NCIA Request for Information (RFI)

Red Team Mission Planning, Execution, and Debriefing (RT-MPEDS) system

RFI-42619136-RT

NCIA/ACQ/2026/07336
Tuesday, 07 July 2026

NCIA Request for Information (RFI)

To: **Industry Partners**

Subject: **Red Team Mission Planning, Execution, and Debriefing (RT-MPEDS) system**

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 comprehensive red team mission planning, execution, and debriefing system (RT-MPEDS). To that end, we are issuing the attached Request for Information (RFI) RFI-42619136-RT to solicit feedback from capable and interested industry partners.

2. This RFI is issued for planning 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, 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 and B) with a view to providing recommendations for improving performance outcomes, competition, and efficiency; and identifying any risks or concerns that should be considered during the planning phase.

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 Line Sigh, Senior Contracting Officer at RFI-42619136-RT@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:

Line Sigh
Digitally signed by Line Sigh
Date: 2026.07.07 16:25:44 +02'00'

Line Sigh
Senior Contracting Officer

Enclosure:

- Request for Information with Annexes A and B
- 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 the development of a comprehensive red team operations management system. This Request for Information (RFI) is issued solely for informational 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, and shaping the strategy for any future solicitation.

C. Background

1. NCIA requires a Red Team Mission Planning, Execution, and Debriefing (RT-MPEDS) system to manage the complete lifecycle of NATO red team operations, from initial planning through active execution to comprehensive debriefing and archiving. The RT-MPEDS system must integrate multiple specialized components that address specific phases of the red team operations lifecycle.

2. Current tooling in this domain is fragmented: planners rely on generic platforms with no Red Team context; operators use disconnected custom-built tools; debriefing is handled offline, resulting in loss of knowledge, Indicators of Compromise (IOC) reuse risk, and inadequate audit trails.

3. The RT-MPEDS system will support NATO's cyber defense capabilities by providing red teams with advanced tools for mission planning, real-time operations management, evidence collection, and comprehensive reporting, while ensuring operational security and compliance with NATO policies.

4. High-level Objectives:

1. Deliver an integrated, open-source platform that covers the full Red Team lifecycle: mission planning, execution, and debriefing.
2. Eliminate dependence on fragmented, generic tooling by providing purpose-built components with Red Team operational context.
3. Implement dual-control (four-eyes) security mechanisms for sensitive operations including Tool Vault access.
4. Ensure all intellectual property is fully owned by NCIA, with full source code access and no proprietary lock-in

5. Expected Outcome:
The target outcome is to use the information collected to develop our acquisition strategy for an upcoming procurement. The procurement will aim to establish a partner to deliver the required system with the following high-level components:

- Mission Planning Component: Provide comprehensive mission planning capabilities with automated infrastructure provisioning and configuration management.

- Mission Execution Component: Provide real-time operational management, monitoring, and collaboration capabilities during active red team engagements.
- Mission Debriefing Component: Enable comprehensive post-mission analysis, reporting, knowledge capture to improve future operations, archiving and auditing capabilities.
- Mission Debriefing Component: Enable comprehensive post-mission analysis, tracking of findings and remediation measures, reporting, knowledge capture to improve future operations, archiving and auditing capabilities.

The scope and initial requirements are further elaborated in Annex B, C and D.

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 **28 July 2026**.

b. Responses should be submitted in PDF, Word, and/or Excel format and must not exceed **15 pages**, including:

i. Response to questions in Annex A
ii. Analyse Annex B and C and give comments/feedback as explicitly mentioned in Annex D.

excluding:

i. Cover page
ii. Company brochures or product literature (if included)
iii. Attachments such as past performance references

c. Use the following subject line for submission

i. "Response to RFI-42619136-RT – [Company Name]"

d. 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. Line Sigh, Senior Contracting Officer

2. RFI-42619136-RT@NCIA.NATO.INT

Annex A – Questions to Industry

1. Respondents are encouraged to provide the following information in their response:

   a. **Company Information**
      i. Legal Business Name
      ii. Address
      iii. Website
      iv. Primary Point of Contact
      v. Email address

   b. **Technical Capability**
      i. Summary of relevant capabilities and past performance

   c. **Feedback and Recommendations**
      i. Responses to the following questions based on the scope and requirements established in Annex B-D listed, using the given table format:

No.	Question / Information Requested	Max. words	Supplier Response	Evidence / Attachment Reference (if applicable)
Business background and approach				
1	Describe your company profile, primary technical disciplines, and identify key personnel and their availability.	200 words		
2	State what percentage of the software development effort on an engagement of this scope and duration would be performed directly by your own employees, versus subcontracted. Identify any subcontracting partners you would expect to engage and the role they would perform.	200 words		
3	Describe your organization's experience designing and building software systems from the ground up. Confirm your organization's standard position on delivering all resulting source code, documentation, and intellectual property exclusively to the customer under an inner-source model, with no public release. Your organization is free to use open-source libraries, frameworks, or components during development.	200 words		
Software Development				
4	Provide a detailed case study where your team transformed a set of user needs into a secure, resilient production system. Describe the requirements process, architecture decisions, testing strategy,	450 words		

No.	Question / Information Requested	Max. words	Supplier Response	Evidence / Attachment Reference (if applicable)
	security assurance activities, production challenges, and measurable outcomes.			
5	Provide two to three examples of custom-built software systems — not resold, configured, or repackaged COTS products — that your organisation has designed and delivered for clients, ideally involving multiple independently deployable components, role-based access control, audit logging, or encryption. Provide links to public repositories, demonstrations, or other independently verifiable evidence where available.	450 words		
6	*Explain your approach for converting user stories into: Functional requirements, Non-functional requirements, Acceptance criteria, and Test cases.*	450 words		
7	Describe your organization's standard practices for secure software development — for example secure coding standards, code review, and dependency or vulnerability management — drawing on past projects involving sensitive or regulated data, in any sector.	450 words		
8	Describe the most safety-critical, mission-critical, or business-critical system your organization has delivered. Describe the system purpose, User population, Availability requirements, Security requirements, Verification approach.	450 words		
AI-Related development				
9	Describe any prior experience your organisation has building a software integration layer that connects an existing large language model (LLM) — open-source or self-hosted, not one your organisation trained or built — to another system or data source. Specifically describe how such a layer transferred data (e.g. logs) into the model, triggered downstream actions based on the model's output, and returned results to an end user. Provide verifiable evidence (links, examples) where available. Note: your organisation is not required to have trained, fine-tuned, or built an LLM itself — only to have integrated with one.	450 words		

No.	Question / Information Requested	Max. words	Supplier Response	Evidence / Attachment Reference (if applicable)
Ways of working				
10	Describe your proposed Agile development methodology: sprint cadence, customer involvement, review and acceptance milestone structure, and how you will manage classified requirements over the course of the contract.	450 words		
11	Describe a project where initial requirements were incomplete or ambiguous. How did you elicit requirements? What artifacts did you produce? How did requirements evolve?	450 words		
12	Describe your approach to component-level testing and user acceptance validation	450 words		
13	Sample user story (illustrative only, unrelated to the customer's actual requirements): "As a system administrator, I want to receive an alert when incoming data matches a defined condition, so that I can review the details and decide whether any follow-up action is needed." Describe how your team would break this user story down into sprint-ready tasks, including how you would handle the human review step before any action is taken. Alternatively, or in addition, provide a short code sample or a link to comparable past work illustrating your typical engineering approach.	450 words		
14	Provide sample deliverables (redacted if necessary): • Architecture document • Threat model • Test strategy • Requirements specification • Traceability matrix	450 words		
15	What would be your proposed high-level architecture, major building blocks and their interactions?	450 words		
Additional Questions or Concerns				
16	Please describe any Innovations or alternatives we should consider	200 words		
17	Please provide your estimated Rough Order Magnitude (ROM), including any assumptions upon which they are based	200 words		

No.	Question / Information Requested	Max. words	Supplier Response	Evidence / Attachment Reference (if applicable)
18	Please describe any risks, concerns, or barriers you foresee	200 words		
19	Please share your suggestions for risk mitigation or enhancing competition	200 words		

Annex B – Scope

The RT-MPEDS system shall deliver the following high-level components:

- Mission Planning Component: Provide comprehensive mission planning capabilities with automated infrastructure provisioning and configuration management.
- Mission Execution Component: Provide real-time operational management, monitoring, and collaboration capabilities during active red team engagements.
- Mission Debriefing Component: Enable comprehensive post-mission analysis, tracking of findings and remediation measures, reporting, knowledge capture to improve future operations, archiving and auditing capabilities.

The user roles and responsibilities that will rely on this system are as follows:

1. **Mission Planner Leader:** adds users to the platform with correct authorization and accountability; adds need to know/to execute permissions to users based on their mission roles
2. **Mission Planner:** gathers information about past/related missions and documents all information for current mission (Objectives, scope, timing, limitations, etc.) so that all stakeholders have a clear and shared understanding of the mission statement; establishes and fills in SITREP templates as red teaming operations progress; relies on an interactive, automated timeline of events and team actions that allows filtering based on major and minor actions and events; is able to look-up missions based on criteria like mission name, team members, IOCs, etc.; is able to assign permissions to who is able to view, add, modify, etc. mission information; can upload documentation associated with the mission; can generate and edit mission data for the Red Team Support and Execution team, who deploys needed infrastructure for the mission; has a mechanism to generate Rules of Engagement document for the mission; can provide documents for approval to the Mission Authority; can view both the red and blue picture of a mission, for a clear overview of the full mission terrain.
3. **Mission Authority:** signs Rules of Engagement, so the mission is authorized and the Mission Planner is aware of the approval.
4. **Red Team Support:** provisions and stages infrastructure for a Red Team operation using Infrastructure-as-Code (e.g., Ansible); workstations provisioned with Red Team tools, networks, C2, etc; is able to view IOCs that have been used in all missions; can access to a dashboard the status of all the C2; can create user accounts; can create and customize alerts, so when a component (service, container) is failing the Red Team Support can quickly act upon this. Configures and maintains the locally-deployed Large Language Model (LLM) in support of the Red Team Operators during mission execution.
5. **Red Team Leader:** has access to a dashboard that provides real-time information about the mission, as well as the status and availability of the mission C2; has access to all objectives in order to distribute the objectives/tasks to Red Team Operators; is able to archive all the data related to a mission in a secure way; is able to see and search IOCs that have been used in all missions; is able to export the situational awareness data for offline work; is able to share information securely with the Red Team Operators, this includes: file sharing, chat, video, reporting, project management, wiki); can assign permission to push/pull tools/scripts in the secure Tool Vault, so that a 4-Eyes principle is applied; can use the staged infrastructure to lead the execution of the Red Team Operation.
6. **Red Team Operator:** can share information securely with the Red Team Operators and the Red Team Leader, including: file sharing, chat, video, reporting, project management, wiki); can store and access the tools/scripts in a secure Tool Vault

protected by at least two keys owned by different people, so that the 4-Eyes principle can be applied; can access a knowledge base for information about past missions and preparations; Can create and customize alerts for C2 components; Can use the staged infrastructure to execute the Red Team Operation.

7. **Mission Debriefing Operator:** can create report templates and send completed reports to stakeholders; can capture and keep documented lessons learned from each operation
8. **Mission Planner Auditor:** can see all the Mission Planning logs; can unarchive a Mission Execution archive; review all the IOCs that have been used during a mission.

The system must also maintain strict security controls between red team operation and across different classification levels.

Deliverables:
The RT-MPEDS system must integrate multiple specialized components while maintaining strict security controls across different classification levels. The RT-MPEDS system establishes a NATO-owned, unified, inner source[1] red team platform. It will support NATO's cyber defence capabilities by providing red teams with advanced tools for mission planning, real-time operations management, evidence collection, and comprehensive reporting, while ensuring operational security and compliance with NATO policies.

The following components are in scope of this delivery:

Deliverable	Description	Frequency	Format
Mission Planning Component (SWR-PLN)	Fully functional mission planning software module covering mission creation, RoE workflow, event timeline, IOC search, and mission data package generation	One-time	inner-source software
Mission Execution Component (SWR-EXE)	Fully functional mission execution software module covering dashboards, Tool Vault, collaboration environment, IOC registry, C2 monitoring, screen cast, and operational closure package generation	One-time	inner-source software
Mission Debriefing Component (SWR-DEB)	Fully functional debriefing module covering report templating, stakeholder distribution, lessons learned, and auto-population from imported operational data package	One-time	inner-source software
IaC Provisioning Framework	Ansible-based (or equivalent) infrastructure provisioning tooling consuming mission data packages to deploy operator workstations, collaboration backend, mission networks, and C2 servers	One-time	inner-source software / scripts
Offline AI Decision Support Module	Locally-deployed LLM integration within the Mission Execution Component, providing Red Team Operators with AI-assisted reconnaissance analysis, attack path suggestions, and operational decision support, fully operational in air-	One-time	inner-source software

[1] "Inner source applies open source principles within an organization, while open source involves public collaboration on software projects." Inner source = open source but only within an org.

Deliverable	Description	Frequency	Format
	gapped environments		
System Requirements Specification (SRS) (final)	Agreed and baselined SRS reflecting any scope changes at contract award	At contract award	Document (.docx / .pdf)
Architecture & Design Documentation	Technical design, component interface specifications, and data flow documentation	At delivery milestones	Document
Test & Validation Reports	Results of functional acceptance testing against requirements	Per milestone	Report
User & Administrator Training Materials	Role-based training documentation for all stakeholder roles	At delivery	Document
Source Code Repository	Complete source code with full version history, human-readable and customer-owned	Continuous	Git repository

New user stories, features, or enhancements that are proposed during delivery are recorded in a product backlog rather than automatically added to the current scope.

Annex C - Requirements

The following is a non-exhaustive list of requirements.

a. Software requirements of the Mission Planning Component:

- Granular Role-Based Access Control (RBAC) capability
- Live Mission recording and archiving function into a structured mission data form allowing Mission Planners to record and maintain live mission information including objectives, scope, timing, limitations, and all other relevant parameters
- Search capability supporting filtering by criteria including mission name, assigned team members, and Indicators of Compromise (IOCs) for Mission Planners Auditors to search and review all IOCs used during any given mission, enabling substantiated responses to Blue Team inquiries regarding Red Team activity attribution
- Compartmented document library for each mission
- Rules of engagement (RoE) creation and validation tool including a validation workflow through mission leadership for each mission
- Support for electronic digital signature of the RoEs by designated authorities, and support for manual recording of RoEs approvals signed via paper or alternative out-of-system means
- Creation of Situation Reports (SITREP) templates that automatically pulls live mission data and supports manual import of situational awareness data exported by the Red Team Leader from the Mission Execution component, enabling rapid situation reporting in both connected and offline scenarios
- Generate and edit structured mission data packages for the Red Team Support and Execution teams, containing all information required to deploy and operate mission infrastructure
- Dashboards displaying a combined red and blue operational picture, providing Mission Planners with a comprehensive overview of the mission terrain from both offensive and defensive perspectives
- Generate structured mission data packages for the Red Team Support and Execution teams, containing all information required to deploy and operate mission infrastructure

b. Software requirements of the Mission Execution Component:

- Automated mission events' timeline with filtering function according to event's severity factor, enrichable by the operators with evidence management.
- Searchable, cross-mission IOC registry accessible to authorized Red Team Support and Red Team Leader personnel, enabling verification that no IOC is reused across different missions
- Real-time mission dashboard displaying current scope, objectives, and mission status at all times during an active operation
- Mapping of timeline events to the mission objectives to present to the Mission Leader a workflow of technical actions supporting an objective.
- Encrypted archive containing all mission-related data with decryption access restricted exclusively to selected personnel holding the appropriate keys
- Export functionality for situational awareness data in a structured format importable by the Mission Planning component, supporting offline and disconnected operation scenarios
- Secure, integrated team collaboration environment accessible to Red Team

Leaders and Red Team Operators, encompassing file sharing, real-time chat, video conferencing, operational reporting, project management, and wiki capabilities
- Secure Tool Vault for the storage and retrieval of tools and scripts, enforcing a four-eyes (dual-control) approval principle whereby Red Team Leaders authorize push and pull access, and tools are protected by at least two keys owned by different individuals
- Knowledge base for Red Team Operators containing mission preparation documentation and historical operational information from previous missions
- Consolidated, real-time C2 status dashboard giving immediate visibility into the availability and health of all deployed C2 infrastructure components for Red Team Support and Red Team Leader, including customizable C2 component-level alerts, providing immediate notification when beacons become active, go silent, or experience failures
- Offline LLM capability: Implement integration with offline, locally-deployed Large Language Models to assist with real-time reconnaissance analysis, attack path suggestions, operational decision support and automated timeline augmentation.
- Video casting capability from the Red Team Operator screen session to the OPS room video wall, without requiring action from the operator, and controlled by the Red Team Leader

c. Software requirements of the Mission Debriefing Component:
- Tool allowing the creation, editing, and management of customizable report templates according to destination stakeholders and audience, including an integrated final report distribution feature
- A lesson learned capturing tool from the Mission Execution Component that enables follow-up actions and long-term institutional knowledge retention

d. Additional requirements
- **System integration across all components**, including structured inter-component data exchange interfaces supporting both connected and air-gapped operating scenarios.
- **Full delivery of human-readable, customer-owned source code** in a version-controlled repository (e.g. GitHub).
- **Cybersecurity / secure-by-design support.** The solution shall be engineered and maintained following secure-by-design practices. The Contractor shall:
  - Provide evidence of secure development lifecycle and vulnerability management practices;
  - Support NCIA security assurance activities, including cooperation during NCIA security testing (including penetration testing);
  - Commit to remediation of Critical/High/Medium findings within agreed timeframes as part of acceptance and throughout operations.
- **Air-gap & Autonomous Operation:** The Mission Execution Component shall operate in full autonomous, air-gapped mode with no runtime dependency on external connectivity or on any other RT-MPEDS component.
- **Use of AI/LLMs:**
  - The locally deployed LLM shall produce a response to operator queries within an acceptable latency threshold under operational load conditions, to be defined in the agreed acceptance criteria.
  - The LLM shall be provided on dedicated hardware without requiring Internet access for model download, or runtime operation.
  - Access to the LLM shall be restricted to authorized Red Team Operators,

Red Team Support, and Red Team Leaders, enforced by the platform RBAC.

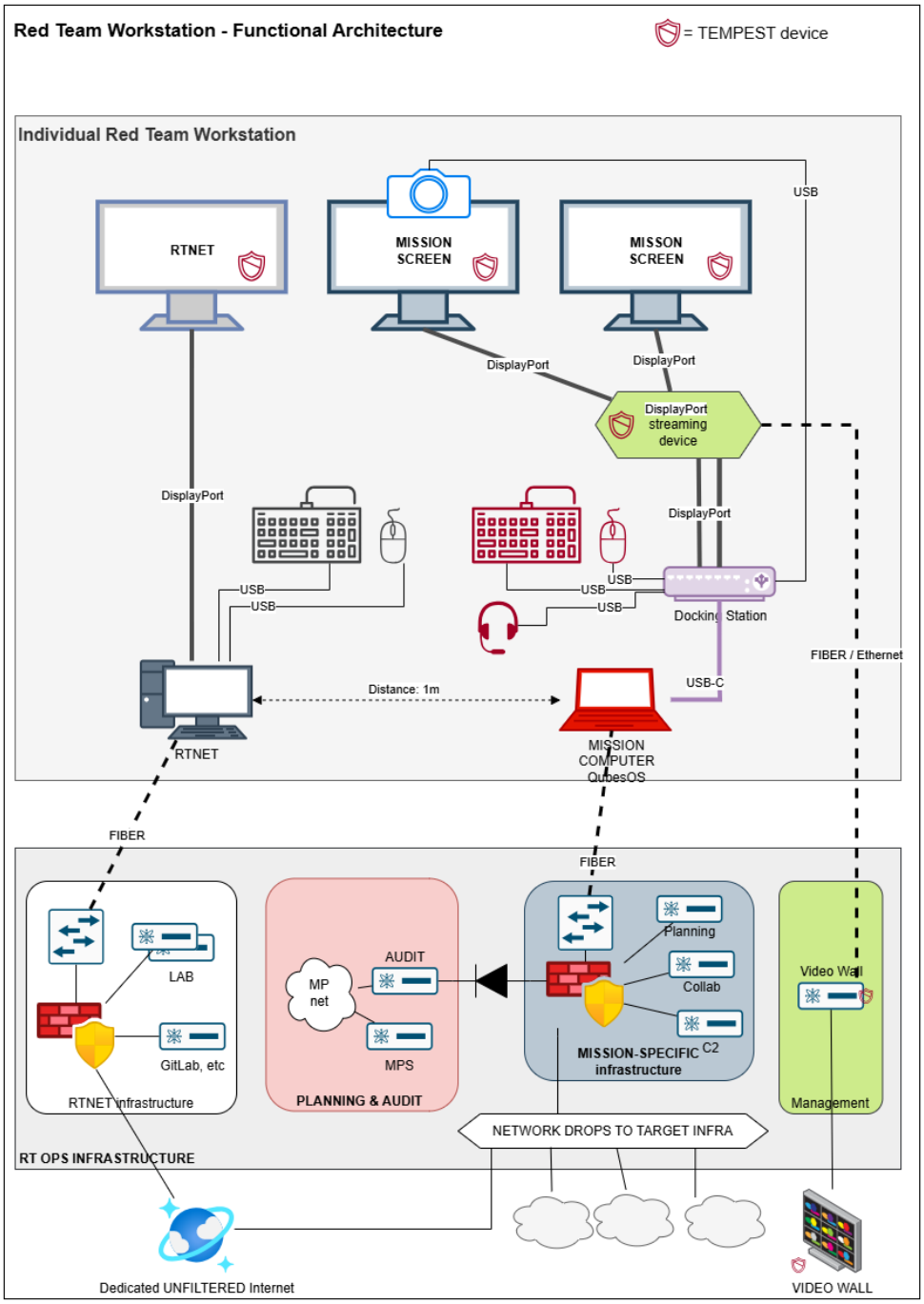
- **Infrastructure Provisioning:**
  - The IaC provisioning pipeline shall enable repeatable, version-controlled, and auditable deployment of the full Mission Execution Component infrastructure from a single mission data package, without manual transformation.
- **Audit & Logging:** Audit logs shall be tamper-evident, protected against unauthorized access and modification, and shall support search and filter by user, action type, and UTC timestamp across all components.
- **Modularity & Updatability**: All software components shall be independently deployable and updatable without requiring simultaneous redeployment of other components.
- **Quality & Acceptance:** All deliverables shall meet quality standards as defined in the agreed acceptance criteria and be accompanied by test evidence demonstrating compliance with all shall-level requirements provided at contract award.
- **Source code & Intellectual Property:** Source code shall be human-readable, well-documented, and delivered in a version-controlled repository owned and controlled by NCIA throughout the contract period and following contract conclusion.

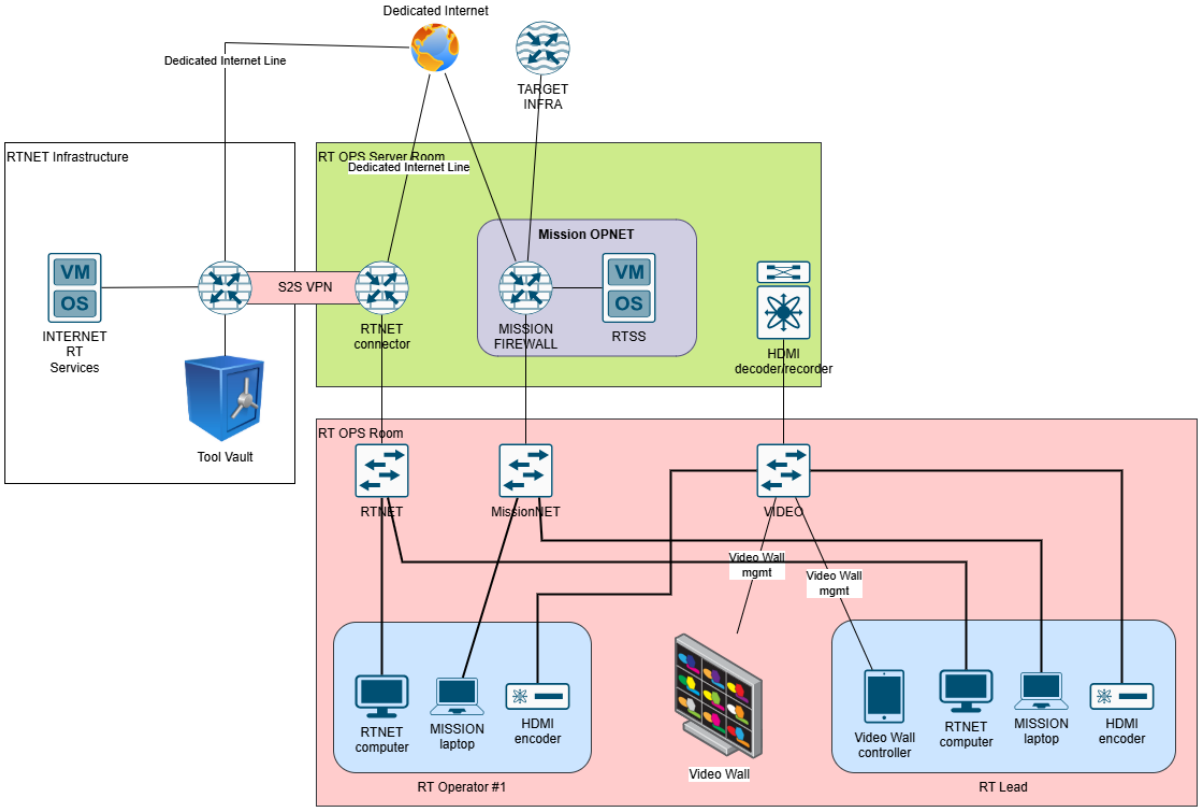
Purchaser Furnished Equipment (PFE) / Information (PFI)

a. Existing Red Team operational policies, classification guidelines, and access control policy documentation.
b. OPS room physical layout drawings and network topology specifications for integration planning purposes.
c. Stakeholder role definitions and representative user stories for acceptance testing.
d. IT security standards and compliance requirements applicable to the platform.

Annex D – Notional high-level diagrams

The following diagrams illustrate how the Red Teaming solution could be built. NATO is interested in industry feedback on this architecture approach including modifications or alternative approaches.




Dedicated Internet
Dedicated Internet Line
TARGET INFRA
RTNET Infrastructure
RT OPS Server Room
Dedicated Internet Line
Mission OPNET
VM
OS
INTERNET RT Services
S2S VPN
RTNET connector
MISSION FIREWALL
VM
OS
RTSS
HDMI decoder/recorder
Tool Vault
RT OPS Room
RTNET
MissionNET
VIDEO
Video Wall mgmt
Video Wall mgmt
RTNET computer
MISSION laptop
HDMI encoder
RT Operator #1
Video Wall
Video Wall controller
RTNET computer
MISSION laptop
HDMI encoder
RT Lead