Accountable, Consulted, Informed, Quality Review (RACIQ) (See Appendix B. RACIQ Chart Example below) that communicates the Contractor's participation by various roles in completing program tasks and deliverables.

10.3.1. This matrix will assist a more comprehensive understanding of the Contractor's understanding of the cross-functional activities that are associated with IDCS contract activities, tasks and deliverables. The Contractor is responsible for populating this RACIQ chart with the specific names of individuals fulfilling each role within their organization.

10.3.2. This RACIQ chart shall be updated as needed in each MSR to reflect any changes in personnel or responsibilities. Appendix C is an example of a RACIQ chart: Once a RACIQ chart is completed it will be reviewed by the program office and will be approved if it is acceptable to the Government.

10.4. The Contractor shall establish processes and assign appropriate resources to effectively administer the requirements. The Contractor shall respond to Government requests for contractual actions in a timely manner. The Contractor shall have a single point of contact between the Government and Contractor personnel assigned to support contracts or TOs.

10.5. The Contractor shall assign work effort and maintain proper and accurate time keeping records of personnel assigned to work on the requirement.

11.DELIVERABLES

All deliverables shall be submitted in accordance with the schedule and format defined in individual DD Form 1423s associated with the TOs. The Government reserves the right to add additional Contract Data Requirements Listings (CDRLs) as needed to support future TOs. (CDRL example noted below in Table 1)

Table 1: Contract Data Requirements (CDRLs)

Example CDRLs	Title/Subtitle	DID	Delivery Frequency
A001	Monthly Status Report/ Cost Summaries	DI-MGMT-80368A & DI-FNCL-80331A	7th calendar day of each month
A002	OPSEC Plan Review	DI-MGMT-80934C	Annual
A003	Technical Reports	DI-MISC-80508B	Upon Request or delivery of capability
A004	Software Design Description	DI-IPSC-81435A	Quarterly
A005	Software User Manual / Release Documentation	DI-IPSC-81443A	5 days prior to production release / As Required
A006	Hardware Installation Reports	DI-MGMT-80453B	10 days prior to installation
A007	Training Materials/Manuals	DI-ILSS-80872	5 days prior to production release
A008	Test Plans and Reports	DI-NDTI-80583A & DI-NDTI-80809	10 days prior to event
A009	Software Test Reports (STR)	DI-MISC-80508B	7th Calendar Day of each month
A010	Security Assessment Reports	DI-MISC-80048B	Quarterly
A011	Project Presentation	DI-ADMN-81505	IAW Task Order Requirements (Upon Significant Milestones)
A012	Contractor Business Data Report (CSDR)	DI-FNCL-81765B	IAW Task Order Requirements (As Required by DoD CSDR Policy)
A013	Software Resources Data Reporting	DI-MGMT-82035A	IAW Task Order Requirements (Monthly)
A014	Technical Data Report	DI-MGMT-82165	IAW Task Order Requirements (As Needed)

A015	Cost and Hour Report (FlexFile)	DI-FNCL-82162	IAW Task Order Requirements (Monthly)
A016	Quantity Data Report	DI-MGMT-82164	IAW Task Order Requirements (Monthly)
A017	Maintenance and Repair Parts Data Report	DI-MGMT-82163	IAW Task Order Requirements (Monthly)
A018	Software Version Description	DI-IPSC-81442A	IAW Task Order Requirements (Upon Software Release)
A019	Commercial Off-The-Shelf (COTS)/Manual and Associated Supplemental Data	DI-TMSS-80527C	IAW Task Order Requirements (Upon COTS Procurement)
A020	Capability/Software Requirements Specification (C/SRS)	DI-IPSC-81433	IAW Task Order Requirements (Update as Needed)
A021	System/Subsystem Specification (SSS)	DI-IPSC-81431A	IAW Task Order Requirements (Update as Needed)
A022	System/Subsystem Description (SSDD)	DI-IPSC-81432A	IAW Task Order Requirements (Update as Needed)
A023	Database Design Description (DBDD)	DI-IPSC-81437A	IAW Task Order Requirements (Update as Needed)
A024	Technical Report-System Security Plan (SSP)	DI-MISC-80508B	IAW Task Order Requirements (Annual Review & Update)
A026	Test Description	DI-NDTI-80583A	IAW Task Order Requirements (As Testing Occurs)
A027	Software Programmers Guide (SPG)	DI-IPSC-81633	IAW Task Order Requirements (Update as Needed)
A028	Interface Control Document (ICD)	DI-CMAN-81248A	IAW Task Order Requirements (Update as Needed)
A029	Maintenance Support Plan	DI-ILSS-81225	IAW Task Order Requirements (Annual Review & Update)

A030	Conference Minutes	DI-ADMIN-81250A	IAW Task Order Requirements (Within 5 Business Days of Conference)
A031	Equipment Installation Instructions	DI-MISC-81321	IAW Task Order Requirements (Upon Equipment Installation)
A032	Vulnerability Analysis Report (VAR)	DI-MISC-80049A	IAW Task Order Requirements (Monthly or Quarterly, depending on sensitivity)
A033	Site Preparation Requirements and Installation Plan	DI-MGMT-80033A	IAW Task Order Requirements (Prior to Installation)
A034	Test Description (Installation & Test Procedures)	DI-NDTI-80583A	IAW Task Order Requirements (As Installation Testing Occurs)
A035	Software Transition Plan (STrP)	DI-IPSC-81429A	IAW Task Order Requirements (Update as Needed)
A036	Technical Report (DR Closure Plan)	DI-MISC-80508B	IAW Task Order Requirements (Monthly/As Needed)
A037	Software Documentation	DI-IPSC-81756	IAW Task Order Requirements (Update as Needed)
A038	Security Test Plan	DI-NDTI-81351	IAW Task Order Requirements (Update as Needed)
A039	Technical Report (Generic Report)	DI-MISC-80508B	IAW Task Order Requirements (As Needed)
A040	Technical Report (System Architect Views)	DI-MGMT-81644B	IAW Task Order Requirements (Update as Needed)
A041	Multimedia Requirements (Videos)	DI-MGMT-81997A	IAW Task Order Requirements (As Needed)

A042	Software Bill of Materials	DI-SESS-82433	IAW Task Order Requirements (As Needed)
A043	Subcontractor Management Plan	DI-SESS-82408	IAW Task Order Requirements (Annual Review & Update)
A044	Company Employee List	DI-MISC-81364	IAW Task Order Requirements (Monthly)
A045	Cybersecurity Plan	DI-MGMT-81448B	IAW Task Order Requirements (Annual Review & Update)
A046	Incident Response Plan	DI-MGMT-81957	IAW Task Order Requirements (Annual Review & Update, Upon Major Incidents)
A047	Vulnerability Management Plan	DI-MGMT-81958	IAW Task Order Requirements (Annual Review & Update)
A048	Configuration Management Plan	DI-CMAN-80727B	IAW Task Order Requirements (Annual Review & Update, Upon Significant Changes)
A049	Risk Management Plan	DI-MGMT-81427A	IAW Task Order Requirements (Monthly/Quarterly Review & Update)
A050	Data Rights Assertion List	DI-IPSC-81424A	IAW Task Order Requirements (Update as Needed)
A051	License Agreements	DI-MGMT-82090A	IAW Task Order Requirements (Upon License Procurement)
A052	Source Code	DI-IPSC-81465B	IAW Task Order Requirements (As Needed)
A053	Supply Chain Risk Management Plan	DI-SESS-82243A	IAW Task Order Requirements (Annual Review & Update)

A054	Security Architecture Description	DI-MISC-82161	IAW Task Order Requirements (Annual Review & Update, Upon Significant Changes)
A055	Data Dictionary	DI-IPSC-81436A	IAW Task Order Requirements (As Needed)
A056	Physical Security Plan	DI-MGMT-80435A	IAW Task Order Requirements (Annual Review & Update)
A057	AI/ML Model Documentation Package	DI-IPSC-82500	IAW Task Order Requirements (As AI/ML Models are Developed/Updated)
A058	Big Data Architecture and Implementation Plan	DI-MGMT-81473	IAW Task Order Requirements (Update as Needed)
A059	Quantum Computing Implementation Report	DI-MISC-80508B	IAW Task Order Requirements (As Needed)
A060	Neural Engine Performance Analysis Report	DI-MISC-80508B	IAW Task Order Requirements (As Needed)
A061	Microprocessor Design and Test Data	DI-ELEC-81872	IAW Task Order Requirements (As Needed)
A062	Hardware Integration Plan	DI-MGMT-81649	IAW Task Order Requirements (Prior to Hardware Integration Activities)
A063	AI/ML Ethics and Governance Plan	DI-MGMT-82090A	IAW Task Order Requirements (Annual Review & Update)
A064	Data Lineage and Provenance Report	DI-MISC-80508B	IAW Task Order Requirements (As Needed)
A065	Technology Transition Plan (AI/ML focus)	DI-IPSC-81429A	IAW Task Order Requirements (As Needed)

A066	Algorithm Security Assessment Report	DI-MISC-80049A	IAW Task Order Requirements (Quarterly, Upon Algorithm Changes)
A067	Data Security and Privacy Plan	DI-MGMT-81959	IAW Task Order Requirements (Annual Review & Update)
A068	Containerization and Kubernetes Deployment Plan and Specification	DI-IPSC-82100	IAW Task Order Requirements (As Needed, Prior to Deployment)
A069	Container Security Scanning and Vulnerability Report	DI-MISC-80049A	IAW Task Order Requirements (Monthly or Quarterly)
A070	RMF Security Package (SSP, SAR, POA&M)	DI-MISC-80048B/80508B/82161	IAW Task Order Requirements (Annual Review & Update, Upon System Changes)
A071	ATO Package Updates and Maintenance	DI-MGMT-80727B	IAW Task Order Requirements (As Needed to Maintain ATO)
A072	Cloud Security Architecture Design	DI-MISC-82161	IAW Task Order Requirements (Annual Review & Update, Upon Cloud Environment Changes)
A073	Cloud Migration Plan	DI-MGMT-81447	IAW Task Order Requirements (Prior to Migration Activities, Update as Needed)
A074	Cloud Service Provider (CSP) Security Assessment	DI-MISC-80049A	IAW Task Order Requirements (Annually, Upon CSP Security Changes)
A075	DevSecOps Pipeline Definition and Implementation	DI-MGMT-80453B	IAW Task Order Requirements (Update as Needed)
A076	Static Code Analysis Reports	DI-MISC-80049A	IAW Task Order Requirements (As Needed)

A077	Dynamic Application Security Testing (DAST) Reports	DI-MISC-80049A	IAW Task Order Requirements (As Needed)
A078	Software Composition Analysis (SCA) Reports	DI-MISC-80049A	IAW Task Order Requirements (As Needed)
A079	Infrastructure as Code (IaC) Security Scans	DI-MISC-80049A	IAW Task Order Requirements (Monthly or Quarterly)
A080	Infrastructure as Code (IaC) and Configuration as Code (CaC) Repository Access	DI-SESS-82433	IAW Task Order Requirements (As Needed)
A081	Cloud Environment Provisioning and Security Compliance Report	DI-MISC-80049A	IAW Task Order Requirements (Monthly or Quarterly)
A082	Hybrid Cloud Architecture Diagram and Documentation	DI-MGMT-81644B	IAW Task Order Requirements (Annual Review & Update)
A083	Hardware Lifecycle Management Plan and Inventory Report	DI-MGMT-80368A	IAW Task Order Requirements (Annual Review & Update)
A084	Certificate to Field (CtF) Readiness Report	DI-MISC-80508B	IAW Task Order Requirements (Prior to Deployment)
A085	API Specification and Interface Control Document (ICD) Compliance Report	DI-CMAN-81248A	IAW Task Order Requirements (Update as Needed)
A086	Software Component Security Attestation	DI-MISC-80049A	IAW Task Order Requirements (As Needed)
A087	Container Registry Scan Report	DI-MISC-80049A	IAW Task Order Requirements (Monthly or Quarterly)
A088	Regression Test Report	DI-NDTI-80809	IAW Task Order Requirements (As Needed)

A089	Quantum-Resistant Cryptography Implementation Plan and Assessment	DI-MISC-80508B	IAW Task Order Requirements (Update as Quantum Computing Threat Landscape Evolves)
A090	Zero Trust Architecture Implementation Report	DI-MISC-82161	IAW Task Order Requirements (Annual Review & Update)
A091	Cyber Survivability Attributes (CSA) Compliance Assessment Report	DI-MISC-80508B	IAW Task Order Requirements (Annually)
A092	Threat Hunting Activity Report	DI-MISC-80049A	IAW Task Order Requirements (Monthly or Quarterly)
A093	Incident Response Exercise Report	DI-MISC-80049A	IAW Task Order Requirements (Annually)
A094	Data Pipeline Architecture Diagram and Documentation	DI-MGMT-81644B	IAW Task Order Requirements (Update as Needed)
A095	AI/ML Model Performance Monitoring Report	DI-MISC-80508B	IAW Task Order Requirements (Monthly or Quarterly)
A096	Data Governance Plan and Compliance Report	DI-MGMT-82090A	IAW Task Order Requirements (Annual Review & Update)
A097	Data Security and Privacy Impact Assessment	DI-MGMT-80052	IAW Task Order Requirements (As Needed)
A098	Enterprise Service Bus (ESB) Architecture Diagram and Documentation	DI-MGMT-81644B	IAW Task Order Requirements (Update as Needed)
A099	API Gateway Specification and Usage Report	DI-MISC-80508B	IAW Task Order Requirements (Monthly or Quarterly)
A100	Interoperability Test Plan and Report	DI-NDTI-80583A	IAW Task Order Requirements (As Needed)

A101	C2 Application Architecture Diagram and Documentation	DI-MGMT-81644B	IAW Task Order Requirements (Update as Needed)
A102	Cyber Intelligence Platform Integration Report	DI-MISC-80508B	IAW Task Order Requirements (Quarterly)
A103	Operational Order (OPORD) Generation and Distribution Process	DI-MGMT-80453B	IAW Task Order Requirements (As Needed)
A104	DDIL Communication Architecture Diagram and Documentation	DI-MGMT-81644B	IAW Task Order Requirements (Update as Needed)
A105	Enterprise Architecture Artifact Repository Access	DI-SESS-82433	IAW Task Order Requirements (Continuous Read-Only Access for Government)
A106	Requirements Traceability Matrix	DI-MGMT-81447	IAW Task Order Requirements (Update as Needed)
A107	Analysis of Alternatives (AoA) Report	DI-MISC-80508B	IAW Task Order Requirements (As Needed)
A108	Control Plane Architecture Document	DI-MISC-82161	IAW Task Order Requirements (Annual Review & Update)
A109	National Institute of Standards and Technology (NIST) Publication Report	DI-MISC-80508B	IAW Task Order Requirements (Annual Review & Update)
A110	Test and Evaluation Strategy (TES) Document	DI-NDTI-81297A	IAW Task Order Requirements (Annual Review & Update)
A111	Test Environment Configuration Management Plan	DI-MGMT-80727B	IAW Task Order Requirements (Update as Needed)
A112	Independent Verification and Validation (IV&V) Report	DI-MISC-80508B	IAW Task Order Requirements (As Needed)
A113	Service Level Agreement (SLA) Monitoring and Reporting	DI-MGMT-80368A	IAW Task Order Requirements (Monthly)

A114	Training Plan and Curriculum	DI-ILSS-80872	IAW Task Order Requirements (Update as Needed)
A115	Transition Plan and Progress Report	DI-MGMT-81447	IAW Task Order Requirements (Update as Needed)
A116	Transition Playbook	DI-MGMT-80453B	IAW Task Order Requirements (Update as Needed)
A117	Risk Management Plan and Mitigation Report	DI-MGMT-81427A	IAW Task Order Requirements (Update as Needed)
A118	Innovation Proposal and Implementation Plan	DI-MGMT-80453B	IAW Task Order Requirements (As Needed)
A119	Subcontractor Management Plan and Performance Report	DI-SESS-82408	IAW Task Order Requirements (Annual Review & Update)
A120	Communications Plan	DI-ADMN-81505	IAW Task Order Requirements (Update as Needed)

12.APPENDICES

Appendix A. IDCS Capability Areas & Objectives Matrix

1. Cloud Services and Infrastructure Management	CR #7
1.1 Implement Infrastructure as Code (IaC) and Configuration as Code (CaC) practices for automated provisioning, configuration, and management of infrastructure resources.	CR #7
1.2 Monitor infrastructure health and performance, implementing proactive measures to prevent outages and ensure operational continuity.	CR #4, CR #7
1.3 Implement automated processes for the secure and compliant provisioning of new cloud environments (e.g., accounts, subscriptions, resource groups), ensuring the immediate application of organizational security policies, cost controls, and compliance guardrails.	CR #7
1.4 Develop, implement, and maintain a centralized framework for defining, enforcing, and auditing cloud guardrails across all provisioned environments, ensuring continuous alignment with evolving security standards and regulatory requirements.	CR #7, CR #4, CR #5
1.5 Ensure the infrastructure supports a modular, scalable, and secure control plane architecture, enabling centralized management, configuration, and orchestration of IDCS components and services across hybrid cloud environments (incorporating Cloud One, Platform One, JWCC and other authorized environments). This includes support for Infrastructure as Code (IaC) and Configuration as Code (CaC) to automate control plane provisioning and management.	CR #7
1.6 Implement mechanisms for automated control plane scaling, redundancy, and failover to ensure high availability and resilience of the overall IDCS platform, aligned with Cyber Survivability Attributes (CSAs) and DoD Zero Trust guidance.	CR #7
1.7 Design, build, and maintain a secure, resilient, and scalable hybrid cloud infrastructure (incorporating Cloud One, Platform One, and other authorized environments) to host IDCS services and applications.	CR #7
1.8 Manage and sustain on-premises hardware, including servers, storage, and networking equipment, ensuring high availability and performance.	CR #7
1.9 Implement and manage robust network infrastructure, ensuring secure and reliable connectivity for all IDCS components and users, including support for diverse network environments and enclaves.	CR #7
1.10 Provide lifecycle management for all hardware platforms, including garrison, deployable (e.g., DMSS-comparable), mobile, and sensor platforms (fixed and SFF sensors, MRT-C).	CR #7
1.11 Ensure infrastructure solutions meet energy efficiency (KPP Energy), sustainment (KPP Sustainment), and force protection (KPP Force Protection) requirements.	CR #7

2. Agile Software Engineering and DevSecOps	CR #4, CR #5, CR #7
2.1 Apply DevSecOps principles and practices to the development, testing, and deployment of control plane components, integrating automated security testing (SAST, DAST) and continuous monitoring into the CI/CD pipeline. Ensure that control plane software meets Certificate to Field (CtF) requirements and utilizes Iron Bank hardened containers (or similar approved process).	CR #5
2.2 Design the control plane with modularity and well-defined APIs to facilitate integration with existing and future IDCS components, external systems (e.g., JCWA, ABMS), and third-party services. Implement rigorous interface management and version control.	CR #5
2.3 Design, develop, and maintain high-quality, secure, and modular software applications and services for the IDCS SoS, adhering to approved coding standards and minimizing technical debt.	CR #4, CR #5, CR #7
2.4 Implement and manage a robust DevSecOps framework, including automated Continuous Integration/Continuous Delivery (CI/CD) pipelines for rapid and reliable software releases.	CR #4, CR #5, CR #7
2.5 Integrate security best practices and automated security testing (e.g., SAST, DAST) into all stages of the Software Development Lifecycle (SDLC).	CR #4, CR #5
2.6 Develop and maintain containerized applications using industry's best practices and ensure compatibility with approved container orchestration platforms (e.g., the PMO prescribed Kubernetes distribution)	CR #7
2.7 Conduct thorough software testing, including unit, integration, system, performance, and user acceptance testing, to ensure software quality and reliability.	CR #4, CR #5, CR #8
2.8 Manage software configurations, versions, and releases effectively using appropriate tools and processes.	CR #7
2.9 Provide software sustainment, including bug fixes, patches, and enhancements for new and legacy IDCS software components.	CR #7
3. Cybersecurity Operations and Compliance	CR #4, CR #5, CR #6, CR #7, CR #8
3.1 Ensure compliance with DFARS Clause 252.204-7012 for safeguarding covered defense information and cyber incident reporting.	CR #7
3.2 Implement and manage Identity and Access Management (IAM) solutions, including multi-factor authentication (MFA).	CR #7
3.3 Address and mitigate risks associated with quantum computing through the assessment and implementation of quantum-resistant cryptography where appropriate.	CR #7

3.4 Implement and maintain a multi-layered security architecture based on Zero Trust principles across the IDCS SoS.	CR #4, CR #5, CR #7
3.5 Implement a Zero Trust security model for the control plane, enforcing least privilege access, continuous authentication and authorization, and micro-segmentation to minimize the attack surface. Leverage Identity and Access Management (IAM) solutions, including multi-factor authentication (MFA), for control plane access control.	CR #5, CR# 6, CR#7
3.6 Implement continuous security monitoring, intrusion detection, and threat hunting capabilities specifically tailored for the control plane. Integrate with Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) systems for automated incident response.	CR #5, CR# 6
3.7 Achieve and maintain Authority to Operate (ATO) for all IDCS components in accordance with the Risk Management Framework (RMF) and NIST SP 800-53.	CR #7
3.8 Ensure compliance with all applicable Cyber Survivability Attributes (CSAs) as defined in the IS-ICD and relevant RDPs (to be provided at a latter date), addressing prevention, mitigation, and recovery.	CR #4, CR #5, CR #6, CR #7, CR #8
3.9 Implement, integrate, and sustain capabilities for continuous security monitoring, intrusion detection, and threat hunting activities within the IDCS platform. Leveraging tools such as SIEM, SOAR, EDR, and NTA solutions, to enable DCO operators.	CR #4, CR #5
3.10 Perform regular vulnerability assessments, penetration testing, and security audits to identify and remediate security weaknesses.	CR #4, CR #5, CR #8
3.11 Develop and implement incident response plans and procedures to effectively manage and remediate security incidents.	CR #5, CR #6
4. Data Management, Analytics, and AI/ML Integration	CR #2, CR #4, CR #5, CR #7
4.1 Design, develop, and manage robust data pipelines for ingesting, processing, transforming, and storing large volumes of diverse data (e.g., logs, network traffic, threat intelligence) from various sources, including ELX and BDP.	CR #2, CR #4, CR #7
4.2 Implement and manage scalable data storage solutions (e.g., data lakes, data warehouses) ensuring data availability, reliability, and security.	CR #7
4.3 Develop and deploy advanced data analytics capabilities, including statistical analysis, machine learning (ML) models, and AI-driven tools, to enhance threat detection, prediction, and response.	CR #2, CR #4, CR #5
4.4 Create and maintain interactive dashboards and visualization tools to provide real-time situational awareness and facilitate data-driven decision-making for DCO operators.	CR #2, CR #4, CR #5
4.5 Establish and enforce data governance policies, data quality standards, and metadata management practices across the IDCS.	CR #7

4.6 Ensure data security and privacy in compliance with DoD regulations and policies, including data-at-rest and data-in-transit encryption.	CR #7
4.7 Support the integration and operationalization of AI/ML capabilities, adhering to responsible AI principles and CDAO guidance.	CR #2, CR #4, CR #5, CR #7
5. System and Enterprise Integration Services	**CR #7**
5.1 Define and manage standardized interfaces and protocols for control plane communication and data exchange between IDCS components, external systems, and authorized users. Ensure compliance with Interface Control Documents (ICDs).	CR #7
5.2 Provide platform engineering expertise to establish and maintain common services, tools, and environments that support the integration and operation of the IDCS control plane.	CR #7
5.3 Define, document, and manage interfaces between IDCS components, external systems (e.g., JCWA, ABMS), and other DoD enterprise services, adhering to Interface Control Documents (ICDs).	CR #7
5.4 Perform integration of COTS, GOTS, and custom-developed software and hardware components into the IDCS architecture.	CR #7
5.5 Ensure interoperability with legacy DCO systems during transition and with modernized DCO capabilities.	CR #7
5.6 Develop and manage APIs to facilitate secure data exchange and service integration across the IDCS and with external partners.	CR #7
5.7 Provide platform engineering expertise to establish and maintain common services, tools, and environments that support the integration and operation of IDCS capabilities.	CR #7
5.8 Conduct rigorous integration testing to validate end-to-end functionality and interoperability.	CR #7, CR #8
5.6 Support integration efforts with solutions from multiple vendors, ensuring a cohesive and unified IDCS SoS.	CR #7
6. Command, Control, Communications, and Cyber Intelligence (C4I) Support	CR #1, CR #2
6.1 Develop, integrate, and sustain C2 applications that provide comprehensive situational awareness, mission planning, tasking, and execution monitoring for DCO operations.	CR #1
6.2 Integrate and manage cyber intelligence platforms and tools to collect, analyze, correlate, and disseminate threat intelligence from various sources (e.g., CTIC/Pulse, BDP Threat Hub).	CR #2
6.3 Support the development and dissemination of operational orders in human and machine-readable formats.	CR #1
6.4 Facilitate timely, data-driven feedback into the DCO operations and C2 tasking cycle.	CR #1

6.5 Ensure secure and resilient communication capabilities for DCO forces operating in diverse environments, including DDIL conditions.	CR #7
6.6 Support DCO planning activities by integrating ISR, situational awareness, and risk management data.	CR #2, CR #3
6.7 Develop and integrate C2 applications that provide comprehensive situational awareness, mission planning, tasking, and execution monitoring specifically for the IDCS control plane.	CR #1
6.8 Integrate and manage cyber intelligence platforms and tools to collect, analyze, correlate, and disseminate threat intelligence relevant to the control plane, enabling proactive threat hunting and incident response. Facilitate timely, data-driven feedback into the DCO operations and C2 tasking cycle.	CR #2, CR# 1
7. Enterprise Architecture and Requirements Management	CR #7
7.1 Develop, document, and maintain the IDCS enterprise architecture, including operational, system, and technical views, ensuring it supports modularity, scalability, and interoperability.	CR #7
7.2 Establish and manage a comprehensive requirements management process, including elicitation, analysis, documentation, validation, and traceability of requirements throughout the IDCS lifecycle.	CR #7
7.3 Ensure IDCS architecture and requirements align with broader DoD and DAF enterprise architecture and strategic directives (e.g., JCWA, Zero Trust).	CR #7
7.4 Conduct analyses of alternatives, including cost and trade space analysis, technology assessments, and roadmap development to guide the evolution of IDCS capabilities and incorporate emerging technologies.	CR #7
7.5 Support configuration management of architectural and requirements artifacts.	CR #7
7.6 Facilitate stakeholder engagement to ensure architectural and requirements alignment with user needs and operational realities.	CR #7
7.7 Ensure that the IDCS enterprise architecture explicitly addresses the control plane's functions, interfaces, and security requirements.	CR #7
7.8 Develops and maintains a control plane architecture and requirements document that is aligned to the National Institute of Standards and Technology (NIST) publications, best practices, DoD/DISA policies/directives, and government policy letters	CR #7
8. Test, Evaluation, and Validation Services	CR #8
8.1 Manage a tailored, comprehensive Test and Evaluation (T&E) program, including the development and implementation of a Test and Evaluation Strategy (TES) for the IDCS SoS, in accordance with applicable Air Force instructions, publications, policy, and other guidance for the Software Acquisition Pathway.	CR #8

8.2 Plan, design, and execute various types of testing, including developmental test and evaluation (DT&E), interoperability testing, security testing (including penetration testing), performance testing, and usability testing; and provide comprehensive support for independent operational test and evaluation (OT&E).	CR #8
8.3 Develop and maintain realistic test environments, including simulation capabilities and range integration, that emulate operational conditions.	CR #8
8.4 Utilize automated testing tools and techniques to improve test efficiency and coverage.	CR #8
8.5 Collect, analyze, and report test data to assess system performance against requirements and identify deficiencies.	CR #8
8.6 Support the validation of DCO TTPs and the assessment of operational effectiveness.	CR #8
8.7 Provide Independent Verification and Validation (IV&V) services as required.	CR #8
9. Service Management, Training, and Sustainment Operations	CR #7
9.1 Establish and operate a multi-tiered service desk/help desk to provide timely technical support to IDCS users.	CR #7
9.2 Develop and deliver comprehensive training programs and materials for IDCS users, operators, and maintainers, covering all aspects of the system, in accordance with applicable Air Force instructions, publications, and policies.	CR #7
9.3 Provide ongoing sustainment for deployed IDCS hardware and software, including preventative and corrective maintenance, patch management, and obsolescence management.	CR #7
9.4 Manage the transition of services from legacy systems to modernized IDCS capabilities, ensuring continuity of operations and minimal disruption to users.	CR #7
9.5 Develop and maintain comprehensive system documentation, including user manuals, administration guides, and troubleshooting procedures.	CR #7
9.6 Implement IT Service Management (ITSM) best practices for managing IDCS services.	CR #7
9.7 Support the logistical requirements for IDCS, including asset management, sparing, and deployment support.	CR #7
10.Program Management, Governance, and Innovation	CR #1, CR #7
10.1 Provide comprehensive program and project management for awarded Task Orders, including planning, execution, monitoring, control, and reporting. This encompasses documenting all aspects of program management activities and developing key artifacts such as integrated schedules, roadmaps, and briefing materials, all in accordance with Government oversight.	CR #1, CR #7

10.2 Implement and manage a robust risk management process, identifying, analyzing, mitigating, and monitoring program risks.	CR #1, CR #7
10.3 Facilitate effective communication and collaboration among Government stakeholders, prime contractors, subcontractors, and other vendors.	CR #1, CR #7
10.4 Ensure adherence to all contractual requirements, including cost, schedule, performance, and reporting (e.g., CSDR).	CR #1, CR #7
10.5 Develop and implement strategies for optimizing resource utilization, achieving cost efficiencies, and delivering value to the Government.	CR #1, CR #7
10.6 Foster a culture of continuous improvement and innovation, identifying and proposing new technologies, methodologies, and processes to enhance IDCS capabilities and DCO practices.	CR #1, CR #7
10.7 Provide support for overarching IDIQ-level governance, coordination, and reporting as required by the Government.	CR #1, CR #7
10.8 Manage subcontractor performance and ensure seamless integration of subcontractor efforts.	CR #1, CR #7

Appendix B. RACIQ Chart Example

Deliverable Subject to Evaluation	Responsible (Performs the work)	Accountable (Owns the KPI)	Consulted (Provides Input)	Informed (Kept Aware)	Quality Review (Ensures Standards)
Tested Code	Contractor Developer, Contractor Tester	Contractor QA Lead	Contractor Security SME (for security-related tests)	Contractor Project Manager, Government Program Manager	Contractor QA Team, Contractor Development Lead
Properly Styled Code	Contractor Developer	Contractor Development Lead	Contractor Style Guide SME, Government Style Guide SME (if applicable)	Contractor Project Manager	Contractor Development Lead, Automated Linting Tools
Deployed	Contractor DevOps Engineer	Contractor DevOps Lead	Contractor Developer, Contractor Security SME	Contractor Project Manager, Government Program Manager	Contractor DevOps Lead, Contractor Security Team
Documented	Contractor Developer, Contractor Technical Writer	Contractor Technical Writer Lead	Contractor Developer Lead, Government Documentation SME (if applicable)	Contractor Project Manager	Contractor Technical Writer Lead
Security	Contractor Security Engineer, Contractor Developer	Contractor Security Lead	Government Security SME, Contractor DevOps Engineer	Contractor Project Manager, Government Program Manager	Contractor Security Lead, Automated Security Scanning Tools
Project Lead or Program Manager (MSRs, PI Planning)	Contractor Project Manager, Contractor Program Manager	Contractor Program Manager	Government Program Manager, Government Technical Leads	Government Program Manager, Stakeholders	Contractor Program Manager
Manpower (GSA Minimum Qualifications)	Contractor HR, Contractor Hiring Manager, Contractor Team Leads	Contractor Program Manager	Contractor Legal (if needed)	Government Program Manager, Government Contracting Officer	Contractor Program Manager, Contractor HR

Appendix C. References:

DoD 5000.02, *Operation of the Adaptive Acquisition Framework* (https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500002p.pdf)

DoDI 5000.87, *Operation of the Software Acquisition Pathway* (https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500087p.pdf)

Federal Acquisition Regulation (FAR) (https://www.acquisition.gov/browse/index/far)

Defense Federal Acquisition Regulation Supplement (DFARS) (https://www.acquisition.gov/dfars)

Integrated Defensive Cyberspace Operations (DCO) Information Systems Initial Capabilities Document (IS-ICD) *(may be provided at a later date)*

IDCS Requirements Definition Packages (RDPs) *(may be provided at a later date)*

DoD Enterprise DevSecOps Reference Design (https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0_Public%20Release.pdf?ver=2019-09-26-115824-583)

DoD Enterprise DevSecOps Strategy Guide (https://dodcio.defense.gov/Portals/0/Documents/Library/DoDEnterpriseDevSecOpsStrategyGuide.pdf)

DevSecOps Enterprise Container Hardening Process Guide (https://dl.dod.cyber.mil/wp-content/uploads/devsecops/pdf/Final_DevSecOps_Enterprise_Container_Hardening_Guide_1.2.pdf)

DoD Directive 5205.02E, *DoD Operations Security (OPSEC) Program* (https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/520502e.PDF)

DoD Manual 5202.02, *Operations Security (OPSEC)* (https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/520502m.pdf)

AFI 10-701, *Operations Security* (https://static.e-publishing.af.mil/production/1/af_a3/publication/afi10-701/afi10-701.pdf)

National Security Decision Directive Number 298

NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations* (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf)

Committee on National Security Systems (CNSS) Instruction 1253 (https://www.dcsa.mil/portals/91/documents/ctp/nao/CNSSI_No1253.pdf)

DoDI 8500.01, *Cybersecurity* (https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf)

DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology* (https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf?ver=2019-02-26-101520-300)

Cyber Survivability Endorsement Implementation Guide https://www.dau.edu/sites/default/files/Migrated/CopDocuments/Guide%20-%20Cyber%20Survivability%20Endorsement%20Implementation.pdf