F-35 JOINT PROGRAM OFFICE (F-35 JPO) / SERVICES ACQUISITION TEAM (SAT)

PROGRAM SECURITY SUPPORT SERVICES

SINGLE AWARD - INDEFINITE DELIVERY / INDEFINITE QUANTITY (ID/IQ)

TASK ORDER 0004

CYBERSECURITY SUPPORT

STATEMENT of WORK (SOW)

12 AUGUST 2020

---

1. OVERVIEW

DRAFT

The F-35 Lightning II Program (also known as the Joint Strike Fighter Program) is a joint, multi-national program and is the Department of Defense's (DoD) focal point for defining affordable next generation strike aircraft weapon systems among the United States (U.S.) Air Force (USAF), U.S. Navy (USN), U.S. Marine Corps (USMC), and U.S. allies composed of seven (7) cooperative international partners: the United Kingdom, Italy, Netherlands, Canada, Australia, Denmark, and Norway. The program's objective is to develop and deploy the F-35 Air System (AS), a three (3) variant family of highly common and affordable 5th Generation strike fighter aircraft that meets the operational needs of the USAF, USN, USMC, and cooperative partner international services. Additional production of the F-35 is made through Foreign Military Sales (FMS). The F-35 Enterprise is defined as, but not limited to: Air Vehicle (AV), AS, AS Ground Support, Support Equipment Systems, Depot Maintenance, Business, Flight Test, and Training Systems. The F-35 security team has a mature Program Protection Plan (PPP), robust policies and procedures and established Special Access Program (SAP) facilities throughout the world. Requirements continue to evolve as the program matures and the F-35 security team is responsible for ensuring that any new security challenges are appropriately identified and safeguarded in accordance with (IAW) DoD regulations and specifications.

2. SCOPE

The F-35 Joint Program Office (F-35 JPO) requires program security support services to support its critical mission of developing, deploying and sustaining the next generation strike fighter aircraft. The program security support disciplines consist of Program Management, General Security Support, Information Security Support, Industrial Security Support, Physical Security Support, Personnel Security Support, Counter-Intelligence Support, Special Security Studies, Foreign Disclosure Support, Program Protection Cybersecurity/Security Control Assessment Services, and Program Protection Engineering Services. The Program Security Support Services

encompass the management and control of controlled unclassified information (CUI), collateral/general service (GENSER) information, SAP information, North Atlantic Treaty Organization (NATO) information, Critical Nuclear Weapons Design Information (CNWDI) and Sensitive Compartmented Information (SCI). This is an Indefinite Delivery/Indefinite Quantity contract which sets forth the conditions and clauses under which future acquisitions between the parties shall be governed. This Task Order (TO) will be used as a means of providing Cybersecurity Support to the F-35 JPO.

3. TASK ORDER PERFORMANCE REQUIREMENTS

The Contractor shall furnish the necessary personnel, as captured in Section 9.0, to perform the following tasks as aligned with paragraphs 3.10 and 3.11 of the ID/IQ SOW:

3.1. Provide Project Management. The contractor shall provide project management under this TO, including but not limited to the following tasks:

3.1.1. Provide management and oversight of all activities performed by contractor personnel, including subcontractors, to ensure all F-35 program security support services satisfy the requirements identified in this SOW

3.1.2. Gather and provide all data for deliverables as detailed in Section 7.0

3.1.3. Provide management, direction, administration, quality assurance, and leadership of the execution of this TO

3.1.4. Organize, direct, and manage contract operation support functions, involving multiple, complex, and interrelated project tasks

3.1.5. Manage teams of contract support personnel at multiple locations

3.1.6. Maintain and manage the client interface at the senior levels of the client organization and serve as the primary interface and point of contact with Government program authorities and representatives on technical and program/project issues

3.1.7. Meet with Government and contractor personnel to formulate and review task plans and deliverable items

3.1.8. Ensure conformance with program task schedules and costs

3.1.9. Direct efforts of cross-competency team(s) to include contractors at multiple locations

3.1.10. Oversee contractor personnel program/project operations by developing procedures, planning and directing execution of the technical, programming, maintenance and administrative support effort and monitoring and reporting progress

3.2. Provide Program Protection Cybersecurity Services. The Contractor shall provide Cybersecurity Services throughout the cybersecurity lifecycle process for Information Systems (IS), Platform Information Technology (PIT), Information Technology (IT) Services, and IT products that are or will be assessed or assessed and authorized by Authorizing Officials (AOs) within the F-35 Enterprise. The contractor shall prepare materials for, and participate in, weekly staff meetings. The contractor shall perform all six steps of the RMF/JSIG processes as captured below, with a focus on Steps 4 and 5, Assessing Security Controls and Authorizing the System.

DRAFT

3.2.1. **Step 1: Categorize System**. The Contractor shall participate, as required, in the system categorization of each system and maintain the formal decision document as a part of the F-35 System's Security Assessment Package

3.2.2. **Step 2: Select Security Controls**. The Contractor shall provide assistance to the Information System Owner (ISO) in Security Control Traceability Matrix (SCTM) negotiations for formal tailoring of system security control requirements. The Contractor shall maintain the formal SCTM submission as part of the F-35 System's Security Assessment Package

3.2.3. **Step 3: Implement Security Controls**. The Contractor shall participate in Preliminary and Critical Design Reviews (PDR/CDR) to ensure proposed design and implementation of controls are in accordance with DoD cybersecurity standards and have not deviated from the tailored SCTM

3.2.4. **Step 4: Assess Security Controls**. The Contractor shall create a Security Assessment Report which shall encompass evaluation of all written artifacts within the formal Security Assessment Package submitted by the ISO, results of the Independent Validation and Verification (IV&V) test, and Security Assessment (SA) event

3.2.5. **Step 5: Authorize System.** The Contractor shall validate all required artifacts in the Information System Security Manager / Engineer (ISSM / ISSE) assembled Security Assessment Package are current and representative of the systems being presented for AO adjudication. The Contractor shall provide a formal written recommendation within the Security Assessment Report to the AO for review and final acceptance

3.2.6. **Step 6: Monitor Security Controls.** The Contractor shall evaluate Continuous Monitoring (ConMon) Plans and shall participate in Operational Assessments

DRAFT

3.3. Provide Security Control Assessor Services. The Contractor shall perform oversight of the development, implementation and evaluation of information system security program policy, with special emphasis placed upon integration of existing SAP network infrastructures. The Contractor shall perform analysis of network security, based upon the RMF Assessment and Authorization (A&A) process and advise customer on IT certification and accreditation issues.

3.3.1. Perform oversight of the development, implementation and evaluation of information system security program policy; special emphasis placed upon integration of existing SAP network infrastructures

3.3.2. Perform analysis of network security, based upon the RMF and Joint Special Access Program Implementation Guide (JSIG) authorization and assessment processes (A&A); advise customer on IT and A&A issues

3.3.3. Perform risk assessments and make recommendations to customers

3.3.4. Advise the AO, Delegated Authorizing Official (DAO), Office of Chief Information Officer (OCIO), and/or Program Security Officer (PSO) on assessment methodologies and processes

3.3.5. Evaluate certification documentation and provide written recommendations for accreditation to Government Program Managers (PMs)

3.3.6. Review system security to accommodate changes to policy or technology

3.3.7. Evaluate IT threats and vulnerabilities to determine whether additional safeguards

are needed

3.3.8. Advise the government concerning the impact levels for confidentiality, integrity, and availability for the information on a system

3.3.9. Facilitate ensuring certification for each information system

3.3.10. Develop, implement, provide guidance, and enforce Automated IS (AIS) security policies and procedures

3.3.11. Facilitate the necessary technical training for Information System Security Officers (ISSOs), network administrators, and other AIS personnel to carry out their duties

3.3.12. Develop, review, endorse, and recommend action by the DAO of system certification documentation

3.3.13. Facilitate ensuring procedures are in place for clearing, purging, declassifying, and releasing system memory, media, and output

3.3.14. Conduct certification tests that include verification that the features and assurances required for each protection level fare functional

3.3.15. Maintain a repository for all system certification/accreditation documentation and modifications

3.3.16. Coordinate AIS security inspections, tests, and reviews

3.3.17. Develop policies and procedures for responding to security incidents and for investigating and reporting security violations and incidents

3.3.18. Facilitate ensuring proper protection and/or corrective measures have been taken when an incident or vulnerability has been discovered within a system

3.3.19. Facilitate ensuring that data ownership and responsibilities are established for each AIS, to include accountability, access rights, and special handling requirements

3.3.20. Develop and implement an information security education, training, and awareness program, to include attending, monitoring, and presenting local AIS security training

3.3.21. Complete and document security testing and evaluations

3.3.22. Evaluate threats and vulnerabilities to ascertain whether additional safeguards are needed

3.3.23. Assess changes in the system, its environment, and operational needs that could affect the accreditation

3.3.24. Conduct periodic testing of the security posture of the AIS

3.3.25. Facilitate ensuring configuration management for security-relevant AIS software, hardware, and firmware are properly documented.

3.3.26. At the conclusion of each security assessment activity, prepare the final Security Assessment Report containing the results and findings from the assessment

3.3.27. Evaluate and monitor Plan of Action and Milestone (POA&M) activities to ensure proper and timely remediation actions are taken with respect to identified weaknesses and suspense dates for each IS based on findings and recommendations from the Security Assessment Report

3.3.28. Facilitate ensuring that system recovery processes are monitored to ensure that security features and procedures are properly restored

3.3.29. Facilitate ensuring all AIS security-related documentation is current and accessible to properly authorized individuals

3.3.30. Facilitate ensuring that system security requirements are addressed during all

DRAFT

phases of the system life cycle

3.3.31. Participate in self-inspections; identify security discrepancies and report security incidents

3.3.32. Coordinate all technical security issues outside of area of expertise or responsibility with Senior Systems Engineer (SSE)

3.3.33. Provide expert research and analysis in support of expanding programs and area of responsibility

3.3.34. Perform file transfers between local systems to storage devices

3.4. Provide Program Protection Cybersecurity (CS) Specialist Services. The contractor shall perform cybersecurity compliance assessments in alignment with Security with Staff Assistance Visits (SAVs) and Operational Assessment (OA) both CONUS and OCONUS. The contractor shall provide written accounts of each OA or SAV cybersecurity compliance assessment to event lead, and maintain knowledge and share site/files for lessons learned from each event. The contractor shall maintain and update Cybersecurity SAV and OA Checklists, database entries and required files for each event. The contractor shall schedule OA/SAV meetings and provide weekly updates to Enterprise Information System Security Manager (ISSM) and Government SAP Security Officer (GSSO). The contractor shall prepare materials for, and participate in, weekly staff meetings.

4. GENERAL INFORMATION

DRAFT

4.1. Period of Performance. The period of performance (PoP) consists of 12 months.

4.2. Place(s) of Performance. The primary place of performance for the this requirement is Arlington, VA.

4.2.1. The contractor may be required to support cybersecurity services, via travel, at Government sites including, but not limited to, the following as requested by the Government:

- Eglin AFB, FL
- Fort Worth, TX
- China Lake, CA
- Point Mugu, CA
- Wright-Patterson AFB, OH
- Orlando, FL
- OCONUS locations

4.3. Hours of Operations. The contractor shall provide the required services and staffing coverage during normal working hours. Core hours are 0900-1500, Monday through Friday (except on the legal holidays specified in paragraph 3.5.3). Some supported Government offices have flexibility to start as early as 0500/0530 and end as late as 1900, Monday through Friday.

4.4. Compressed Work Schedule (CWS). CWS is not permitted on this effort.

4.5. Extended Core Business Hours. Contractor Staff may be required to work beyond normal

core business hours. In the event that additional hours must be worked, prior approval must be obtained from the Contracting Officer Representative (COR).

4.6. Overtime. Refer to ID/IQ.

4.7. Telework. Telework is not permitted on this effort.

4.8. Meeting Support. In support of the tasking outlined in this TO, the contractor shall have the capability to support meetings at the TOP SECRET classification level at Government facilities in both CONUS and OCONUS locations.

4.9. IT Operating Environment. Refer to ID/IQ.

4.10. Transition/Mobilization. Refer to ID/IQ.

4.11. Management of Contractor Personnel. Refer to ID/IQ.

4.12. Installation Closure. Refer to ID/IQ.

4.13. Holidays. Refer to ID/IQ.

4.14. Information Technology. Refer to ID/IQ.

DRAFT

4.15. Section 508 Compliance. Refer to ID/IQ.

4.16. Government Furnished Property (GFP). Refer to ID/IQ.

5. SECURITY REQUIREMENTS

5.1. DD-254, Contract Security Classification Specification. The contractor shall comply with security requirements specified in the ID/IQ DD-254. Information or data that the contractor accesses shall be handled at the appropriate classification level, unclassified information shall be handled as "For Official Use Only". Distribution is authorized to the Requiring Office's Organization and supported Activity only. Other requests for deliverables under this contract shall be referred to the TPOC/COR of this contract for approval.

5.2. Personnel Clearance Requirements. All personnel on this TO must have at minimum a **Top Secret** Clearance at day one of TO Performance (PoP). Personnel may not have an interim clearance at time of contract award unless approved in advance by the Government. Key positions designated as Special Access Required (SAR) must have a final clearance and be eligible for access under the Special Access Program (SAP) Nomination Process prior to on-boarding at the F-35 Joint Program Office or associated sites. Key positions designated as Sensitive Compartmented Information (SCI) must have a current TS SCI clearance at the time of contract award. Non-key positions with SAR and SCI requirements may possess a TS clearance and be adjudicated for SAR and SCI while performing duties in accordance with this SOW. The contractor is responsible for ensuring that all personnel receive the requisite investigation and are favorably adjudicated in accordance with DoDM 5220.22, National Industrial Security Program Operating Manual

(NISPOM). If a contractor fails to be favorably adjudicated for SAR or SCI while performing under this contract, that contractor cannot perform and must be replaced with another candidate.

5.3. Citizenship Requirements: Refer to ID/IQ.

5.4. Command Access Cards (CAC) / Local Badges: Refer to ID/IQ.

5.5. SAAR-N: Refer to ID/IQ.

5.6. Information Security. Refer to ID/IQ.

5.7. Anti-Terrorism Force Protection and Emergency Management: Refer to ID/IQ.

6. TRAVEL AND OTHER DIRECT COSTS

6.1. Travel. Travel shall be allowable only when it is essential to the performance of the tasks detailed in this TO. Refer to ID/IQ.

6.2. Other Direct Costs (ODC). Refer to ID/IQ.

7. CONTRACT DELIVERABLES AND APPLICABLE DOCUEMNTS

DRAFT

7.1. Contract Status Reporting: The following contract deliverables shall be provided in response to this TO:

Table 7.1. Deliverables

Name	No. of Copies	SOW Reference	Due
Management and Staffing Plan	1	3.1, 7.1.1	Per ID/IQ
Quality Control Plan	1	3.1, 7.1.2	No later than 30 calendar days after award and as needed post-award to capture any Contractor requested changes to the approved plan for further approval
Kick-Off Meeting & Slides	1	3.1, 7.1.3	No later than 10 business days of TO award notification for Government review.
Monthly Status Report	1	3.1, 7.1.4	Per ID/IQ
Monthly Expenditure Report	1	3.1, 7.1.5	Per ID/IQ
Weekly Activity Reports (WAR)	1	3.1, 7.1.6	Per ID/IQ
Hiring Status Report	1	3.1, 7.1.7	Per ID/IQ

Name	No. of Copies	SOW Reference	Due
Transition-In Plan	1	3.1, 7.1.8	Per ID/IQ
Travel Authorization Request	1	3.1, 7.1.9	No later than 10 calendar days before the first travel date (CONUS) or 15 calendar days (OCONUS) for COR approval
Trip Report	1	3.1, 7.1.10	No later than 5 business days after the last day of travel
Meeting Minutes	1	3.1, 7.1.11	No later than 3 business days of the meeting conclusion
Problem Notification	1	3.1, 7.1.12	Per ID/IQ
Transition-Out Plan	1	3.1, 7.1.13	Per ID/IQ
Staff Meeting Agenda and Slides	1	3.2, 3.3, 7.1.14	Weekly; no later than 2 business days prior to the meeting
Training Syllabi and Materials	1	3.3.20, 7.1.15	No later than 10 business days before training is conducted

Notes:

1. Submit one copy each electronically in Adobe (PDF) or as a Microsoft Office Suite product to the CO, COR, PM, CS, and acquisition analyst. If copies exceed five (5) megabytes of data, send through AMRDEC SAFE (Safe Access File Exchange) at https://safe.amrdec.army.mil/SAFE/. Submit classified reports only to the GCC point(s) of contact via SIPRNet or JWICS, as appropriate.
2. All deliverables shall be submitted by the established due date. If the due date falls on a weekend or holiday, the deliverable shall be submitted on the next business day. Unless specified otherwise, calendar days will be used. If the submittal is rejected by the Government the Contractor shall resubmit within 15 days.
3. The deliverables listed are not all inclusive and do not relieve the Contractor of responsibility for providing deliverables as required elsewhere in the SOW and the main ID/IQ if applicable.
4. All deliverables must meet professional standards and meet the requirements set forth in contractual documentation. The Contractor shall be responsible for delivering all end items specified unless otherwise directed by the COR/TPOC. Contractor format is acceptable for this effort, unless otherwise stated, as long as all required analysis is completed and provided to the Government.

DRAFT

7.1.1. Management and Staffing Plan. As required per the ID/IQ. Contractor shall include data pertinent to this TO as part of the ID/IQ Management TO deliverable.

7.1.2. Quality Control Plan. The Contractor shall provide a Quality Control Plan (QCP) in accordance with the timelines captured in Table 7.1 that aligns with the ID/IQ Management TO approved plan. The Contractor shall establish and maintain a QCP that ensures services are

performed in accordance with this requirement (see Section 8), applicable laws and regulations, and best commercial practices.

7.1.3. Kick-Off Meeting and Slides. The Contractor shall attend the contract Kick-Off Meeting and submit Kick-Off slides in accordance with the timelines captured in Table 7.1. The Contractors slides shall capture (at a minimum) the following data:

- Introduction of key personnel
- Roles and responsibilities
- Communication plan and lines of communication overview
- Schedule showing major tasks and milestones with start/completion dates
- Security requirements/issues/facility access procedures (if applicable)
- Sensitivity and protection of information (if applicable)
- Government Furnished Information (GFI) and Equipment (GFE) (if applicable)
- Initial deliverables (if applicable)
- Current status of transition-in plan (as proposed and approved by the Government)
- Any other information the contractor deems pertinent

7.1.4. Monthly Status Report. As required per the ID/IQ. Contractor shall include data pertinent to this TO as part of the ID/IQ Management TO deliverable.

7.1.5. Monthly Expenditure Report. As required per the ID/IQ. Contractor shall include data pertinent to this TO as part of the ID/IQ Management TO deliverable.

DRAFT

7.1.6. Weekly Activity Report. As required per the ID/IQ. Contractor shall include data pertinent to this TO as part of the ID/IQ Management TO deliverable.

7.1.7. Hiring Status Report. As required per the ID/IQ. Contractor shall include data pertinent to this TO as part of the ID/IQ Management TO deliverable.

7.1.8. Transition-In Plan. As required per the ID/IQ. Contractor shall include data pertinent to this TO as part of the ID/IQ Management TO deliverable.

7.1.9. Travel Authorization Request. The Contractor shall submit a travel authorization request in accordance with the timelines capture in Table 7.1 that includes (at a minimum) the following data for COR approval prior to incurring any costs (the Government may provide a travel authorization request template for use post-award):

- Contract number
- Name of traveler
- Dates
- Origin and destination
- Owning IPT being supported
- Organization to be visited
- Purpose of travel
- Estimated airfare

- Estimated lodging within regulatory limits
- Estimated per diem
- Estimate ground transportation
- POV use
- Miscellaneous costs
- Justification as to why teleconferencing or video teleconferencing cannot be used
- Employee signature
- IPT signature

7.1.10. Trip Report. The Contractor shall submit a trip report in accordance with the timelines capture in Table 7.1 that includes (at a minimum) the following data:

- Personnel who traveled
- Dates of travel
- Destination(s)
- Purpose of trip
- Cost of the trip
- Approval authority
- Summary of events, action items, and deliverables

7.1.11. Meeting Minutes. The Contractor shall submit meeting minutes in accordance with the timelines capture in Table 7.1 that capture (as a minimum) the following data:

DRAFT

- Meeting attendees and their contact information
- Meeting date
- Meeting location
- Purpose of meeting
- Summary of events

7.1.12. Problem Notification. As required per the ID/IQ. Contractor shall include data pertinent to this TO as part of the ID/IQ Management TO deliverable.

7.1.13. Transition-Out Plan. As required per the ID/IQ. Contractor shall include data pertinent to this TO as part of the ID/IQ Management TO deliverable.

7.1.14. Staff Meeting Agenda and Slides. Contractor shall draft an agenda and slides in accordance with the timelines capture in Table 7.1 that capture (as a minimum) the following data:

- Meeting date, location and purpose
- Team roles and responsibilities
- Current status of activities being performed under the TO
- Any issues requiring discussion

7.1.15. Training Syllabi and Materials. The Contractor shall submit training syllabi and materials in accordance with the timelines capture in Table 7.1 that capture (as a minimum) the following data:

- Instructor(s) information and contact
- Course description and purpose
- Learning goals and expected outcomes
- Any applicable resources (e.g. associated DoD policy or regulations)
- Course policies and expectations
- Materials to be used in the course (e.g. PowerPoint slides)

7.2. Applicable Documents. The Contractor shall comply with regulations or publications captured in Attachment 1 at the ID/IQ level. This list is not all-inclusive; additional policies may be identified as the program matures. The Contractor is responsible for ensuring that tasks executed on this TO are in accordance with regulations, documents and policies applicable to this particular TO.

7.3. Enterprise-Wide Contractor Manpower Reporting Application (ECMRA): Refer to ID/IQ

8. QUALITY

8.1. Contractor Quality Control. Refer to ID/IQ

8.2. Service Summary. The Service summary captured in Attachment 3 will serve as and/or be used to develop the Government Surveillance Activity Checklist (SAC) to audit performance in accordance with this TO. The SAC will identify the audit methods and procedures the Government will use to evaluate Contractor performance. The Government will provide a copy of the SAC and any updates to the Contractor as applicable.

DRAFT

9. KEY PERSONNEL, LABOR CATEGORIES, AND QUALIFICATIONS

9.1. Key Personnel. The following positions are considered key personnel in support of this requirement and are indicated in bold font in Section 9.2:

- **Project Manager**
- **Security Control Assessor, Team Lead**

9.2. Labor Categories and Full-Time Equivalents (FTE). The contractor shall be responsible for employing personnel with experience level and education as outlined in Section 9.3 and 9.4 that pertain to the labor categories specified. In addition to possessing clearance, certification (cert) and specific requirements for each labor category by level, personnel employed for each labor category will also possess the ability to perform SOW tasks that correspond with the labor category and knowledge of documents/regulations that align with the specific labor category. An FTE equals 1920 hours. The Standard Occupational Codes (SOC) are in accordance with the Bureau of Labor Statistics 2018 Standard Occupational Classification System.

Labor Category	SOC	FTE	Duty Location	Level	Clear-ance	Cert	Specific Requirements

Project Manager (KEY)	**11-1021**	**1**	**Contr-actor**	**Senior**	**Top Secret SCI/ SAR**	**N/A**	• **Ability to fulfill tasks at SOW 3.1 and oversee contractor personnel associated with all other tasks on this TO** • **3 years cybersecurity-related experience** • **Demonstrated experience with flag-officer level briefings and senior-level interface** • **Demonstrated knowledge of DoD 5000 series (DoD acquisition)**
Security Control Assessor (Team Lead, KEY)	**15-1212**	**1**	**Gov't, Arling-ton VA**	**Senior**	**Top Secret SCI/ SAR**	**IAT/ IAM Level III at date of hire**	• **Ability to fulfill tasks at SOW 3.2 and 3.3** • **Specialized experience with flag-officer level briefings and senior-level interface** • **Demonstrated knowledge of aircraft programs and systems** • **5 years team leadership or management experience**
Security Control Assessor	15-1212	10	Gov't, Arlington VA	Senior	Top Secret SCI/ SAR	IAT/ IAM Level III within one year of hire	• Ability to fulfill tasks at SOW 3.2 and 3.3 • Demonstrated knowledge of aircraft programs and systems
Security Control Assessor	15-1212	3	Gov't, Arlington VA	Mid	Top Secret SCI/ SAR	IAT/ IAM Level III within one year of hire	• Ability to fulfill tasks at SOW 3.2 and 3.3 • Demonstrated knowledge of aircraft programs and systems

DRAFT

Total FTE: 15 (28,800 hours)
IAT = Information Assurance Technician
IAM = Information Assurance Manager

9.2.1.1. Minimum Education. Refer to Paragraph 9.3. For the Project Manager, the

required degree shall be in Management, Administration, Business, IT, Cybersecurity, Science or related discipline. For Security Control Assessor, the required degree shall be in Business, IT, Cybersecurity or related discipline. Refer to Paragraph 9.4 for allowable substitution for lack of the required degree level.

9.2.1.2. Minimum Experience. The contractor shall be responsible for employing personnel with at least the minimum experience described in Paragraph 9.3

9.3. Experience Level Definition. The contractor shall be responsible for employing personnel with the qualifications and skills required to successfully accomplish the tasking outlined in the SOW. The experience required in this TO is different from the standard at the ID/IQ level. The professional labor category experience and education requirements corresponding to the three levels specified for this TO (Junior, Mid and Senior) are as follows:

- JUNIOR: N/A for this TO

- MID: A Mid level person within a labor category for this TO has five or more years of experience performing work related to the labor category functional description and a BA/BS degree or a qualifying substitution as identified in Section 9.4. Four years must pertain specifically to the labor category (e.g. Security Control Assessor must have at least four years performing duties specific to Security Control Assessment and Cybersecurity) while the remaining experience must pertain to a related labor category (e.g. any other security discipline). A Mid level person typically performs all functional duties independently.

DRAFT

- SENIOR: A Senior level person within a labor category for this TO has at least 10 years of experience performing work related to the labor category functional description and a MA/MS degree, or a qualifying substitution as identified in Section 9.4. Six years must pertain specifically to the labor category (e.g. Security Control Assessor must have at least six years performing duties specific to Security Control Assessment and Cybersecurity) while the remaining experience must pertain to a related labor category (e.g. any other security discipline). A Senior level person typically works on high-visibility or mission critical aspects of a given program and performs all functional duties independently. A Senior level person may oversee the efforts of less senior staff and/or be responsible for the efforts of all staff assigned to a specific job.

9.4. Education Level Substitution. The following qualification substitution chart details the combination of education/experience that can be used as a substitute for the degree requirements applicable to the above experience/education levels:

Bachelor's Degree	6 years of additional work experience related to the labor category functional description may be substituted for a Bachelor's Degree
	Associate's Degree plus 4 years of additional work experience related to the labor category functional description may be substituted for a Bachelor's Degree.

Master's Degree	Bachelor's Degree plus 4 years additional work experience related to the labor category functional description may be substituted for a Master's Degree.

- Note: All degrees shall be obtained from an accredited college or university as recognized by the U.S. Department of Education.

10. ATTACHMENTS

- Attachment 1 – Applicable Documents – Refer to ID/IQ
- Attachment 2 – Level of Effort – No Separate Attachment - Refer to Section 9.2
- Attachment 3 – Task Order Service Summary
- Attachment 4 – Purchase Request Form - Refer to ID/IQ
- Attachment 5 – Travel Authorization Request Form - Refer to ID/IQ

DRAFT

Attachment 2

Task Order Services Summary

Performance Objective	Performance Standard	Performance Threshold
Provide qualified personnel for task order performance	Qualified personnel are in place for task order performance	Performance is acceptable when qualified personnel are in place for task order performance no later than (NLT) 45 calendar days following task order award unless authorized by the Contracting Officer
Retain personnel with specified qualifications	Effectively replaces / substitutes personnel	Performance is acceptable when task order vacancies do not exceed 30 calendar days
Review unclassified and/or classified artifacts submitted for Assessment and Authorization (A&A) in accordance with National and Department of defense policies	Coordinate daily review of unclassified and/or classified artifacts proposed for A&A	Performance is acceptable when comments for resolution are submitted within 10 business days from receipt
Provide cybersecurity expertise to perform OCONUS assessment support	Provide status reports of cyber activities to key personnel Government lead(s)	Performance is acceptable when requested information is received within 5 business days of request from Government lead(s)
Provide A&A recommendation	Review all completed artifacts submitted for ongoing authorization including Government lead(s) input	Performance is acceptable when Security Control Assessor (SCA) recommendation is received 5 business days after all updated A&A documentation is received for ongoing authorization

DRAFT