Science and Technology Organization
Centre for Maritime Research and Experimentation
La Spezia – Italy

Request For Quotation

RFQ CMRE-26-012

Remedial Action for CMRE CCTV Network Infrastructure

Thursday, 18 June 2026

Contents

Part I Bidding Instructions

1 General

1. This Request for Quotation (RFQ) intends to solicit quotes for the Remedial Action of the CMRE CCTV Network Infrastructure, at the NATO Science and Technology Organization - Centre for Maritime Research and Experimentation (CMRE) located in La Spezia, Italy.
2. The objective is to identify a qualified contractor to carry out remedial works on the existing CCTV network infrastructure in order to improve the security, manageability, and resilience of the system. The contractor shall provide all labour, materials, equipment, configuration support, testing, and documentation necessary to complete the activities described in Part II Statement of Work (SOW).
3. This solicitation is expected to result into a Firm Fixed Price services type contract in accordance with the (CMRE) Terms & conditions; Contract award is contingent upon funding availability; Partial bidding is not allowed.
4. STO-CMRE Standards Terms & Conditions dated May 2026 are applicable to this procurement and can be viewed and/or downloaded from the CMRE website at www.cmre.nato.int/general-information.

2 Classification

1. This Request For Quotation (RFQ), as well as the prospective resulting contract - are NATO UNCLASSIFIED documents. Some information concerning the CCTV network are classified at NATO RESTRICTED level.
2. The Contractor shall comply with instruction reported in the “Security Aspect Letter” and in the ‘’Contract Security Clause’’ in Part III.

3 Definitions

1. The term “Bidder” shall refer to the bidding entity that has completed a bid in response to this RFQ.
2. The term “Contracting Authority’’ or ‘’Contracting Officer” (CO) designates the official who executes this RFQ and will award and administer the resulting contract on behalf of the CMRE.
3. “Contracting Officer`s Technical Representative” or “COTR” is the official who is appointed by the CO to assist in the technical management and day-to-day supervision of the resulting contract.
4. The term “Contractor” shall refer to the bidding entity to whom the contract is awarded.
5. The term “day(s)” as used in this RFQ shall, unless otherwise stated, be interpreted as meaning calendar days.
6. The term “NATO” shall refer to the North Atlantic Treaty Organisation.
7. The “Prospective Bidder” shall refer to the entity that has indicated thereon its intention without commitment, to participate in this RFQ.
8. The term “CMRE” shall refer to NATO Science & Technology Organisation – Centre for Maritime Research and Experimentation.

4 Eligibility

This RFQ is open to governmental or commercial entities:

1. Established in a North Atlantic Treaty Organisation Alliance member nation.
2. Working in the required field and legally authorised to operate in the country or countries in which this contract is to be performed at the time of bidding.
3. Has the required prior experience and past performance including size, cost and scope.
4. All proposed personnel on this requirement must be citizens of a NATO member nation.

5 Duration of the Contract

1. The contract awarded shall be effective upon date of award.
2. Period of Performance: The works must start no later than 20 calendar days from date of contract award and must be completed no later than 6 calendar weeks from date of contract award.

6 Exemption of Taxes

All prices and rates quoted shall be exclusive of any taxes and duties from which STO-CMRE is exempt pursuant to the provisions of "Agreement on the status of the North Atlantic treaty Organization, National Representatives and International Staff" (Ottawa Agreement), Articles IX and X and the Italian law ART. 72 of the D.P.R. 26/10/1972 n. 633 and subsequent modifications.

7 Amendment or Cancellation of the Solicitation

1. CMRE reserves the right to amend or delete any one or more of the terms, conditions, or provisions of the RFQ prior to the date set for bid closing. A solicitation amendment or amendments shall announce such action.
2. CMRE reserves the right to cancel, at any time, this RFQ either partially or in its entirety. No legal liability on the part of CMRE shall be considered for recovery of costs in connection to bid preparation. All efforts undertaken by any bidder shall be done considering and accepting, that no costs shall be recovered from CMRE.

8 Bidders conference, site visit and requests for clarifications

1. In case of perceived ambiguities found in this solicitation, Prospective Bidders shall seek clarification at their earliest convenience. Any explanation regarding the meaning or interpretation of this RFQ, terms, clauses, provisions or specifications, shall be requested in writing from the Contracting Officer. The Contracting Officer must receive such requests for clarification no later than 5 (five) working days prior to the bid closing date.
2. **Bidders' conference & site visit**: a mandatory bidders conference and site visit will take place on **Tuesday 30 June, at 10:00 hrs local time**. Interested prospective bidders must confirm their participation by sending an email to Contracting@cmre.nato.int no later than 25 June 2026, 10:00 hrs local time.
3. Prospective Bidders are invited to inspect the site where the works will be performed and to satisfy themselves regarding all general and local conditions that may affect the cost of contract performance, to the extent that the information is reasonably obtainable.
4. Information in response to inquiries / requests for clarification to a prospective bidder shall be furnished to all prospective bidders by e-mail. All addendums and any necessary solicitation amendment(s) shall be incorporated into this RFQ. Oral Interpretations shall not be binding.

9 Bid Closing Date

1. Bids shall be submitted by **09.00 hours, local time, 27 July 2026**. Bids received after the stated date and time, will not be considered.
2. Send bids via e-mail as Adobe® .pdf file(s) to: Contracting@cmre.nato.int

NOTE: Please DO NOT send your bid to any other e-mail address otherwise your bid may be determined non-compliant with this RFQ.

10 Bid Validity

Bids shall remain valid for a period of thirty (30) days from the applicable closing date set forth within this RFQ. CMRE reserves the right to request an extension of bids' validity. Bidders shall be entitled to either grant or deny this extension of bids' validity. If the Bidder declines to extend the validity period, CMRE may treat the bid as withdrawn.

11 Content of Quotations

The entire quotation shall be split in 2 packages:

1. The Financial quotation containing :
    a. Price Quotation (schedule of prices Annex 4 for Price quotation).

2. Admin and Technical quotation containing:

    a. Compliance statement (See Annex 2)
    b. Past performance (See Annex 3): Bidders shall cite at least one past performance based on contracts held within the last five years that are of similar size and scope, financial magnitude and complexity to the tasks, activities, and deliverables detailed in the SOW.
    c. Technical Compliance matrix (See Annex 5).

12 Quotation Submission

1. Quotations shall be submitted electronically in two separate PDF documents; one containing the Admin/Technical submittals and one containing the Financial Quotation, to: Contracting@cmre.nato.int
2. Email subject shall include the solicitation number along with company name (for example: RFQ CMRE-26-012_Tech_ABC Inc. / RFQ CMRE-26-0012_FIN_ABC Inc.). Allow sufficient time in your submission should you encounter email size challenges or else.
3. Price quotations shall be in EURO (€) currency.
4. Prices shall be on a Firm Fixed Price Basis and include any relevant discount schedule.
5. No oral bids or oral modifications or telephonic bids will be considered.
6. It is the ultimate responsibility of a prospective bidder to ensure that all quotation submissions are reviewed for compliance in order to meet the RFQ required technical, contractual and administrative specifications.

13 Late Quotations

1. It is solely the bidder's responsibility to ensure that the quotation reaches CMRE prior to the established closing date and time. Only if it can be unequivocally demonstrated that the late arrival of the quotation package was the result of NATO staff negligence (mishandling) shall the bid be considered, as long as it is received before an award is made.
2. A delay in email exchange due to the server or size restrictions does not constitute a delay attributable to NATO.

14 Quotation Withdrawal

A bidder may withdraw their quotation up to the date and time specified for bid closing. Such a withdrawal must be communicated in writing via email addressed to the CMRE Contracting Officer.

15 Quotations Evaluation

1. The evaluation of quotations and determination as to the responsiveness and technical adequacy or technical compliance of the products or services requested, shall be the responsibility of CMRE. Such determinations shall be consistent with the evaluation criteria specified in the RFQ.
2. CMRE is not responsible for any content that is not clearly identified in any quotation package.
3. Quotations shall be evaluated and awarded based upon the **lowest priced, technically compliant bid**. The following factors will be considered:
    a. Successful administrative submission of bid packages as requested in paragraph 11.
    b. Successful determination of Technical Compliance. An offer will be considered technically compliant if it clearly confirms, as a minimum, the following:
        i. Past performance (See Annex 3): Bidders shall cite at least <u>one</u> past performance based on contracts held within the last five years that are of similar size and scope, financial magnitude and complexity to the tasks, activities, and deliverables detailed in the SOW.
    c. Acceptance of RFQ's Terms and Conditions (see Annex 2).

16 Quotations Clarification

During the entire evaluation process CMRE reserves the right to discuss any bid in order to clarify what is offered and interpretation of language within the bid to resolve potential areas of concern. In no case will Bidders be allowed to change their price bid.

17 Award

1. CMRE intends to award a firm fixed price contract to the Bidder whose quotation represents the Lowest Priced Technically Compliant offer to NATO.
2. CMRE reserves the right to negotiate minor deviations to the listed terms and conditions to this RFQ, if/as required.

18 Communications

All communication related to this RFQ, between a prospective bidder and CMRE shall only be through the CMRE Contracting Officer. Designated contracting staff shall assist the CMRE Contracting Officer in the administrative process. There shall be no contact with other CMRE personnel regarding this

RFQ. Such adherence shall ensure Fair and Open Competition with equal consideration and competitive footing leverage to all interested parties.

19 CMRE Point of Contact

All correspondence and enquiries relevant to this RFQ, shall be addressed to the CMRE Contracting Office at the following email address: Contracting@cmre.nato.int

Part II Statement of Work

1. Introduction

NATO CMRE located in La Spezia, Italy requires a qualified contractor to carry out remedial works on the CCTV network infrastructure in order to improve the security, manageability, and resilience of the system. The contractor shall provide all labour, materials, equipment, configuration support, testing, and documentation necessary to complete the following activities. Additional details and existing CCTV Network diagram will be available for consultation at CMRE premises.

2. Scope of Work

2.1 Switch Replacement

- Replace all five switches with suitable, supported and managed models (Cisco Catalyst 1300 series or equivalent, subject to CMRE approval) taking into consideration specifics needs for each location (e.g. number of interfaces, PoE power budget).
- Install suitable physical security measures for the racks hosting CCTV network across CMRE buildings.

2.2 Network Hardening

- Apply network security hardening to the newly installed switches to match the configuration described in the Cisco Switches NATO Security Guide (PASEP). The networking configuration must comply with this configuration and pass an audit as documented in the Cisco Switches NATO Security Guide Appendix B.
- Apply hardening to the workstation connected to the CCTV network, including disabling all additional unnecessary services that increase the attack surface and are not required for operational use.

2.3 Testing and Validation

- Verify correct operation of the CCTV network following replacement and hardening activities.
- Confirm that CCTV connectivity, management access, and system functionality are restored and operating correctly.

2.4 Documentation

- Update all relevant CCTV network documentation, including network diagrams, equipment inventory, IP addressing, switch configuration details, rack/cabinet locations, and hardening measures applied.
- The contractor shall ensure that all works are carried out by suitably qualified personnel, in accordance with applicable security, safety, manufacturer, and CMRE site requirements. Upon completion, the contractor shall provide a service report including actions performed,

equipment installed or replaced, configuration changes, test results, full configuration backups of all deployed switches and any recommendations for further improvement.

3. Security Aspects

Some information concerning the CCTV network are classified at NATO RESTRICTED level. The Contractor shall comply with instruction reported in the “Security Aspect Letter” and in the Contract Security Clause (Part III).

Part III Special Provisions & Clauses

1. Security Aspects Letter (SAL) [Handling NATO RESTRICTED]

1. In the performance of this contract, the prime Contractor and any Sub-contractor(s) are required to comply with NATO security regulations as implemented by the NSA/DSA of the nation in which the Company is registered/located and as established in the attached Contract Security Clause (**Security Classification Check List** provided separately after contract award).

2. All NATO Classified Information (NCI) shall be protected in accordance with the requirements established by the NSA/DSA of the nation in which the Company is registered and its premises are located and as established in the attached Contract Security Clause.

3. In particular, the Contractor shall:

   a) Appoint an officer to be responsible for supervising and directing security measures in relation to the Request for Proposals (RFP), contract or sub- contract;
   b) submit in due time to the related NSA/DSA the Facility Security Clearance (FSC) request and personal particulars of the person the contractor wishes to employ on the project with a view to obtaining NPSCs at NR level, only if required by the related NSA/DSA;
   c) maintain, preferably through the appointed officer/manager responsible for the security measures, a continuing relationship with the NSA/DSA and the Contracting Authority in order to ensure that all NATO classified information involved in the bid, contract or sub-contract is properly safeguarded;
   d) limit the copying/duplication of any classified materiel (including documents) to the absolute minimum to perform the contract;
   e) supply the NSA/DSA, when so requested by the latter, with any information on the persons who will be required to have access to NATO Classified Information;
   f) maintain a record of employees taking part in the contract/project and who have been cleared for access to NATO Classified Information. This record must show the period of validity and the level of the clearances, when required by the related NSA/DSA;
   g) deny access to NATO classified information to any persons other than those authorised to have access by the NSA/DSA or, when such authorization is not required for NR information access only, as determined by the need-to-know;
   h) limit the dissemination of NATO classified information to the smallest number of persons as is consistent with the proper execution of the contract or sub- contract;
   i) comply with any request that persons to be entrusted with NATO classified information sign a statement undertaking to safeguard that information and signifying their understanding of their obligations under national legislation on the safeguarding of classified information, and that they recognise that they may have comparable obligations under the laws of the other NATO nations in which they may have access to classified information;
   j) report to the NATO STO CMRE Security Officer and to the NSA/DSA of the nation in which the Company is registered/located any breaches or suspected breaches of security, suspected sabotage or subversive activity, any breach giving rise to doubts as to the trustworthiness of an

employee, any changes in the ownership, supervisory or managerial staff of the facility or any changes that affect the security arrangements and security status of the facility, and any other information which may be required by the NSA/DSA, such as reports on holdings of NATO classified information or materiel;

k) immediately notify NATO STO CMRE Security Officer of any actual or suspected compromise/loss of NCI, any actual or suspect cyber security incident, relevant to this Contract;
l) obtain the approval of NATO STO CMRE and related NSA/DSA before beginning negotiations with a view to sub-contracting any part of the work which would involve the Sub-contractor having possible access to NATO classified information, and to place the Sub-contractor under appropriate security obligations which in no case may be less stringent than those provided for his own contract;
m) undertake not to utilise, other than for the specific purpose of the bid, contract or sub-contract, without the written permission of NATO STO CMRE, any NATO classified information supplied to the contractor, and return to NATO STO CMRE all classified information referred to above, as well as that developed in connection with the contract or sub-contract, unless such information has been destroyed, or its retention has been duly authorised by the contracting office or the sub-contracting officer. Such NATO classified information shall be returned at such time as the contracting office may direct; and
n) comply with any procedure established with respect to the dissemination of NATO classified information in connection with the contract or sub-contract.

4. Any person taking part in the performance of work the classified parts of which are to be safeguarded must possess the appropriate NATO security clearance issued by his NSA/DSA, when required by their national law.

5. Unless specifically authorised to do so by NATO STO CMRE (and the NSA/DSA of the nation where the Contractor/Company is registered, as applicable), the Contractor may not pass on any NATO classified information to any third party to whom a request to supply goods or services has been submitted.

6. No change in level of classification or de-classification of documentation or materiel may be carried out unless written authority in this respect is obtained from NATO STO CMRE.

7. No CIS may be used for processing classified information without prior accreditation by the responsible authorities. At the level of NR, such accreditation will be in accordance with the attached Contract Security Clause.

8. Failure to implement these provisions and the security regulations established by the NSA of the nation in which the Company is registered/located may result in termination of this contract without reimbursement to the Contractor or claim against NATO, NATO STO CMRE or the national government of the said nation.

9. After contract award, the Contracting Authority will provide a **Security Classification Check List** that indicates the degree of classification of the data and materiel (equipment, information, technical manuals, and specifications) which may be handled in the performance of work under this contract and which shall be safeguarded in accordance with the provisions of this letter.

10. The contractor shall destroy or return any classified information provided or generated under the contract unless the contracting authority has given written approval to retain such classified information, e.g. for warranty purposes.

11. The **Bidder/Contractor shall acknowledge receipt of this SAL** (and any additional Security Instruction made part of the contract) and confirm that it understands and will comply with the security aspects defined. With respect to contracts involving only NR information, the **Bidder/Contractor shall also be required to confirm that it will comply with the provisions of the Contract Security Clause** and specifically that any company CIS used to handle or process NR classified information has been appropriately security accredited.

2. Contract Security Clause for Inclusion in Tenders and Contracts Involving NATO RESTRICTED INFORMATION

INTRODUCTION

1. This contract security clause is published by the Security Committee (AC/35) in support of NATO Security Policy, C-M (2002)49, and its supporting directives.

BACKGROUND

2. This contract security clause contains rules and regulations that shall be applied by the Contractor addressing the minimum security requirements for the protection of NATO RESTRICTED (NR) information received or produced by it as a result of the contract.

This security clause addresses all aspects of security (personnel security, physical security, security of information, Communication and Information System (CIS) Security, and industrial security) that the Contractor is required to implement.

3. This contract security clause forms part of the contract and shall provide direction to ensure compliance by Contractors on the protection of NR information.

SECTION I - RESPONSIBILITY

4. Contractors handling and/or storing NR information shall appoint an individual of suitable seniority who shall act as the Security Officer (SO) of the facility with responsibility for ensuring the protection of NR information in compliance with the provision of this security clause and any other additional requirements advised by the Contracting Authority. The SO shall also act as the point of contact with the Contracting Authority or if applicable with the National Security Authority (NSA) or Designated Security Authority (DSA).

SECTION II - PERSONNEL SECURITY

5. A Personnel Security Clearance (PSC) is not required for access to information classified NR. Individuals who require access to NR information shall be briefed on security procedures and their responsibilities by the nominated SO, have a need-to-know and acknowledge in writing that they fully understand their security responsibilities and the consequences if information passes into unauthorised hands either by intent or through negligence. A record of the acknowledgement of responsibilities by Contractor's employees shall be retained by the facility security officer.

SECTION III - PHYSICAL SECURITY

6. NR information shall be stored in a locked container that deters unauthorised access; such as a locked desk or cabinet, or in a room or area to which access is controlled (hereinafter referred to as Administrative Zone4).
7. NR information shall be handled in Administrative Zones or held under personal custody.

SECTION IV - SECURITY of INFORMATION

Control and Handling

8. Unless a NATO Nation has specifically mandated contractors under their jurisdiction to do so, NR information is not required to be individually recorded or processed through a Registry System.

Access

9. Access to NR information shall be granted only to personnel involved in the contract who fulfil the conditions according to Paragraph 5, second sentence.

Reproduction

10. Documents, extracts, and translations of information classified NR may be reproduced by individuals authorised for access to the information and on equipment with controlled access.

Destruction Requirements

11. NR information shall be physically destroyed in such a manner that ensures it cannot be reconstructed in full or in part.

12. Destruction of reproduction equipment utilising electronic storage media shall be in accordance with the applicable requirements in section VI.

Packaging

13. Information classified NR shall, as a minimum, be transmitted in a single opaque envelope or wrapping. The markings on the package shall not reveal that it contains information classified NR.

Carriage/ Movement within a Contractor's Facility

14. NR information carried within the perimeter of the site or establishment shall be covered in order to prevent observation of its contents.

National/International Transmission

15. The carriage of NR material shall as a minimum be in a single opaque envelope or packing (no marking shall be visible on the outer envelope) and may be:

(a) moved by postal or commercial services;
(b) carried by Contractor's personnel; or
(c) transported as freight by commercial services.

Release

16. NR shall not be released to entities not involved in the contract without the prior approval of the contracting authority.

Security Incidents

17. Any Incident, which has or may lead to NR information being lost or compromised shall immediately be reported by the SO to the Contracting Authority.

SECTION V - SUB-CONTRACTING

18. Sub-contracts shall not be let without the prior approval of the Contracting Authority.

19. Sub-contractors shall be contractually obliged to comply with the provisions of this document and any other additional security requirements issued by the Contracting Authority.

Notification of Contracts

20. Contractors/Sub-contractors under the jurisdiction of a NATO Nation requiring by their national laws and regulations notification of contracts involving NR shall notify their NSA/DSA about any such contracts they have been awarded.

International Visits

21. Visits involving NR information will be arranged directly between the SO responsible for the visitor and the SO of the facility to be visited without formal requirements. The SO of the facility to be visited should be asked if a request for visit is required to be provided to its NSA/DSA and if so, the SO of the facility to be visited should submit a visit request to its NSA/DSA on behalf of the visitor. However, visitors are not required to hold a PSC.

SECTION VI - HANDLING OF NATO RESTRICTED INFORMATION ON INFORMATION AND COMMUNICATION SYSTEMS (CIS)

Security Accreditation of Communication and Information Systems (CIS)

22. CIS used within national industrial facilities to handle NATO classified information shall be accredited by the respective national Security Accreditation Authorities or their delegated SAAs, ensuring that the NATO's minimum security standards are met. The security accreditation of CIS handling NR information may be delegated to Contractors according to national laws and regulations.

23. This contract security clause contains the rules and regulations that shall be applied by the contractor's SO or other appropriate officer to address and satisfy the minimum security requirements for the protection of NR information received or produced by the contractor as a result of the contract. This clause includes specific provisions to be satisfied by the contractor for the accreditation of the contractor's CIS handling NR information. The contractor shall provide the Contracting Authority with a written statement of compliance confirming that its CIS has been accredited in compliance with the minimum requirements specified below. This written statement may be included in the contractor's response in acknowledgement of the receipt and requirements of the Security Aspects Letter associated with the contract.

24. It is the responsibility of the contractor to implement these minimum security requirements when handling NR on its CIS.

25. The SO shall assess and verify the compliance of the CIS over its entire life-cycle, in order to ensure that it continues to be consistent with the requirements of this document.

26. The following describes the minimum security requirements for handling NR information on contractors' CIS that shall be met:

26.1 Identity & Access Management
26.1.1. An up-to-date list of authorised users shall be maintained by security management staff.
26.1.2. Credentials shall be established and maintained to identify authorised users.

26.1.3. Users shall themselves authenticate to, and be authenticated by, the system before any access to the CIS will be granted.
26.1.4. Passwords shall be a minimum of 12 characters long and shall include numeric and “special” characters (if permitted by the system) as well as alphabetic characters;
26.1.5. Passwords shall be changed at least every 12 months. Passwords shall be changed as soon as possible if they have, or are suspected to have been compromised or disclosed to an unauthorised person.
26.1.6. Password reuse is prohibited for 10 generations (i.e. users cannot re-use their last 10 passwords on a system). Password shall be unique and never be reused on other systems/accounts.
26.1.7. The system shall provide only limited feedback information to the user during the authentication process.
26.1.8. Accounts that are no longer required shall be deleted.
26.1.9. When the authentication of the person is not enforced by physical security measures surrounding the location where the system is installed (e.g. perimeter/building security) or by non-technical security measures surrounding the office areas where components of system are located (e.g. server rooms, user workstation areas), two-factor authentication shall be used.

26.2 Access Control
26.2.1. The identification and authentication data shall be used by the system to determine user privileges, in accordance with the access control requirements set out in the security-related documentation.
26.2.2. From the user account only, it shall be possible for the security management staff to identify the specific user and/or roles.
26.2.3. Mechanisms shall be implemented to restrict access to only that information to support a given project or contract, taking into account the need-to-know principle.
26.2.4. Access to security and system information shall be restricted to only authorised security and system administrators.
26.2.5. Access privileges shall be implemented to restrict the type of access that a user may be permitted (e.g., read, write, modify, and delete).
26.2.6. The system (e.g. Operating System) shall lock an interactive session after a specified period of user inactivity by clearing or overwriting display devices, making the current contents unreadable and by disabling any user’s data access/display devices other than unlocking the activity of the session.
26.2.7. The system shall allow user-initiated locking of the user’s own interactive session by clearing or overwriting display devices, making the current contents unreadable and by disabling any user’s data access/display devices other than unlocking the activity of the session.
26.2.8. Security mechanisms and/or procedures to regulate the introduction or connection of removable computer storage media (for example USB, mass storage devices, CD-RWs) to user workstations/portable computing devices shall be implemented.

26.3 Security Audit

26.3.1. An audit log shall be generated and maintained. System Level, Application Level and User Level events shall be included in the log, as required by the relevant Security Authority as a result of a Risk Assessment. For each of the auditable events, it shall associate individual user identities to those events, and shall include date and time of the event, type of event, user identity, and the outcome (success or failure) of the event. The following events shall always be recorded:

- all log on attempts whether successful or failed;
- log off (including time out where applicable);
- the creation, deletion or alteration of access rights and privileges;
- the creation, deletion or alteration of passwords.

26.3.2. The audit trail and associated archive shall be protected from unauthorised deletion and/or modification; it shall be presented in human readable format either directly (e.g., storing the audit trail in human-readable format) or indirectly (e.g., using audit reduction tools) or both.
26.3.3. Access to audit information shall be controlled; access permissions shall be established to permit access only by the appropriate security management staffs.
26.3.4. The audit data shall be retained for a period agreed by the Contracting Authority, based, where appropriate, on the requirements established by the NSA or DSA.
26.3.5. A means shall be available to analyse and review system activity and audit data, looking for possible or real security violations (analysis may work in support of intrusion detection/automatic response to an imminent security violation).

26.4 Protection against Malicious Software
26.4.1. Virus/malicious code detection software shall be installed on all servers, portable computing devices and workstations dependant upon the vulnerability of the underlying operating system environment. It shall be configured to automatically check on the introduction of removable media (e.g., CDs, USB mass storage devices, flash memory).
26.4.2. The virus/malicious code detection software shall be regularly updated.

26.5 Mobile Code
26.5.1. The source of the mobile code shall be appropriately verified.
26.5.2. The integrity of the mobile code shall be appropriately verified.
26.5.3. All mobile code shall be verified as being free from malicious software.
26.5.4. Available technical measures shall be enabled to ensure the use of mobile code is appropriately managed. For example, Microsoft Office applications and Internet Browser applications shall be configured to control import/acceptance of mobile code as well as use and creation of mobile code.

26.6 Availability
26.6.1. Security measures ensuring availability of NR information shall be implemented when required by the Contracting Authority.

26.7 Import/Export of Data

26.7.1. Data transfers between machines, virtual or physical, in different security domains shall be controlled and managed to prevent the introduction of NR data to a system not accredited to handle NR data.
26.7.2. All data imported to or exported from the CIS shall be checked for malware.

26.8 Configuration Management
26.8.1. A detailed hardware and software configuration control system shall be available and regularly maintained.
26.8.2. Configuration baselines shall be established for servers, LAN Components, Portable Computing Devices and workstations.
26.8.3. Configuration checks shall be made by appropriate Security Management staff on hardware and software to ensure that unauthorised hardware and software has not been introduced.
26.8.4. An inventory of hardware and software should be maintained, with equipment and cabling labelled as part of the inventory.
26.8.5. The configuration of the security enforcing and security relevant functions of the operating system shall only be subject to change by a limited number of authorised system and security administrators.
26.8.6. The security configuration of the operating system shall be maintained with the implementation of the appropriate security patches and updates. Regression Aspects i.e. any potential adverse effects of the modification on existing security measures, shall be considered and appropriate action taken.
26.8.7. The installation and configuration of application software with security relevant or security-enforcing functions shall be subject to a limited number of authorised system and security administrators.
26.8.8. The configuration of the operating system shall be subject to periodic checks to ensure its security compliance.
26.8.9. Changes to the system or network configuration shall be assessed for their security implications/impacts.
26.8.10. The Basic Input/Output System (BIOS) or similar firmware shall be password protected in order to protect access to the system's password data.

26.9 Security Management
26.9.1. Mechanisms shall be implemented which manage security data and functions; only defined authorised users (or roles) may perform security functions and access security relevant data.
26.9.2. The compromise or suspected compromise of NR information shall be immediately reported for inspection and investigation purposes, through the SO, to the Contracting Authority and, if required by national laws and regulations, to the relevant NSA or DSA.

26.10 Approved products
26.10.1. An approved product is one that has been approved for the protection of NR information either by NATO or by the National CIS Security Authority (NCSA) of a NATO Nation or in accordance with national laws and regulations.

26.10.2. The relevant NSA, NCSA or DSA shall be consulted, through the Contracting Authority, to determine, whether approved products shall be used, unless already defined by the NATO policies or equivalent national laws and regulations.

26.11 Security Testing

26.11.1. The system shall be subject to initial and periodic security testing to verify that security measures work as expected.

26.12 Transmission Security

26.12.1. NR information transmitted over a CIS not accredited to handle NR information (e.g. Internet) shall be encrypted using approved cryptographic products.

26.13 Wireless LAN

26.13.1. The range of Access Points shall be set to minimise exposure to external attacks, special attention shall be given to the selection of antennae, their location, power and signal propagation.

26.13.2. NR information transmitted over a wireless connection shall be encrypted using an approved cryptographic product.

26.14 Virtualisation

26.14.1. When existing systems are combined using a virtualisation product, the accreditation of each of the systems shall be reviewed to ensure that any mitigations and assumptions previously made are still appropriate.

26.14.2. A deployed virtualisation product itself shall be treated as at least the highest Protective Marking of any of its virtual machines (i.e. NR).

26.14.3. Virtual Machines shall be appropriately configured and managed. System patching, administration of accounts, and maintenance of anti-virus software, shall all be performed as if the machine were a physical machine. The host-operating machine shall also be correctly configured and maintained.

26.14.4. Network routing provided internally by the virtualisation product to connect virtual machines shall not be considered as a security measure. For example, a firewall shall not be virtualised.

26.14.5. The administrative interface for the hypervisor, shall only be used for administration of the hypervisor, and shall not be used for the normal administration of services provided by the virtual machines.

26.14.6. Access to the hypervisor functions shall be appropriately controlled.

26.14.7. The ability to “cut-and-paste” between virtual machines shall be appropriately configured and controlled.

26.14.8. The ability to create virtual machines shall be appropriately configured and controlled.

26.14.9. Virtual Machines shall be suitably de-commissioned after use.

26.14.10. Software based virtual networks created between virtual machines shall be appropriately configured, controlled and monitored.

26.14.11. Virtual Servers and Virtual Workstations shall not be located on the same physical host.

26.14.12. Virtual machines operating in different areas of the system architecture shall not be located on the same physical host, for example, virtual machines operating in a De-Militarised Zone (DMZ) shall not be located on the same physical host as those operating in the LAN.
26.14.13. The management of the Virtualisation infrastructure shall be appropriately controlled. Only Virtual Management, patch management, anti-malware and Active Directory communication mode shall be allowed.
26.14.14. Management of the Virtualisation infrastructure shall be performed via a dedicated Administrative account.
26.14.15. The Storage Area Network (SAN) used for Virtualisation shall be isolated and only accessible by the physical host.
26.14.16. The SAN used to host Virtualisation operating at different security classifications shall be isolated onto separate Logical Unit Numbers.
26.14.17. Modifications to the 'Master Copy/Version' of a Virtual Machine shall be appropriately controlled.
26.14.18. Network cards shall not be shared across Virtual Machines that are operating in different Security Domains.

26.15 Interconnections to a CIS not accredited to handle NR information
26.15.1. Security requirements, specific to interconnection scenarios, are listed in the latest versions of the NATO documents entitled "INFOSEC Technical and Implementation Directive for the Interconnection of Communications and Information Systems (CIS)" (current reference AC/322-D/0030-REV5) and "Supporting Document on the Interconnection of NR Communications and Information Systems (CIS) to the Internet" (current reference AC/322-D (2010)0058). These Directives may be obtained from the Contracting Authority.
26.15.2. Interconnection to another CIS, especially the internet, will significantly increase the threat to a contractor's CIS and therefore the risk to the security of the NR information handled by the contractor's CIS. A security risk assessment shall be performed to identify the additional security requirements that need to be implemented as part of the security accreditation process.
Security requirements can also be found in the latest version of the NATO document entitled "Technical & Implementation Directive on CIS Security" (current reference AC/322-D/0048-REV3). This Directive may be obtained from the Contracting Authority.
26.15.3. When performed, the security risk assessment shall be included with the statement of compliance to the Contracting Authority.

26.16 Disposal of IT Storage Media
26.16.1. For IT storage media that has at any time held NR information the following sanitisation shall be performed to the entire storage media prior to disposal:
- EEPROM and Flash Memory (e.g. USB sticks, SD cards, solid state drives, hybrid hard drives): overwrite with random data at least three times, then verify storage content matches the random data;
- Magnetic Media (e.g. hard disks): overwrite or degauss;
- Optical Media (e.g., CDs and DVDs): shred or disintegrate into pieces of 10mm2 or less;

- Other storage media: seek security requirements from the Security Accreditation Authority.

26.17 Portable Computing Devices (laptops, tablets, etc)
26.17.1. Portable computing devices not using approved encryption shall only be used or stored in an appropriately secure location. Portable computing devices and drives containing NR information that do not use approved encryption shall not be taken outside the contractor's premises unless held under personal custody. The term "drives" includes all removable media. Any authentication token and/or password(s) associated with the encryption product shall be kept separate from portable computing devices whenever it is not in use, left unattended or in transit.

Physical Security of CIS Handling NR information

27. Areas in which CIS are installed to display, store, process, or transmit NR information shall be established, as a minimum, as Administrative Zones. For mobile solutions (e.g. laptop) used outside of Administrative Zones, the user shall ensure that the displayed content is protected in a way that NR information is not exposed to unauthorised individuals.

28. CIS areas housing servers, network management system, network controllers and communications controllers should be established as separate and controlled areas with an appropriate access control system. Access to these CIS areas should be limited to only specifically authorised persons.

Security of NR Removable Computer Storage Media

29. Removable computer storage media containing NR information are required to be labelled with that classification marking. Measures shall be in place to prevent unauthorised access to NR removable computer storage media in order to maintain the need-to-know principle. Use of CIS Equipment Privately Owned by Contractor's Personnel.

30. The use of privately-owned equipment of contractor's personnel (hardware and software) for processing NR information shall not be permitted.

CIS Users' responsibilities

31. CIS users (e.g. end users, administrators) involved in the handling of NR information within the CIS shall be made aware of their responsibilities and the procedures to be followed. The responsibilities and the procedures to be followed shall be documented and acknowledged by CIS users in writing.

Advice
32. Advice or clarification of the provisions of this contract security clause shall be obtained from the Contracting Authority.

Audit/inspection

33. At the request of the contracting authority or relevant NSA/DSA/SAA, the contractor shall provide evidence of compliance with this Contract Security Clause and permit an audit of inspection of the Contractors processes and facilities by representatives of the contracting authority or the contractors NSA/DSA or relevant NATO security authorities to ensure compliance with these requirements.

Annex 1: Quotation Content Checklist

Quotation Content Checklist

Bidders shall ensure the folloiwng information and/or documents are included in their bid:

□ Bidder's name, address, POC, Contact numbers, email address.

□ Compliance Statement (Annex 2)

□ Past Performance (including References) (Annex 3).

□ Price Quotation (Annex 4)

□ Technical Compliance matrix (See Annex 5).

Annex 2: Compliance Statement

COMPLIANCE STATEMENT

1. It is hereby stated that our Company has read, understood and will comply with all the documentation, terms & conditions which form part of **RFQ CMRE-26-012**, to include - more specifically – the following:
    a. The Statement of Work, Part II.
    b. The CMRE Standards Terms and Conditions dated May 2026, which are applicable to this procurement and located on the CMRE website at https://www.cmre.nato.int/general-information .
    c. The Security Aspects Letter (SAL), Part III.
    d. The Security Clause, Part III.

2. The Bidder certifies that the quotation submitted in response to the referenced solicitation is fully compliant with the provisions of **RFQ CMRE-26-012** and the intended contract with the following proposed MINOR exception(s) - if any; such exemptions are considered by the Bidder non-substantial to the CMRE solicitation provisions issued:

Clause / Reference	Description of Proposed Minor Deviation

Company: _____ Signature: _____

Name &Title: _____ Date: _____

3. Important notice:
   a. Bidders quotations must be based on full compliance with the terms, conditions and requirements of the RFQ and all future clarifications and/or amendments.
   b. The bidder may offer variations in specific implementation and operational details provided that the functional and performance requirements are fully satisfied.
   c. In case of conflict between the compliance statement and the detailed evidence or explanation furnished, the detailed evidence/comments shall take precedence/priority for the actual determination of compliance.
   d. Minor or non-substantial deviations may be accepted by CMRE, while substantial changes will result in potential administrative non-compliance at CMRE's full and exclusive discretion.

Annex 3: Past performance Information Form

PAST PERFORMANCE INFORMATION FORM

Company is required to submit minimum of one (1) past performance reference:

Contracting Entity:

Contract No:

1. Type of Contract (Firm Fixed Price, Requirements):

2. Title of Contract:

3. Description of Work Performance and Relevance to Current RFQ:

4. Contract Euro Amount:

5. Period of Performance:

6. Name, Address, Fax and Telephone No. of Reference:

7. Indicate Whether Reference Acted as Prime or Sub-contractor:

8. Comments regarding compliance with contract terms and conditions:

9. Complete Contact Information for client:

10. Permission to contact client for reference: Yes/ No

Name/Signature of Authorized Company Official_____

This Enclosure is designed to assist the respective company in order to provide CMRE with all necessary documents/information required. For clarification, please refer to Bidding Instructions in part I of this solicitation.

Annex 4: Price Quotation

PRICE QUOTATION

1. Bidders shall provide an all-inclusive, lump-sum Firm Fixed Price (FFP) by filling out the "Total Price" box in the Schedule of Prices.

2. The prices shall be tax and duty free.

3. The prices shall be expressed in Euro.

Schedule of prices

No.	Description/Deliverables	Unit of Issue	Total Price (€)
1	Total Firm-Fixed-Price for Remedial Action for CMRE CCTV Network Infrastructure	Lump-sum/ prezzo a corpo	

Authorizing Company Official:

Printed Name:_____

Position:_____

Authorizing Company (Signature):_____

Title:_____

Date:_____

Annex 5: Technical Compliance Matrix

TECHNICAL COMPLIANCE MATRIX

Compliance Matrix to the STATEMENT OF WORK: Bidders' technical quotation will be assessed based on the criteria mentioned in the following table:

No	ITEM	COMPLIANT/ NOT COMPLIANT
1	Past Performance (including References)	

(End of RFQ)