NCIA/ACQ/2026/07399
Friday, 03 July 2026

NCIA Request for Information (RFI)

To: **Industry Partners**

Subject: **MALWARE ANALYSIS AND DETECTION ENGINEERING PLATFORM**
RFI-424358-TSSU-MA-DE

1. The NATO Communications and Information Agency (NCIA) is conducting market research to identify qualified vendors and gather input on potential solutions to support the upcoming acquisition for a Malware Analysis and Detection Engineering Platform. To that end, we are issuing the attached Request for Information (RFI) 424358 to solicit feedback from capable and interested industry partners.

2. This RFI is issued for planning and budgeting purposes only and is not a request for bids. It is part of NCIA's effort to ensure it has a clear understanding of the marketplace, available capabilities, estimated costs and potential acquisition strategies.

3. We value your insight and invite you to:
- **a.** Share relevant corporate capabilities and experience;
- **b.** Review and comment on our draft requirements (Annexes A & B) with a view in providing recommendations for improving performance outcomes, competition, and efficiency; and identifying any risks or concerns that should be considered during planning.

4. Submission instructions and additional details can be found in the enclosure to this RFI.

5. Only companies from a NATO member country can participate in or respond to this RFI (https://www.nato.int/cps/en/natohq/nato_countries.htm).

6. Should you have any questions or need clarification, please contact Leonora Alushani, Contracting Officer at RFI-424358-TSSU-MADE@ncia.nato.int.

7. We thank you in advance for your time and input, and we look forward to engaging with you as we shape this potential acquisition.

For the Chief of Acquisition:

Leonora Alushani
Contracting Officer

Enclosure:

- Request for Information with Annexes A, B & C
- Distribution List

Distribution List

1. NATO Delegation (Attn: Infrastructure Adviser)

1. Albania	**12.** Greece	**23.** Poland
2. Belgium	**13.** Hungary	**24.** Portugal
3. Bulgaria	**14.** Iceland	**25.** Romania
4. Canada	**15.** Italy	**26.** Slovakia
5. Croatia	**16.** Latvia	**27.** Slovenia
6. Czechia	**17.** Lithuania	**28.** Spain
7. Denmark	**18.** Luxembourg	**29.** Sweden
8. Estonia	**19.** Montenegro	**30.** Türkiye
9. Finland	**20.** Netherlands	**31.** United Kingdom
10. France	**21.** North Macedonia	**32.** United States
11. Germany	**22.** Norway	

2. All NATEXs

NATO Communications and Information Agency

Table of Contents

REQUEST FOR INFORMATION

A. Introduction

1. The NATO Communications and Information Agency (NCIA) is conducting market research to identify potential sources and gather information regarding industry capabilities to support a Malware Analysis and Detection Engineering Platform. This Request for Information (RFI) is issued solely for informational and planning purposes and does not constitute a Request for Proposal (RFP), Request for Quotation (RFQ), or invitation for bid.

B. Purpose

1. The purpose of this RFI is to obtain input from industry to help inform the NCIA's acquisition planning. Responses to this RFI will assist in refining requirements, identifying capabilities, budget planning and shaping the strategy for any future solicitation.

C. Background

1. Malware analysis within NCIA is performed by the NCSC Cyber Threat Investigation Section. The section provides in-depth cyber threat analysis, malware analysis, and digital forensics in support of incident response activities, as well as proactive efforts to identify and investigate cyber threat activity. Its work supports the development of actionable cyber threat information to strengthen the defensive posture of the NATO Enterprise and NATO Operations and Missions networks.
2. Within this section, the service provides technical analysis capabilities in response to cybersecurity incidents and other cyber investigation requirements. This includes both digital forensics and malware analysis. The service is often engaged where more advanced or specialized technical analysis is required, comparable to a higher-tier technical support function for cyber investigations.
3. In addition to incident response, the team conducts continuous service improvement activities and maintains the specialized skills required to keep pace with evolving adversary techniques, including methods intended to hinder forensic examination, malware reverse engineering, detection engineering, and technical analysis.
4. The current malware analysis capability is supported by a distributed ecosystem of tools and environments. This includes a small cloud-based foothold used to receive suspicious samples, store analysis artefacts, and access general IT capabilities such as team collaboration and source code versioning. Suspicious samples may be received through a dedicated mailbox and are analysed using isolated workstations that are disconnected from NATO networks.
5. Analysis activities are typically performed using purpose-built virtual machines, including static analysis environments, dynamic analysis or victim environments, and anonymization environments used to access external or higher-risk resources where required. The team also makes use of commercial tools, vendor-provided documentation, and capabilities provided by other NATO entities and partner nations, often delivered as Software-as-a-Service.
6. The team also uses an automated malware analysis platform to support the automated detonation, triage, and enrichment of suspicious files and related artefacts. This RFI is not primarily seeking to replace that automated malware analysis capability. Respondents should therefore focus their feedback on the capabilities described in the

attached Epics and User Stories, rather than assuming that the objective is to replace every element of the existing malware analysis ecosystem.

7. On premises, the team uses Jira to receive, manage, and report on malware analysis tasks; Confluence to document procedures, findings, and threat knowledge; and Splunk to support case-by-case research of logs and other telemetry, particularly in proactive investigation scenarios.
8. This RFI seeks industry feedback on how a future Malware Analysis and Detection Engineering capability could be delivered primarily as a fully managed service, implemented and maintained by the Contractor. The intended outcome is to enable Purchaser personnel to perform secure malware analysis, detection engineering, and related workflows with minimal administrative effort, while making use of Commercial-Off-The-Shelf products, standard service capabilities, and limited customization wherever feasible.

D. Submission Instructions

1. Interested parties are invited to respond in accordance with the instructions below:

   a. Submit responses via the email address in section G no later than **12:00 hours Central European Time (CET)** on **17 July 2026**.

   b. Responses should be submitted using the Excel Response template provided in Annex C

   c. The following can be included as a reference in your responses and attached as separate documents:
      i. Company brochures or product literature (optional)
      ii. Attachments such as past performance references (optional)

   d. Use the following subject line for submission
      i. “Response to RFI [424314-NPKI-TPT] – [Company Name]”

   e. All responses should address the items listed in Annex A – Requested Information.

E. Disclaimer

1. This RFI is for planning and informational purposes only and shall not be construed as a solicitation or obligation on the part of the NCIA. The NCIA does not intend to award a contract based on responses to this RFI. Respondents are solely responsible for all costs incurred in responding to this RFI. The NCIA will consider and analyse all information received from this RFI and may use these findings to develop a future solicitation. The NCIA will consider all responses as confidential commercial information and will protect it as such.

2. NCIA reserves the right, at any time, to cancel this informal market survey, partially or in its entirety. No legal liability on the part of NCIA for payment of any sort shall arise and in no event will a cause of action lie with any prospective participant for the recovery of any costs incurred in connection with the preparation of documentation or participation in response hereto. All effort initiated or undertaken by prospective informal market survey participants shall be done considering and accepting this fact.

F. Use of Information Provided through Responses

1. Confidentiality of Responses

The NCIA may incorporate industry comments and responses, in part or in whole, into a future release of a solicitation. Should respondents include proprietary data in their responses that they do not wish to be disclosed to the public for any purpose, or used by NCIA (except for internal evaluation purposes), they must:

a. Mark the title page with the following legend:

This document includes data that shall not be disclosed outside NATO and shall not be duplicated, used, or disclosed – in whole or in part – for any purpose other than for NCIA internal evaluation purposes, unless otherwise expressly authorised by [insert company name]. This restriction does not limit the NCIA's right to use information contained in this data without restriction if it is obtained from another source. The data subject to this restriction are contained in sheets [insert numbers or other identification of sheets]

b. Mark each sheet of data it wishes to restrict with the following legend:

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.

G. RFI Point of Contact

1. Leonora Alushani

2. RFI-424358-TSSU-MADE@ncia.nato.int. .

Annex A – Requested Information

A.1 Purpose and Desired Outcome
The purpose of this Request for Information is to obtain industry feedback on the attached draft Epics and User Stories for a Malware Analysis and Detection Engineering capability, provided in Annex B.

The Purchaser's intent is to validate whether the required operational outcomes can be achieved primarily through existing Commercial-Off-The-Shelf products, standard managed service offerings, configuration, and limited integration wherever possible. The Purchaser does not intend to drive the requirement toward a fully custom-developed solution unless industry feedback demonstrates that this is necessary to achieve the required operational outcomes.

The desired outcome of this RFI is to help the Purchaser refine the attached Epics and User Stories before any potential future solicitation. Industry feedback should help determine whether the required capability can be achieved through existing products and standard managed service offerings, whether the requirements should be adjusted to better align with market capabilities, and where customization or bespoke development may create avoidable cost, complexity, or risk

Respondents are requested to review the Epics and User Stories provided in Annex B and provide structured feedback using the response template in Annex C. Response should focus on practical product capability, managed service delivery, implementation approach, risks, constraints, and recommendations.

Marketing material may be included as supporting information; however, respondents are invited to complete the response template in Annex C to allow consistent comparison of industry responses.

A.2 Scope of Requested Feedback
Respondents are requested to provide feedback on the degree to which their proposed product, platform, service, or combination thereof aligns with the attached Epics and User Stories.

The Purchaser is particularly interested in understanding:

1. Which Epics or capability areas are well supported by the respondent's existing Commercial-Off-The-Shelf products or standard managed service offerings.
2. Which capabilities can be achieved through standard configuration.
3. Which capabilities would require customization, integration, professional services, or bespoke development.
4. Which capabilities are not supported.
5. Which User Stories may be too specific, unnecessarily complex, or misaligned with common product or managed service capabilities.
6. What alternative approaches the respondent would recommend where a User Story is not supported, and why the alternative would better achieve the underlying operational intent.
7. Whether there are industry-standard capabilities, workflows, or product features that should be considered but are not currently reflected in the Epics and User Stories.
8. How the capability would be implemented, operated, maintained, upgraded, and supported by the Contractor.

9. How licensing, renewal, sustainment, support, and service management would typically be structured.

A.3 Response Approach

To reduce response burden and support meaningful comparison across submissions, respondents should first provide feedback at the Epic or capability level.
Detailed User Story-level responses are only required where:

- the capability is not supported natively by the proposed product, platform, or service;
- the capability would require customization;
- the capability would require significant integration;
- the respondent recommends an alternative approach;
- the User Story creates implementation complexity, cost, risk, vendor lock-in, or technical constraints; or
- the User Story should be clarified, consolidated, removed, reprioritized, or reframed.

Respondents should avoid treating the attached User Stories as a compliance matrix. The Purchaser is seeking industry feedback on the feasibility, maturity, and suitability of the required capabilities, including whether the User Stories should be adjusted to better align with existing Commercial-Off-The-Shelf products and standard managed service models.

A.4 Areas of Interest

Respondents are requested to address the following areas in their response and to prioritize responding to A.4.1 through A.4.4, responding to the other areas when applicable and time permitting.

A.4.1 Overall Fit

Respondents should provide a summary of the overall fit between the attached Epics and User Stories and their proposed solution or service. This should include areas of strong alignment, areas of partial alignment, and areas that are not supported or would require significant adaptation.

A.4.2 COTS and Managed Service Alignment

Respondents should identify which capabilities are available through existing Commercial-Off-The-Shelf products, which are available through standard managed service offerings, and which would require configuration, integration, customization, or professional services.

A.4.3 User Story Exceptions, Gaps, Risks, and Recommended Changes

For User Stories that are not fully supported, or where the respondent recommends a different approach, respondents should identify the relevant User Story, describe the issue or gap, and provide a recommended approach.
Relevant feedback may include, but is not limited to:

- the User Story is not supported;
- the User Story is partially supported;
- the User Story requires configuration;
- the User Story requires customization;
- the User Story requires third-party integration;
- the User Story assumes a custom workflow rather than a standard product or service workflow;

- the User Story may introduce unnecessary cost, complexity, risk, or vendor lock-in;
- the User Story should be clarified, consolidated, removed, or reprioritized; or
- the operational intent could be achieved through an alternative product capability, workflow, or managed service approach.

A.4.4 Recommended Additional Capabilities
Respondents should identify any industry-standard capabilities, workflows, or service features that are not reflected in the attached Epics and User Stories but should be considered by the Purchaser.

A.4.5 Implementation, Operation, and Sustainment
Respondents should describe how a comparable capability would typically be implemented, transitioned into service, operated, maintained, and upgraded. This should include key Purchaser responsibilities, key Contractor responsibilities, common dependencies, implementation risks, training considerations, and sustainment considerations.

A.4.6 Configuration, Customization, and Integration
Respondents should describe which capabilities can typically be configured by the Purchaser or Contractor, which changes would require vendor professional services, which changes would require custom development, and how customizations or integrations are maintained through upgrades.
Respondents should also identify relevant APIs, connectors, import/export mechanisms, and integration patterns applicable to the proposed solution or service.

A.4.7 Licensing, Renewal, and Support Model
Respondents should describe the typical licensing, renewal, support, and service model for the proposed capability. This should include relevant licensing metrics, support tiers, software update arrangements, renewal model, optional modules or add-ons, and any separate costs for implementation, migration, training, integration, or sustainment.

Tracking ID	Epic / Goal	User Story / Description
MA	Malware Analysis & Detection Engineering Platform	Delivery of a fully managed Malware Analysis capability as a service, implemented and maintained by the contractor, enabling purchaser personnel to perform secure analysis, detection engineering, and related workflows with minimal administrative effort.
MA-E1	Malware Analysis Lab	Provide a fully integrated platform enabling secure, in-depth manual malware analysis across static and dynamic techniques
MA-E1-BV		Enable in-depth Malware analysis in a controlled environment while minimizing operational overhead
MA-US-1.1		As a Malware Analyst, I want the platform to provide the capability to perform static, dynamic, memory, and network traffic analysis on malware so that I can comprehensively understand its behavior and impact.
MA-US-1.2		As a Malware Analyst, I want to execute Malware in isolated environments so that behavior can be safely observed within environments provisioned and maintained by the platform.
MA-US-1.3		As a Malware Analyst, I want to select multiple OS environments so that Malware can be tested across realistic configurations
MA-US-1.4		As a Tech Lead, I want the platform to be delivered as a fully managed and operational service by the contractor so that no internal setup or infrastructure management is required.
MA-US-1.5		As a Malware Analyst, I want the platform to support extension and customization of analysis capabilities so that I can adapt the environment to evolving analysis requirements
MA-US-1.6		As a Malware Analyst, I want the capability to analyze malware samples originating from various IT platforms, including mobile devices (e.g. IOS, Android), so that threats across all supported environments can be effectively assessed
MA-US-1.7		As a Malware Analyst, I want concurrent execution so that throughput is maximized
MA-US-1.8		As a Malware Analyst, I want long-duration execution so that delayed behavior is captured
MA-US-1.9		As a Tech Lead, I want rapid re-imaging so that efficiency is maintained
MA-US-1.10		As a Malware Analyst, I want encrypted traffic analysis so that hidden communications can be inspected
MA-E2	Detection Engineering Platform	Provide a platform to create, test, and manage detection rules derived from Malware analysis
MA-E2-BV		Enable transformation of Malware insights into operational detection capabilities
MA-US-2.1		As a Detection Engineer, I want to create and manage YARA, Suricata and Snort rules using platform-provided capabilities so that Malware can be identified across both file and network activity
MA-US-2.2		As a Detection Engineer, I want to test rules against stored samples so that rule effectiveness is validated using platform-provided capabilities
MA-US-2.3		As a Detection Engineer, I want to test and compare rules against the existing ruleset to identify duplication and redundancy so that the ruleset remains consistent, optimized, and easy to manage using platform-provided capabilities
MA-US-2.4		As a Detection Engineer, I want version control and rollback for detection rules so that rule changes are controlled and traceable using platform-provided capabilities
MA-US-2.5		As a Detection Engineer, I want to validate and test detection rules before they are approved so that rule quality, accuracy, and performance are ensured using platform-provided capabilities
MA-US-2.6		As a Detection Engineer, I want to import and evaluate detection rules from external sources so that they can be validated and integrated into the ruleset in a controlled manner using platform-provided capabilities
MA-US-2.7		As a Detection Engineer, I want approved detection rules and extracted IOCs to be automatically synchronized with the internal MISP instance so that they can be rapidly distributed and operationalized using platform-provided capabilities
MA-US-2.8		As a Detection Engineer, I want the capability to browse, query, and export detection rules using advanced filtering so that rules can be efficiently managed and shared using platform-provided capabilities
MA-US-2.9		As a Malware Analyst, I want to generate detection rules from analysis results so that insights are operationalized quickly using platform-provided capabilities
MA-E3	Binary Samples Management and Archival	Provide secure storage and lifecycle management of Malware samples and artefacts
MA-E3-BV		Ensure integrity, traceability, and reuse of Malware analysis data
MA-US-3.1		As a Malware Analyst, I want all artefacts stored securely so that they can be retrieved later
MA-US-3.2		As a Malware Analyst, I want to re-analyze stored samples so that new insights can be derived
MA-US-3.3		As a Service Delivery Manager, I want the platform to provide managed backup and archival capabilities so that data is preserved without internal administration
MA-E4	Security and Governance	Ensure secure operation, isolation, and auditability of the platform
MA-E4-BV		Protect sensitive data and ensure compliance with security requirements
MA-US-4.1		As a Security Officer, I want the platform to provide controlled and secure connectivity
MA-US-4.2		As a Malware Analyst, I want simulated network services so that Malware behavior can be observed safely
MA-US-4.3		As a Security Officer, I want all access and actions on malware samples to be recorded so that compliance and audit requirements are met.
MA-E5	Platform Service Management	Provide a platform as a service
MA-E5-BA		Ensure the platform is fully managed by the contractor while enabling purchaser personnel to perform analysis with minimal administrative burden
MA-US-5.1		As a Service Delivery Manager, I want the contractor to operate and maintain the platform so that internal teams are not responsible for infrastructure or system maintenance
MA-US-5.2		As a Service Delivery Manager, I want malware analysis and detection engineering activities to be performed by purchaser personnel so that operational control remains internal
MA-US-5.3		As a System Administrator, I want updates, patches, and upgrades to be managed by the contractor so that the platform remains current without internal efforts
MA-US-5.4		As a Tech Lead, I want all underlying infrastructure (compute, storage, networking) to be provided and maintained by the contractor so that no internal infrastructure management is required.
MA-US-5.5		As a Security Officer, I want all access (e.g. contractor, purchaser) to be controlled, auditable and only accessible by personnel who hold the appropriate clearance so that the platform be maintained without compromising security
MA-US-5.6		As a Service Delivery Manager, I want the contractor to monitor platform health and performance so that issues are proactively identified and resolved.
MA-US-5.7		As a Service Delivery Manager, I want all licensing for the platform and its components to be fully managed by the contractor so that no administrative overhead is required from the purchaser.

MA-US-5.8		As a Service Delivery Manager, I want all recurring licensing and service cost to be clearly defined, simple, and predictable so that they can be easily budgeted and managed over time.
MA-E6	Analyst Workspace and Collaboration	Provide collaborative workspace for analysts and reverse engineers
MA-E6-BV		Improve analyst efficiency and knowledge sharing
MA-US-6.1		As a Malware Analyst, I want shared cases so that collaboration is possible
MA-US-6.2		As a Reverse Engineer, I want shared artefacts and notes so that work is reusable
MA-US-6.3		As a Service Delivery Manager, I want role-based access control so that access is controlled
MA-US-6.4		As a System Engineer, I want the solution to have an Application Programming Interface (API) to allow automation or programmatic usage of all system functions of the Platforms delivered (Malware Analytic platform, Detection Engineering Platform, etc.)
MA-E7	Reporting and Visualization	Provide reporting, dashboards, and search capabilities
MA-E7-BV		Enable clear understanding and communication of Malware behavior
MA-US-7.1		As a Malware Analyst, I want detailed reports so that behavior is understood
MA-US-7.2		As a Malware Analyst, I want context-based search so that I can find data quickly
MA-US-7.3		As a Service Delivery Manager, I want dashboards so that system status is visible
MA-US-7.4		As a Malware Analyst, I want visual execution graphs so that behavior is clear
MA-NFR	Non-Functional Requirements	Define system-wide performance, security, and operational requirements
MA-NFR-1		System shall support defined concurrent analysis capacity and sustained workloads without degradation
MA-NFR-3		System shall provide full audit logging and traceability
MA-NFR-5		System shall ensure secure storage and integrity of information
MA-NFR-6		System shall provide role-based access control across all components
MA-NFR-8		The solution shall be delivered as a contractor-managed platform, including infrastructure, maintenance, monitoring and support
MA-NFR-9		The contractor shall provide and maintain the platform but shall not perform malware analysis or detection engineering activities.
MA-NFR-10		The solution shall require minimal administrative effort from the purchaser, limited to user and access management.
MA-NFR-11		The contractor shall be responsible for patching, updates, performance tuning, and system health.
MA-NFR-12		The solution shall enforce secure, controlled, and auditable access for all users, including purchaser personnel and contractor support staff, in accordance with purchaser-defined security policies, regardless of deployment model.

Statement of Confidentiality
This document includes data that shall not be disclosed outside NATO and shall not be duplicated, used, or disclosed – in whole or in part – for any purpose other than for NCIA internal evaluation purposes, unless otherwise expressly authorized by [insert company name]. This restriction does not limit the NCIA's right to use information contained in this data without restriction if it is obtained from another source.

Respondent Information	
Company Name	
Product / Platform / Service	
Product Version	
Primary point of contact	
Deployment models available	SaaS / Private Cloud / On Prem / Etc.
Proposed Delivery Model	Product / Manage Service / Product with Managed Service, etc.
Relevant Implementation Experience	
Similar Customers or use cases (if applicable)	

Summary of recommended solution(s)	

Use or disclosure of data contained on this sheet is subject to the restriction on the cover page of this document

Overall Fit	
Please provide a short summary of the overall fit between the attached User Stories and your existing COTS / SaaS solution	
Overall alignment with the attached User Stories	Strong / Moderate / Limited / Other
Summary of strongest areas of alignment	
Summary of weakest areas of alignment	
Areas likely to require configuration	
Areas likely to require customization	
Areas likely to require third-party integration	
Areas not supported	
General comments or assumptions	

Epic / Capability-Level Response Matrix

Respondents are requested to complete this section for each Epic or major capability area. Detailed User Story-level responses are only required in the next section where there is a gap, partial alignment, customization requirement, integration requirement, or recommended alternative.

Epic	Overall Alignment	Supported Natively	Supported through Configuration	Requires Customization	Requires Integration	Not Supported	Prof Services Req	Comments
MA-E1								
MA-E2								
MA-E3								
MA-E4								
MA-E5								
MA-E7								

Legend	
Strong:	Capability is substantially supported by existing product or standard service capability
Moderate:	Capability is partially supported by may require configuration, integration, process adaptation , or limited services
Limited:	Capability is only partially supported and would require significant work or adaptation
Not Supported:	Capability is not supported by the proposed product, platform or service

User Story-Level Exceptions, Gaps, Risks, and Recommended Changes

For each Epic marked as "Partial", "Requires Customization", "Requires Integration", "Requires Professional Services", or "Not Supported", respondents should complete the applicable portions in this section. This section should be completed only for User Stories that are not fully supported by existing COTS functionality, or where the respondent recommends a different approach.

Respondents are requested to identify whether the recommended approach would be achieved through:

- *standard product configuration;*
- *workflow or process adaptation;*
- *integration with another tool or platform;*
- *vendor professional services;*
- *custom development;*
- *a change to the User Story; or*
- *an alternative COTS capability that achieves the same operational intent.*

User Stories	Issue Type	Explanation / Concern	Recommended Approach	Rationale	Expected Implementation Approach
MA-US-1.1					
MA-US-1.2					
MA-US-1.3					
MA-US-1.4					
MA-US-1.5					
MA-US-1.6					
MA-US-1.7					
MA-US-1.8					
MA-US-1.9					
MA-US-1.10					
MA-US-2.1					
MA-US-2.2					
MA-US-2.3					
MA-US-2.4					
MA-US-2.5					
MA-US-2.6					
MA-US-2.7					
MA-US-2.8					
MA-US-2.9					
MA-US-3.1					
MA-US-3.2					
MA-US-3.3					
MA-US-4.1					
MA-US-4.2					
MA-US-4.3					
MA-US-5.1					
MA-US-5.2					
MA-US-5.3					
MA-US-5.4					
MA-US-5.5					
MA-US-5.6					
MA-US-5.7					
MA-US-5.8					
MA-US-6.1					
MA-US-6.2					
MA-US-6.3					
MA-US-6.4					
MA-US-7.1					
MA-US-7.2					
MA-US-7.3					
MA-US-7.4					
MA-NFR					
MA-NFR-1					
MA-NFR-3					
MA-NFR-5					
MA-NFR-6					
MA-NFR-8					
MA-NFR-9					
MA-NFR-10					
MA-NFR-11					
MA-NFR-12					

Recommended Additional Capabilities			
Respondents should identify any industry-standard capabilities, workflows, or service features that are not reflected in the attached Epics and User Stories but should be considered by the Purchaser			
Recommended Capability	Reason for Recommendation	Typical Implementation Approach	Relevant Product / Service Feature

Implementation, Operation, and Sustainment	
Respondents should describe how a comparable capability would typically be implemented, transitioned into service, operated, maintained, and upgraded. This should include key Purchaser responsibilities, key Contractor responsibilities, common dependencies, implementation risks, training considerations, and sustainment considerations	
Question	Response
Typical implementation duration for a comparable deployment	
Recommended implementation approach	
Recommended implementation phases	
Key Purchaser responsibilities during implementation	
Key Contractor responsibilities during implementation	
Common implementation risks and blockers	
Recommended training approach	
Knowledge transfer approach	
Data migration considerations	
Service transition considerations	
Upgrade and sustainment approach	
How the managed service would be monitored and reported (if applicable)	
How service quality, availability, and performance would typically be measured	

Configuration, Customization, and Integration	
Respondents should describe which capabilities can typically be configured by the Purchaser or Contractor, which changes would require vendor professional services, which changes would require custom development, and how customizations or integrations are maintained through upgrades. Respondents should also identify relevant APIs, connectors, import/export mechanisms, and integration patterns applicable to the proposed solution or service.	
Question	Response
Capability configurable by Purchaser administrators	
Capabilities configurable by the Contractor as part of the managed service	
Changes requiring vendor professional services	
Changes requiring custom development	
Whether customizations are preserved during upgrades	
Available APIs	
Available connectors or integrations	
Import / Export mechanisms	
Common integrations for similar implementations	
Integration limitations or constraints	
Approach to maintaining integrations over time	
Approach to security testing or validation of integrations	

Licensing, Renewal, and Support Model	
Respondents should describe the typical licensing, renewal, support, and service model for the proposed capability. This should include relevant licensing metrics, support tiers, software update arrangements, renewal model, optional modules or add-ons, and any separate costs for implementation, migration, training, integration, or sustainment.	
Question	Response
Typical licensing model	
Description of licensing model	
Minimum licensing quantities or term commitments	
Required modules, add-ons, or feature licenses	
Optional modules or add-ons	
Renewal model	
Support tiers available	
Software updates included	
Managed service costs included or separate	
Implementation costs included or separate	
Approach to maintaining integrations over time	

Yes	Not supported	Strong
No	Partial Support	Moderate
Partial	Requires Configuration	Limited
	Requires Customization	Not Supported
	Requires Integration	
	Recommend Alternative	
	Requires Clarification	
	Recoomment Revision	
	Recommend Removal	