Request for Information (RFI) – Risk Management and Internal Control (RMIC) Support Services

THIS IS A SOURCES SOUGHT NOTICE, REQUEST FOR INFORMATION (RFI). This is not a Request for Proposal (RFP) or Request for Quote (RFQ). This request for capability information does not constitute an RFP or RFQ and does not commit the Government to contract for any supply or service, whatsoever. Further, the Virginia Contracting Activity (VaCA) is not at this time seeking proposals or quotes and will not accept unsolicited proposals or quotations. Submission of any information in response to this market survey is purely voluntary.

However, responses received will assist the Government if solicitation is issued in the future. The government assumes no financial responsibility for any costs incurred associated with this request for capability information. Not responding to this sources sought does not preclude participation in any future RFP or RFQ, if any is issued. Potential offerors are responsible for monitoring government websites such as GSA or SAM for any potential opportunities. Responses do not guarantee award nor exclude/include your company in any potential acquisition process. No feedback or evaluations will be provided to companies regarding their submissions.

This RFI is being used as a Market Research tool for informational purposes and for preliminary planning purposes to identify potential sources that possess the required experience and expertise to provide the required support. Small and large businesses are encouraged to respond.

1. INTRODUCTION:

The Virginia Contracting Activity (VaCA) invites interested contractors to respond to this Request for Information (RFI) for RMIC Support Services in support of the Defense Intelligence Agency (DIA). VaCA seeks information from qualified industry sources capable of providing enterprise-wide Enterprise Risk Management (ERM) and Risk Management Internal Controls (RMIC) support in highly classified environments.

This RFI is part of VaCA's market research efforts to better understand industry capabilities, innovative approaches, and best practices for Federal ERM and RMIC activities in accordance with DoDI 5010.40, OMB Circular A-123, GAO Green Book, GAO Fraud Risk Management (FRM) Framework, and Supply Chain Risk Management (SCRM). Information received may be used to shape acquisition strategy, refine technical requirements, evaluate small business opportunities, and support development of a future solicitation.

2. PURPOSE:

VaCA is conducting market research to inform of a potential upcoming acquisition for RMIC Support Services. VaCA expects to award a multi-year Blanket Purchase Agreement (BPA) to one or more sources for this initiative. Attachment 1 is the draft Performance Work Statement (PWS) for the BPA. The PWS may be updated on information gathered from this RFI based on industry review and comment.

3. BACKGROUND:

In accordance with DoDI 5010.40, DIA is required to maintain an integrated Enterprise Risk Management (ERM) and Risk Management and Internal Control (RMIC) program. DIA requires support to plan, execute, and document ERM and RMIC activities across all applicable domains, including:

- Internal Control Over Reporting for Financial Reporting (ICOR-FR)
- Internal Control Over Reporting for Financial Systems (ICOR-FS)
- Internal Control Over Reporting for Management Operations (ICOR-O)
- Non-financial information technology systems
- ERM
- FRM, including payment integrity requirements
- SCRM

DIA utilizes ServiceNow's Integrated Risk Management (IRM) solution as the system of record for managing RMIC activities, including risk assessments, control testing, deficiency tracking, corrective action plans, and compliance reporting.

DIA requires support for risk profile and risk register maintenance within ServiceNow IRM, coordination with DoD governance bodies, and compliance with applicable laws, regulations, and policies. Performance is expected to require on-site work in TS/SCI environments in accordance with DIA security requirements. Contractor personnel will support but not replace government-designated Component RMIC manager roles required by DoDI 5010.40.

4. DRAFT SCOPE OF SERVICES

The Government's draft scope and requirements are provided in the attachments. Respondents are encouraged to review both documents and provide comments and recommendations in accordance with Section 5.

Attachment 1: RMIC BPA PWS_8 June 26

5. INFORMATION REQUESTED FROM INDUSTRY

Respondents are requested to provide concise information addressing the following areas:

a. Corporate Capability and Relevant Experience
   1) Experience supporting DoD ERM and RMIC programs in accordance with DoDI 5010.40, OMB Circular A-123, and GAO Green Book, including all RMIC domains (ICOR-FR, ICOR-FS, ICOR-O, non-financial IT systems, ERM, FRM, and SCRM).

   2) Experience supporting SCRM programs in accordance with DIA Directive 5010.1, IC Directive (ICD) 731, IC Standards (ICS) 731-01 through 731-05, Federal Acquisition Supply Chain Security Act, and DFARS 252.239-7018, including:

      a) SCRM risk assessments for Mission-Critical (MC) information and communication technology (ICT) acquisitions
      b) Integration of counterintelligence (CI) threat assessments and cybersecurity vulnerability assessments

   c) SCRM incident reporting and analysis
   d) Coordination with SCRM governance structures and steering groups
   e) Support for interagency information sharing (Federal Acquisition Security Council, ODNI SCRM Task Force)
   f) Application of Federal Acquisition Regulation (FAR) and DFARS SCRM clauses

3) Experience supporting FRM activities in accordance with GAO FRM Framework (GAO 15-593SP) and OMB A-123, including payment integrity (PIIA) requirements, risk assessments, sampling/estimation support, and reporting support.

4) Experience applying applicable standards and guidance, including:
   a) DoDI 5010.40 (DoD Enterprise Risk Management and Risk Management and Internal Control Program)
   b) OMB Circular A-123 (Management's Responsibility for Enterprise Risk Management and Internal Control)
   c) GAO Green Book (Standards for Internal Control in the Federal Government)
   d) GAO FISCAM (Financial Information Systems Control Audit Manual) for system-related controls
   e) GAO FRM Framework (GAO 15-593SP)
   f) DoDI 5015.02 (DoD Records Management Program) and DoD Manual 5200.01, Volume 3 (DoD Information Security Program)

5) Experience developing and maintaining risk profiles and risk registers in line with OSD risk assessment templates, including support for DoD-level enterprise management operations risk profile development.

6) Experience supporting DoD governance bodies, including but not limited to:
   a) Defense Performance Improvement Council Integrated Risk Management Committee
   b) Financial Improvement and Audit Remediation Governance Board
   c) Deputy's Management Action Group
   d) Fraud Reduction Task Force
   e) SCRM Steering Groups

7) Experience supporting GAO audit recommendation closure, tracking of top DoD management challenges, and coordination with Senior Accountable Officials (SAOs) and Assessable Unit Managers (AUMs).

8) Experience with entity-level controls (ELCs), service provider controls (SOC 1 Type 2), complementary user entity controls, and cybersecurity controls (OMB M-17-25 compliance).

9) Experience utilizing ServiceNow's IRM solution as the system of record for RMIC activities, including:
   a) Risk assessment and control testing workflow execution
   b) Deficiency and corrective action tracking and reporting
   c) Workpaper and evidence management
   d) Compliance reporting
   e) Compliance with established system configurations and data governance requirements

f) Integration with other Government repositories as directed

10) Ability to perform on-site in TS/SCI environments and sustain cleared staffing.
11) Up to three (3) recent and relevant past performance examples demonstrating support for integrated ERM and RMIC programs.

b. Technical Approach (BPA)
1) Recommended approach for risk assessment and planning across all RMIC domains, including:
   a) Risk identification, assessment, prioritization, response, and monitoring
   b) Development of risk profiles (OSD template-based) and risk registers
   c) Supply chain risk assessments for MC ICT acquisitions, including CI threat assessment integration and cybersecurity vulnerability assessment coordination
   d) Support for DoD-level enterprise management operations risk profile development
   e) Test planning (test plans, scripts, sampling methodology, schedules)
   f) Integration of ERM, RMIC, and SCRM activities
2) Recommended approach for control testing and evaluation, including:
   a) Design and operating effectiveness testing across all RMIC domains (ICOR-FR, ICOR-FS, ICOR-O, non-financial IT systems, ERM, FRM, and SCRM)
   b) Entity-level Controls (ELCs) testing
   c) Service provider controls evaluation (SOC 1 Type 2 reports)
   d) Complementary user entity controls assessment
   e) Supply chain controls testing for MC ICT acquisitions
   f) Cybersecurity controls testing (OMB M-17-25 compliance)
   g) Application of GAO FISCAM (system controls), GAO FRM Framework (fraud risks), and IC Standards (ICS) 731-01 through 731-05 (supply chain risks)
   h) Workpaper and evidence maintenance sufficient for re-performance and Government review

3) Recommended approach for deficiency identification and reporting, including:
   a) Exception identification and documentation
   b) Material Weakness (MW) and Significant Deficiency (SD) classification by RMIC domain
   c) Root cause analysis methodology
   d) Draft findings packages (criteria/condition/cause/effect, evidence references, severity rationale, recommended remediation)
   e) Escalation protocols and re-testing support
   f) Fraud risk and supply chain risk identification and escalation

4) Recommended approach for corrective action support, including:
   a) Corrective Action Plan (CAP) development and refinement
   b) Milestone establishment and tracking
   c) Validation and re-test support
   d) Coordination with SAOs, AUMs, and governance bodies
   e) Impediment identification and reporting

5) Recommended approach for SOA support, including:
   a) Documentation compilation across all RMIC domains
   b) Supporting documentation for ICOR categories (financial reporting and operations)

c) Executive summary preparation
d) Component and DoD-level SOA consolidation support

6) Recommended approach for repository discipline and knowledge management, including:
    a. Utilization of ServiceNow IRM as the system of record for RMIC activities
    b. Compliance with DIA-established workflows, data structures, and configurations within ServiceNow IRM
    c. Integration with other Government-designated repositories (SharePoint, Advana, or other approved platforms) for supporting documentation as directed
    d. Records management (DoDI 5015.02) and classified information handling (DoD Manual 5200.01, Volume 3)
    e. Traceability and chain-of-custody documentation
    a) Leveraging ServiceNow IRM automation and reporting capabilities
7) Recommended approach for quality control of performance (QC program/QCP), including:
    a. Independent QC review processes
    b. Alignment with applicable standards (DoDI 5010.40, OMB A-123, GAO Green Book, GAO FISCAM, GAO FRM Framework, IC Standards 731)
    c. Application to testing execution and evidence sufficiency
    d. Corrective action processes for performance deficiencies
    e. Integration with Government Quality Assurance Surveillance Plan (QASP)

c. Staffing and Clearance Sustainment
1) Recommended staffing model for a single-award BPA supporting multiple call orders, including:
    a. Approach to scaling across DIA organizations
    b. Support for government-designated Component RMIC manager and other government roles
    c. Coordination with SAOs, AUMs, and governance bodies
    d. Coverage of all RMIC domains (ICOR-FR, ICOR-FS, ICOR-O, non-financial IT systems, ERM, FRM, and SCRM)
2) Clearance sustainment strategy, including:
    a. TS/SCI pipeline management
    b. Onboarding timelines
    c. Continuity and turnover mitigation
    d. Additional access requirements (polygraph, SAP/SAR compartments)
3) Recommended key personnel roles for the BPA, including:
    a. Program Manager qualifications and responsibilities
    b. RMIC Technical Lead qualifications and responsibilities
    c. Domain-specific expertise (financial reporting, financial systems, operations, IT systems, fraud risks, supply chain risks)
    d. Relevant certifications (CPA, CIA, CISA, CGFM, CGAP, CDFM, or equivalent)

d. Transition and Continuity
1) Recommended transition-in approach including:
    a) Knowledge transfer strategies
    b) Access and badging coordination
    c) Continuity of operations

d) Government-designated Component RMIC manager coordination

2) Key transition risks and mitigations, including:
   a) Clearances and facility access
   b) System access provisioning
   c) Data availability and chain-of-custody
   d) Stakeholder dependencies and coordination

e. Contracting and Pricing Input
1) Recommended contract type/structure for the BPA and call orders (e.g., FFP, FFP-LOE, T&M) and rationale.
2) Recommended ordering vehicle approach (e.g., open market, GSA MAS, BPA/call order strategy) and rationale.
3) Rough Order of Magnitude (ROM) estimate for the initial Scope of Work, including key assumptions and cost drivers.
4) Recommended BPA ordering period structure and call order Period of Performance approach (if different from the draft).

f. Performance Standards / Metrics (Call Order Level)
1) Recommended approach for quality control of performance (QC program/QCP approach), including:
   a) Application to testing execution and evidence sufficiency
   b) Alignment with applicable standards (DoDI 5010.40, OMB A-123, GAO Green Book, GAO FISCAM, GAO FRM Framework, IC Standards 731)
   c) Integration with Government QASP
2) Recommended surveillance methods that are practical for Government administration, including:
   a) Performance metrics and indicators
   b) Reporting frequency and format
   c) Government oversight and validation approaches

g. Small Business / Socioeconomic Information
1) Business size and socioeconomic status.
2) Teaming/partnering approach and ability to support enterprise-wide requirements.

h. Risks and Recommendations
1) Key risks to successful performance and recommended mitigations, including:
   a) Technical and operational risks
   b) Schedule and resource risks
   c) Security and access risks
   d) Stakeholder coordination risks
2) Recommended edits to the draft SOO/PWS, including areas that are unclear, overly prescriptive, missing, or not measurable.

i. Draft Document Feedback (PWS Redlines)
1) Provide recommended edits to the draft BPA-level PWS, including areas that are unclear, overly prescriptive, missing, or not measurable. Redlines using track changes or a comment matrix (page/paragraph, issue, recommended change, rationale) are preferred.

j. Organizational Information
   a) Name of Company/Organization

1. Address
2. Website/URL
3. Point of Contact (POC) Name
4. Email Address and Phone Number
5. System for Award Management (SAM) Unique Entity Identifier (UEI) (An offeror must have a UEI and be registered in SAM by the time of award.)
6. Commercial and Government Entity (CAGE)
7. GSA Multiple Award Schedule Contract Number and Expiration Date, if applicable
8. Indicate the size classification of your Company/Organization.
    - Small Business
    - Other Than Small Business
9. Indicate the socio-economic status of your Company/Organization.
    a. SBA-Certified Small Disadvantaged Business (SDB)
    b. Woman-Owned Business
    c. Economically Disadvantaged WOSB (EDWOSB)
    d. Veteran-Owned Small Business (VOSB)
    e. Service-Disabled Veteran-Owned Small Business (SDVOSB)
    f. SBA-Certified HUBZone (HUBZ) Firm
    g. SBA-Certified 8(a)
    h. Alaska Native Corporations (ANC) Tribal, American Indian, Native Hawaiian (NHO)
    i. None
    j. Other

6. RESPONSE INSTRUCTIONS

- Response Due Date: June 30, 2026 at 4:00 p.m. EST
- Submission Method: Email electronic submission to : Section 11 POCs
- Subject Line: RFI Response- Risk Management and Internal Control (RMIC) Requirement."
- Page Limit: Limited to 15 pages, excluding attachments
- Questions: Submit questions to [Insert POC] no later than [Insert date]. The Government may respond via consolidated Q&A at its discretion.

7. REQUESTED RESPONSE FORMAT

To support consistent review, respondents are encouraged to organize responses using the headings in Section 5 and include:

a. Capability statement addressing all RMIC domains and applicable standards
b. Relevant experience/past performance references demonstrating integrated ERM and RMIC support
c. Proposed staffing approach covering all required expertise areas
d. ROM estimate with assumptions for the scope of work
e. Contract vehicle information (e.g., GSA MAS contract number/SINs), if applicable
f. Redlines/comments on Attachment 1 (track changes or comment matrix preferred)

8. DISCLAIMER

This notice is for information and planning purposes only and does not commit the government to an contractual agreement. The RFI does not constitute a solicitation (RFQ/RFP/IFB), or does not obligate the Government to award a contract or pay for response preparation costs. Respondents should not submit classified information, and Proprietary information, if provided, shall be clearly marked. The Government may not provide feedback on individual responses and is not required to respond to all submissions.

9. SECURITY / PLACE OF PERFORMANCE

Performance is expected to require on-site work at DIA facilities and access to classified systems and information. Respondents should address their ability to support TS/SCI-cleared staffing, facility access, and secure handling of Government information consistent with DIA requirements, the DD Form 254, and applicable security guidance (DoD Manual 5200.01, Volume 3). Contractor personnel will support but not replace government-designated roles required by DoDI 5010.40, including the Component RMIC manager position.

10. QUESTIONS/POINTS OF CONTACT

All responses to this RFI must be submitted to Dale Williams, Contract Specialist, at dale.williams2@dodiis.mil via email. Please email responses with the subject line “RFI Response- Risk Management and Internal Control (RMIC) Requirement.” If you have any questions concerning this opportunity, please contact Dale Williams, Contract Specialist at the email listed above, and Demario Grover at demario.grover@dodiis.mil. The government will endeavor to respond to all valid questions submitted.