Defense Intelligence Agency (DIA)
Chief Information Officer’s (CIO) Office

RISK MANAGEMENT FRAMEWORK

MULTI-LEVEL SECURITY (MLS) SYSTEMS SUPPORT SERVICES

CYBER AND SECURITY DIVISION

STATEMENT OF WORK (SOW)

October 21, 2024

Table of Contents

List of Tables

Statement of Work

RISK MANAGEMENT FRAMEWORK

MULTI-LEVEL SECURITY (MLS) SYSTEMS SUPPORT SERVICE

Unclassified

October 21, 2024

GENERAL INFORMATION

This is a non-personal services contract to provide Security Control Assessor (SCA) and Information System Security Manager (ISSM) RMF support to exclusively assess Multi-Level Security (MLS) IT systems. The Government shall not exercise any supervision or control over the service providers performing the services herein. Such service providers shall be accountable solely to the Contractor who, in turn is responsible to the Government.

1 Title of Project

Risk Management Framework Multi-Level Security Systems Support Services

2 Background

The Defense Intelligence Agency's (DIA) mission is to provide all-source defense intelligence to prevent strategic surprise and deliver a decision advantage to war fighters, defense planners, and policymakers. Our customers include warfighters, Office of the Director of National Intelligence (ODNI) and interagency partners that defend America's national security interests. The DIA Chief Information Officer (CIO) Cyber Security Division (CIO4) provides cyber security support within the Department of Defense, (DoD), Intelligence Information System, (DoDIIS), community, the Joint Worldwide Intelligence Communications Systems, (JWICS), community, and the DoD Sensitive Compartmented Information (SCI) Community.

The DIA Director and CIO are focused on enhancing and expanding cyber security support and services to facilitate the overall DIA mission, support DIA personnel, and DIA customers, including DIA's transition to Intelligence Community (IC) Information Technology Enterprise (ITE). This contract vehicle provides supported customers with comprehensive Information Technology (IT) cyber security support services specific to Multi-Level Security (MLS) systems. Detailed mission requirements are defined in Section 5.

3 Objectives

The Defense Intelligence Agency (DIA) Chief Information Office (CIO) Cyber & Security (C&S) Division’s primary objective is to acquire the Subject Matter Expertise (SME) with the requisite cybersecurity Knowledge, Skills, and Abilities (KSAs) to assist in the mission of the C&S Division’s Risk Management Framework (RMF) support with an exclusive focus on assessing MLS systems. These RMF assessments will be performed on behalf of Authorizing Officials (AO) and the Chief Information Security Officer (CISO).

4 Scope

This Cyber Services solicitation is intended to address the RMF mission needs of the CIO specific to MLS systems. The RMF is a structured process used by the Department of Defense (DoD) and other federal agencies to ensure that information systems, including MLS systems, operate securely and meet regulatory requirements. The RMF process includes the following key steps:

- Categorize the Information System:
  - Identify the information types processed by the MLS system
  - Determine the potential impact on the organization should the information be compromised.
- Select Security Controls:
  - Select appropriate security controls from NIST SP 800-53 (Security and Privacy Controls for Information Systems and Organizations) that address the risks identified during categorization.
  - Tailor the controls to the specific requirements of MLS systems, ensuring they cover data separation, access control, and auditing.
- Implement Security Controls:
  - Implement the selected security controls within the MLS system.
  - Ensure that the implementation aligns with the system's architecture and operational environment.
- Assess Security Controls:
  - Conduct an assessment to verify that the security controls are implemented correctly and are effective in their operational environment.
  - Use assessment methods such as testing, inspection, and interviews.
- Authorize Information System:
  - Prepare an authorization package that includes the security plan, security assessment report, and Plan of Action and Milestones (POA&M).
  - Obtain an Authority to Operate (ATO) from the designated official, confirming that the MLS system meets the required security standards.
- Monitor Security Controls:
  - Continuously monitor the MLS system to ensure that security controls remain effective.
  - Conduct periodic assessments and update the security plan as necessary.

The services and capabilities supported by the team will provide responsive, secure, and timely solutions to participating organizations that require the current and future cyber security services, as outlined in the Requirements Section 5 of this document.

.

5 Requirements

5.0 DIA Risk Management Framework (RMF)

5.1 SCA and ISSM personnel are required to have the requisite RMF knowledge, skills, and background as it applies to MLS systems. They must be capable of utilizing numerous cybersecurity-automated tools in areas such as vulnerability management, host-based security evaluation, dynamic and static application security testing, and container scanning. SCAs and ISSMs must also be familiar with both IC and DOD cybersecurity Directives, Instructions, Technical Implementation Guides, cybersecurity best practices, and other applicable guidance. Additional requirements are listed in Table 2 of this document.

5.2 SCAs and ISSMs will utilize manual and automated capabilities to evaluate the cybersecurity hygiene and associated risk to mission of DIA Information Technology Enterprise infrastructure and applications for Steps 1-6 of the RMF. SCAs and ISSMs will use various technical tools to assess target systems capabilities, deficiencies, and vulnerabilities; review technical and administrative documentation; conduct discussions and interviews with responsible system personnel; analyze and assess various data points to identify the risk associated with an assessed system; and provide written documentation and assessment for each assigned system In Accordance with (IAW) the RMF. SCA's focus on RMF steps 0-5, while ISSM's focus on Step 6 Continuous Monitoring (CONMON) activities.

5.3 SCAs will validate the Program's inputs into the RMF system of record for completeness and proper application. The SCA will also verify the program submissions of RMF Body of Evidence (BoE) (e.g., System Security Plan (SSP), Security Controls Traceability Matrix (SCTM), etc.).

5.4 ISSMs will verify Program Managers (PMs) and Information System Security Officers, (ISSOs), maintain and update the infrastructure and systems portions of the RMF BoE once their capability moves to RMF Step 6/CONMON.

5.5 The Contractor will conduct quality assurance oversight to ensure assessments follow DIA RMF processes and Standard Operating Procedures, (SOPs) and that assessments are comprehensive and complete based on the technologies in use by each capability.

5.6 Specific SCA & ISSM duty locations include but are not limited to Offutt Air Force Base (AFB), Nebraska.

Table 1: RMF Deliverables

Work Product Name	Description	Frequency	Distribution	Format
RMF Executive Dashboard	Comprehensive dashboard/visualizations of RMF Step 1-6 data	Within 30 days of award and daily thereafter	Electronically	DIA Visualization Tools
Executive Reporting	Executive-level reporting of various RMF Step 1-6 activities	As required	Electronically	IAW DIA policy and staffing package templates
Security Assessment Report (SAR) with Plan of Action & Milestones (POA&M)	Report detailing findings of security assessment activity	Within 10 days of assessment completion	Electronically	DIA RMF System of Record
RMF Integrated Master Schedule	Master schedule of all upcoming RMF Assessments	Weekly	Electronically	Dashboard

6 Deliverables

6.1. Cyber Services Call Order Deliverables will adhere to the guidance outlined in this Statement of Work (SOW).

6.2. The Contractor shall submit deliverables reports through the Government approved site for review by the appropriate Government personnel. The COR/ACOR shall conduct a review of the contract deliverables for completeness, correctness, and compliance with call order requirements. The Government shall provide written notice to the Contractor of deficiencies or necessary corrections to deliverables within 30 calendar days of receipt of any one deliverable. This notice shall state the action the Government requires of the Contractor in accordance with this contract.

6.3. The Contractor shall submit a Contract Activity Report (CAR) for each contract month to the COR. The report shall be submitted by the tenth calendar day following the close of each calendar month. At the direction of the COR, the CAR may be divided into call order services or geographic coverage areas (e.g., enterprise, regional, or sites) for better visibility and easier understanding. The CAR should be structured to show complete accounting from Contract Line-Item Number, (CLIN), Sub Contracting Line Number (SLIN), Project ID or Application Name, Activity Code, Labor Category and Resource Name. Each CLIN/SLIN will be part of the line of accounting; Project ID (Application Name). Each Activity Code will be managed at the Contractor level and reported to the Government for Internal Use Software Auditing Requirements.

6.4. The Contractor shall deliver a monthly status report that contains the monthly costs per functional area; report shall also contain staffing status to include all vacancies and the number of days the positions have been vacant, deliverables, a summary of key activities accomplished per functional area, and any significant issues, problems, and resolution.

6.5. The Contractor shall deliver new technology and/or capabilities for government consideration at the same time the Contractor submits QBR slides in the form of a White Paper (format to be determined by the Contractor) and shall not exceed 10 pages in length and marked non-proprietary. Submission of an Innovation Report is mandatory. The Contractor shall submit to the Government PM at the same time as the QBR delivery, an electronic copy of the Innovation Report. The Government will respond within 45 calendar days.

6.6. All deliverables shall be IAW applicable security classification guides and provided as detailed in the Call Order's formal Contract Data Requirements List, (CDRLs) DD Form 1423) as well as those referenced in the Requirements Section 5 within this SOW.

6.7. The Contractor shall submit a Call Order Closeout and Transition Report at the end of the call order base year or option year if an option year is not awarded or as directed by the Contracting Officer (CO). The Contractor shall provide a Closeout Report 90 days before the end of the period of performance. This plan shall be called the (Program Name) Contract Task-Order Closeout and Transition Report.

6.8. The Closeout Report shall include all up-to-date critical information needed to sustain operations after this call order expires. The close out report shall include all Government owned property, inventories, Government owned software, existing data center drawings, work center standard operating procedures, existing network drawings, work center SOPs, etc. The closeout report shall be classified IAW the secure classification guide and submitted via the network appropriate for that classification. As applicable, the report shall include at a minimum:

6.8.1. Current access codes, and combinations on all Government owned IT equipment, tools, and software on all networks.

6.8.2. Source copies privileged user administration or scripts developed with funding of this call order (e.g., SMS, SCCM, and OPSWARE scripts and templates).

6.8.3. Current backup report with backup locations, procedures.

6.8.4. Hardware and software inventories (to include definitive software libraries) and discrepancy reports.

6.8.5. Hardware and software maintenance and licensing inventories and discrepancy reports.

6.8.6. Current property inventories of any warehouses, deports, spares.

6.8.7. Outbound Communication Security (COMSEC) inventories if the Contractor is responsible for a COMSEC account or is a hand receipt holder for COMSEC items. The Contractor shall proper accounting of all DoD CCI material. Note: COMSEC and property inventories will be validated via a Government-Contractor walkthrough and mutual agreement of the inventories.

6.8.8. All SOPs, instruction manuals, training materials, etc.,developed with funding of call order.

6.8.9. A complete listing of all open Call orders / Contracts indicating the status completionand any performance issues associated with them.

6.8.10. The Contractor shall work through/walk-through all the property and library inventorieswith Government personnel and resolve discrepancies. Once completed to the Government's satisfaction, the Government will approve the current inventories and the Closeout Report.

6.6.1.1 Upon notification of expiration of this Call order, the Contractor shall be required to work with any incoming Contractors and/or Military/Government personnel for a seamless and end-user transparent transition of operations.

6.6.1.2 Upon expiration of this Call order, the Contractor shall provide to the Government an after-action report that provides the status of the deliverables; clearance report of GFE/GFP, to include software licenses; names of personnel who worked on the call order and written confirmation that they have been read off IAW DoD5105.21-M-1.

6.6.1.3 Final invoices shall be submitted no later than 90 days after the end of the performance period.

7 Government Furnished Property, Material, Equipment, or Information

The Government will provide the Contractor with the following property at theirassigned work locations:

7.1. Access to Non-Secure Internet Protocol Network (NIPRNet), Secure Internet Protocol Network (SIPRNet), and the JWICS networks and systems access, including printers and digital senders.

7.2. Contractor use of DoD Computers is FOR OFFICIAL USE ONLY and its use is subject to monitoring at any time. All data generated or collected on DIA computers becomes the property of the U.S. Government and its release, downloading or transmittalis subject to Government approval. Contractor personnel are not authorized to introduce computer hardware, software, or data storage media, physically or electronically into a government facility, computer, or network device without the prior written approval and notification of the appropriate Government authorities. Downloading and transmitting of information within DIA ‘s custody is prohibited except as provided for in the terms of this contract.

8 Travel and Place of Performance

8.1 Travel Costs

Travel costs will be allowed to the extent that they are reasonable, allocable and allowable under Federal Acquisition Regulation (FAR) 31.205-46. Travel by air will be reimbursed at the actual cost incurred and will not exceed the lowest customary standard coachor equivalent fare offered during normal business hours.

As prescribed in FAR 31.205-46(a), travel costs for lodging, meals, and incidental expenses are limited to the maximum per diem rates in effect at the time of travel set forth in the Federal Travel Regulation (FTR); the Joint Travel Regulations, Volume 2, DoD Civilian Personnel, Appendix A; or the Standardized Regulations (Government Civilians, Foreign

Areas), Section 925, “Maximum Travel Per Diem Allowances for Foreign Areas”. IAW FAR 52.216-7, the Contractor may submit to the COR, in such form and reasonable detail as the representative may require an invoice or voucher supported by a statement of the claimed allowable cost for performing this contract.

The per diem allowance will not be allowed when the period of official travel is ten (10) hours or less during the same calendar day. Travel by privately owned vehicle will be reimbursed at the current GSA approved mileage rate. Current travel policy and per diem rates may be obtained atthe following Internet site: http://www.defensetravel.dod.mil/site/perdiem.cfm

8.2 Travel Reimbursement

Only those travel costs incurred by the Contractor for contracted personnel assigned and working under this SOW shall be allowed for the following expenses: Contractor employee airline tickets, per diem, and miscellaneous incidental expenses. Such transportation costs incurred will be reimbursed at actual costs in accordance with Joint Travel Regulations. Per Diem is not authorized within the designated AOR unless prior written approval is granted by the COR. Per Diem is authorized during pre-deployment training. Only per diem and travel costs shall be reimbursed; incidentals and miscellaneous expenses will not be reimbursed. Regardless of amount, all travel costs shall be documented via copies of the original travel receipts, to be provided with the invoice requesting payment, providing the following information: Traveler’s name, date, and place (city, town, or other similar designation) of the expenses, purpose of the trip, and expense incurred. Local travel, within 50 miles of duty location will not be reimbursed.

8.3 Place of Performance

The place of performance shall vary between the Contractor’s facility and the government facility. The place of performance will be determined by the work assignment. Accordingly, reimbursable travel and per diem for the Contractor’s employees performing work on a regular basis at the designated place of performance is not authorized.

8.4 Work Locations Inside the NCR

Contractor employees shall perform work at government work locations in the Washington, D.C. National Capital Region (NCR). The NCR is defined as falling within the area contained by thelegal borders of: The District of Columbia, Arlington, Fairfax, Loudon, Prince William, and Stafford counties located in the Commonwealth of Virginia (including incorporated cities).

8.5 Work Locations Outside the NCR

Contractor employees may be required to perform work at remote government work locations outside the NCR and Outside the Continental United States, (OCONUS) locations including, but not limited to:

- Offutt AFB, NE

9 Duty Hours

9.1 Duty Hours Continental United States (CONUS)

The core work hours of operations for all personnel assigned within the NCR are Monday through Friday from 0900 hrs. to1430 hrs. local time. On average, a 40-hour work week is anticipated for Contractor personnel however, the week may be extended to meet operational needs with prior written COR approval. The PM shall obtain COR written approval prior to any Extended Work Week, (EWW), performance exceeding 40 hours per week to ensure funding availability.

Contractor personnel assigned to Combatant Command (COCOMs) and other national agencies outside of the NCR shall adhere to the supported headquarters core hours at their assigned location.

9.2 Duty Hours (OCONUS)

Contractor personnel supporting OCONUS contingency operations may work twelve (12) hours per day, seven (7) days per week, and eighty-four (84) hours per week from Monday through Sunday. In non-contingency locations, the Contractor may work on average eight (8)hours per day, five (5) days per week, and forty (40) hours per week from Monday through Friday. Contractor personnel shall not exceed the designated work weeks without the COR’s prior written approval. Any variations to the hours will be determined at the call order level.

9.3 Holidays and Government Closings

Contracting personnel requiring access to government-controlled facilities outside of core office hours will be considered on a case-by-case basis. Government approved implementation or sustainment activities to be performed outside core duty hours, weekends, or federal holidays, and will require authorization from the COR. Specific procedures for obtaining this approval will be provided by the Government.

Table 2 Labor Categories

Labor Category	Category Description	Education Requirements	Experience Requirements
Mid-level Cyber Control Assessor Special Systems Engineer II	• Analyzes and defines security requirements for applications and systems across all technology layers. • Gathers and organizes technical information about an organization's mission goals and needs, existing security products, and ongoing programs in cybersecurity. • Performs assessment and risk analyses of systems and applications during all phases of the system development life cycle. • Participate, and sometimes lead, in the planning, execution and reporting of security audits and network vulnerability assessments with minimal supervision. • Perform interviews, examinations, and testing of security controls. • Assist in preparation of assessment deliverables – Security Control Assessment Report, Security Risk Assessments, etc. • Plan, execute and report on information technology, privacy, and operational reviews to identify mission, privacy, security, compliance, information technology and regulatory risks.	Bachelor's degree in computer science or a related technicaldiscipline.	8 years of experience or the equivalent combination of education, professional training, or work experience. Candidates must possess DoD 8570 IAT III level certification.
Senior Cyber Control Assessor	• Analyzes and defines security requirements for applications and systems across all technology layers. • Gathers and organizes technical information about an organization's mission goals and needs, existing security products, and ongoing programs in cybersecurity. • Performs assessment and risk analyses of systems and applications during all phases of the system development life cycle. • Act as Cybersecurity Consultant.	Bachelor's degree in computer science or a related technicaldiscipline.	12 years of experience or the equivalent combination of education, professional training, or workexperience. Candidates must possess DoD 8570 IAT III level certification.

Labor Category	Category Description	Education Requirements	Experience Requirements
	• Lead in the planning, execution and reporting of security audits and network vulnerability assessments with minimal supervision. • Perform interviews, examinations, and testing of security controls. • Assist in preparation of assessment deliverables – Security Control Assessment Report, Security Risk Assessments, etc. • Plan, execute and report on information technology, privacy, and operational reviews to identify mission, privacy, security, compliance, information technology and regulatory risks.		
Senior Principal Cyber Engineer Architect III	• Leads, plans, schedules, and controls complex projects and activities with customers, support groups, and vendors on concurrent projects. • Assists in the planning and engineering of the organization's cloud computing infrastructure and applications. Familiar with standard concepts, practices, and procedures of cloud technology, including Software as Service (SaaS), Platform as Service (PaaS), or Infrastructure as a Service (IaaS). Must have experience with various cloud platforms such as AWS, Azure and Google Cloud.	Bachelor's degree in computer science or a related technicaldiscipline.	12 years of experience or the equivalent combination of education, professional training, or workexperience. Candidates must possess DoD 8570 IAT III level certification.

Labor Category	Category Description	Education Requirements	Experience Requirements
	• Develops policies and procedures to ensure in the Cloud IT environment information systems reliability and accessibility and to prevent and defend against unauthorized access to systems, networks, and data. Evaluates current Cloud system performance, cost, and compatibility attributes in comparison to commercial off-the-shelf software and/or development applications and makes recommendations for enhancement, redesign, and Cloud migration.		

10 Security Requirements

The DIA has determined that performance of this contract requires that the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor), requires access to sensitive DIA information, the Contractor shall have a facility clearance, and that the Contractor will adhere to the following:

See the DD254 and the Security Continuation Pages (SCP) for DIA Security Requirements.

11 Information Security

All persons performing work under this contract shall protect and safeguard information in accordance with DoD, (as applicable) and DIA directives, instructions, and procedures. These same persons shall immediately report any deviation or violation of this guidance, or any unusual or suspicious activity to the DIA Security Office. These same persons will provide assistance and full cooperation in any subsequent investigations or inquiries conducted by DIA or other governmental agencies.

12 Non-Disclosure Requirements

All the Contractor’s personnel shall sign, prior to beginning performance, a Non-Disclosure Agreement (NDA) IAW DFARS 227.7103-7 and/or a DSS NDA. The Contractor is bound by all NDAs signed by its employees. In the event the Contractor’s employee violates any of the terms of the NDA, the Contractor will be considered in breach of contract. This could result in a termination for default.