राष्ट्रीय परीक्षा एजेंसी
National Testing Agency
Excellence in Assessment
आज़ादी का अमृत महोत्सव
(उच्चत्तर शिक्षा विभाग, शिक्षामंत्रालय, भारत सरकार के तहत एक स्वायत्त संगठन)
(An Autonomous Organization under the Department of Higher Education, Ministry of Education, Government of India)

No.: A-A8/17/2026-Admin (15066)(2)

Date: 25/07/2026

VACANCY NOTIFICATION

National Testing Agency invites applications for one (1) post of **General Manager – Information Security (Chief Information Security Officer)** from interested/eligible/suitable candidates on contract basis initially for a period of three (3) years, extendable based on performance and organizational requirement

For Eligibility Criteria / Qualification / Experience, Process of Application and Selection, etc., please see the detailed advertisement attached with this Vacany Notification.

Eligible candidates may submit their applications in the format provided at Annexure-I alongwith all required document as mentioned in the detailed advertisement which should reached by email to: ***dir-admin@nta.gov.in***. within 30 days from the date of publication of this advertisement.

25.7.2026

V V Patil, IOFS
Director (Administration)

पहलीमंजिल, एनएसआईसी-एमडीबीपीबिल्डिंग, ओखलाइंडस्ट्रियलएस्टेट, नईदिल्ली-110020
First Floor, NSIC-MDBP Building, Okhla Industrial Estate, New Delhi -110020
फ़ोन/Telephone: 011-69095-250/वेबसाइट/Website: nta.ac.inई-मेल/e-mail: vv.patil@nta.ac.in

Advertisement for Engagement of General Manager - Information Security (Chief Information Security Officer) on Contract Basis

1. About the National Testing Agency

The National Testing Agency (NTA) has been established as a premier, specialist, autonomous and self-sustained testing organisation under the Ministry of Education, Government of India, to conduct entrance examinations for admission and fellowship in higher educational institutions. NTA conducts some of the country's largest and most high-stakes examinations - including JEE (Main), NEET (UG), UGC-NET, CUET (UG & PG), CMAT, GPAT and several others - collectively serving crores of candidates every year, across 500-plus cities in India and at select international centres.

NTA's digital ecosystem - covering candidate portals, application and registration platforms, fee payment, admit cards, computer-based testing systems, item banks, result-processing engines, and integrations with national digital public infrastructure - holds the personal data of crores of candidates and is the foundation of every examination outcome. The cyber-security of these systems, and of the underlying infrastructure, is therefore non-negotiable. NTA is undertaking a comprehensive strengthening of its information-security capability in line with applicable laws, including the Digital Personal Data Protection Act 2023, the Information Technology Act 2000, CERT-In directions and MeitY guidelines. To lead this critical function, NTA invites applications for engagement of a General Manager - Information Security (designated Chief Information Security Officer) on a contractual basis from candidates with the requisite qualifications and experience.

2. Position Details

Name of Post	General Manager - Information Security (Chief Information Security Officer / CISO)
Number of Positions	01 (One)
Nature of Engagement	Contract, initially for a period of three (3) years, extendable based on performance and organisational requirement.
Age Limit	Preferably below 55 years as on the last date of application. Relaxation may be considered for exceptional candidates with strong cyber-security leadership credentials.
Remuneration	Consolidated monthly remuneration, commensurate with qualifications, experience and industry benchmarks, to be decided by the competent authority. The remuneration package will be competitive and negotiable for exceptional candidates.

Job Location	National Testing Agency, Head Office, New Delhi. The position may require travel to data-centre sites, partner institutions and stakeholder offices, especially during examination cycles and incident response.
Reporting To	Director General, National Testing Agency.

3. Role Overview

The General Manager - Information Security, designated as NTA's Chief Information Security Officer (CISO), will head the cyber-security function of the Agency and be responsible for the security posture of all NTA systems, applications, networks, data and digital workflows. The role spans the full information-security stack - threat modelling, security architecture, vulnerability management, security operations, identity and access management, application security, encryption, cloud security, data-protection compliance, third-party risk management, incident response, and security culture - across the entire technology footprint of NTA.

The role requires a seasoned cyber-security leader with deep technical command, strong governance instincts and the ability to operate at the intersection of security, technology and public-trust. The CISO will report to the Director General, NTA, and will work closely with NTA's technology, test-security, vigilance, candidate experience, and finance & legal functions. The incumbent will be the Agency's senior-most interface with CERT-In, NCIIPC, MeitY and other Government cyber-security bodies, and with empanelled security partners and auditors. Given the centrality of the digital examination ecosystem to NTA's mandate and public credibility, the CISO is one of the most institutionally critical positions in NTA.

4. Qualifications and Experience

Essential Qualifications	• B.E. / B.Tech. / M.E. / M.Tech. / M.Sc. in Computer Science, Information Technology, Electronics, Cyber Security, or an allied discipline from a recognised university or institution of repute. A Master's degree or higher in Cyber Security or Information Security will be an added advantage. • Consistently good academic record. • Minimum 12 years of post-qualification experience in information security, cyber security, security operations, or allied functions. • Of these, at least 5 years must be at a senior leadership level (e.g., Chief Information Security Officer, Head of Information Security, Senior Director - Cyber Security, Vice President - Information Security) in a large enterprise. • At least one professional certification in information security from among: CISSP, CISM, CISA, CRISC, CGEIT, CCISO, OSCP, GIAC (any track), or equivalent from a recognised international body.
Desirable Experience	• Prior experience as CISO or Head of Information Security in a large transaction-intensive organisation - banking, financial services,

	telecom, e-commerce, e-governance, or major public-sector technology platform. • Demonstrated experience of having successfully led the response to at least one major cyber-incident from detection through containment, eradication, recovery and post-incident review. • Experience of running an in-house or outsourced 24x7 Security Operations Centre (SOC) at scale. • Prior engagement with CERT-In, NCIIPC, MeitY, STQC or similar Government cyber-security bodies on advisories, audits or incident reporting. • Familiarity with the Digital Personal Data Protection Act 2023 and its operational implementation, including the role of the Data Protection Officer. • Experience of cloud security architecture across AWS, Azure or GCP - including identity, network, data, workload and DevSecOps controls. • Familiarity with ISO 27001, NIST CSF, PCI DSS, SOC 2, and other recognised cyber-security frameworks.
Skills and Competencies	• Strong technical command across the information-security stack - network security, application security, endpoint security, cloud security, identity & access, data protection, cryptography and DevSecOps. • Excellent governance instincts - ability to define policy, set standards, drive compliance and run committees and governance forums. • Proven incident-response and crisis-management capability under pressure, with clarity on technical containment, communication and stakeholder coordination. • Outstanding stakeholder-management skills - across senior Government functionaries, regulators, partners, vendors, auditors and senior leadership. • Strong analytical orientation, with the ability to use threat intelligence, security telemetry and risk metrics to drive prioritisation and decisions. • High personal integrity, ability to handle highly confidential and sensitive information with absolute discretion, and a strong public-service orientation.

5. Key Roles and Responsibilities

The CISO will be responsible for the following, which is indicative and not exhaustive:

5.1 Information-Security Strategy, Policy and Governance

- Define and maintain NTA's information-security strategy, policies, standards, procedures and architecture across the entire technology stack.
- Establish and chair a structured Information Security Governance forum with regular reporting to the Director General and Governing Body, covering risk posture, control effectiveness, audit findings and incident landscape.
- Build and maintain NTA's Information Security Manual - a master document codifying all policies, standards, SOPs and incident-response playbooks.
- Define security risk-appetite statements, security KPIs and a risk register, and maintain these through periodic review cycles.
- Run a structured security exception-management process, with documented sign-offs and time-bound remediation plans for accepted exceptions.

5.2 Security Architecture and Engineering

- Define security architecture standards across the entire technology stack - applications, APIs, databases, networks, cloud, endpoints, mobile and identity.
- Drive the adoption of zero-trust principles, secure-by-design and privacy-by-design across all NTA platforms, in coordination with NTA's technology function.
- Establish secure development standards (SAST, DAST, dependency-scanning, secure code review) and integrate them into the software-delivery pipeline.
- Define and enforce data-classification, data-handling, data-retention, data-encryption (at rest and in transit) and key-management standards.
- Establish standards for cryptography, certificate management, secrets management and Hardware Security Modules (HSMs) for high-sensitivity workloads such as question-paper systems and result systems.

5.3 Security Operations Centre and Threat Management

- Operate a 24x7 Security Operations Centre (SOC) capability - in-house or through empanelled Managed Security Service Providers (MSSPs) - with continuous monitoring, threat hunting, and incident response.
- Build and maintain a Security Information and Event Management (SIEM) platform with comprehensive log coverage, use-case engineering and analytics.
- Establish threat-intelligence feeds, threat-hunting processes and proactive detection capabilities for advanced persistent threats and emerging attack patterns.

- Run a continuous vulnerability management programme - asset discovery, vulnerability scanning, prioritisation, remediation tracking, and metrics on time-to-remediate.
- Maintain a structured cycle of penetration tests, red-team exercises, secure code reviews, third-party security audits and bug-bounty engagements (where applicable).

5.4 Identity, Access and Privilege Management

- Establish and enforce identity and access management (IAM) standards across all NTA systems, including for employees, contractors, vendors and candidates.
- Implement privileged access management (PAM) for all administrative and high-impact accounts, with session recording, just-in-time access and approval workflows.
- Drive multi-factor authentication, single sign-on, conditional access and modern authentication mechanisms across the technology footprint.
- Run periodic user-access reviews, joiner-mover-leaver controls, and orphan-account clean-ups across all critical systems including question paper systems and result systems.
- Define and enforce role-based access control with least-privilege, particularly for teams handling confidential examination material.

5.5 Regulatory Compliance and Data Protection

- Drive compliance with CERT-In directions, MeitY guidelines, the Digital Personal Data Protection Act 2023, the Information Technology Act 2000, ISO 27001 and other applicable standards.
- Serve as, or work closely with, NTA's Data Protection Officer (DPO) on the operational implementation of the Digital Personal Data Protection Act 2023 - covering data-fiduciary obligations, consent management, data-subject rights, breach notification and cross-border transfer controls.
- Maintain NTA's records of processing activities, privacy impact assessments and data-flow maps; institutionalise privacy-by-design across the candidate-data lifecycle.
- Coordinate with NTA's finance and legal function on cyber-security and data-protection compliance for vendor contracts, including data-processing agreements, breach-notification clauses and audit rights.
- Submit prescribed compliance reports, breach notifications and incident reports to CERT-In, the Data Protection Board (when constituted) and other regulatory authorities, as required.

5.6 Cyber-Incident Response and Crisis Management

- Lead NTA's cyber-incident response across the full lifecycle - detection, triage, containment, eradication, recovery and post-incident review.
- Maintain a comprehensive Cyber Incident Response Plan with named roles, decision trees, communication protocols and regulatory notification timelines.

- Run table-top exercises and crisis-simulation drills periodically, covering scenarios such as ransomware, data breach, DDoS, application compromise, supply-chain attack and insider threat.
- Coordinate cyber-incident response with NTA's vigilance, candidate experience and legal functions to ensure coherent technical, legal and communication response.
- Coordinate with CERT-In, NCIIPC and other Government cyber-security bodies on cyber-incidents impacting NTA, including timely notifications and post-incident reports.
- Conduct structured post-incident reviews and translate findings into concrete control improvements, SOP updates and training inputs.

5.7 Security of Examination-Critical Systems

- Define and oversee enhanced security controls for examination-critical systems - covering question paper systems, candidate registration, fee payment, admit card systems, computer-based testing platforms, OMR processing, normalisation engines and result systems.
- Establish strict access controls, encryption standards, immutable logging and tamper-evident storage for all examination-critical workloads.
- Run pre-examination security readiness reviews of all examination-supporting systems before each examination cycle, in coordination with NTA's technology function.
- Coordinate with NTA's test-security function on the technical security of examination-day workflows - including biometric authentication, face-matching, CCTV systems and live monitoring infrastructure.
- Maintain an examination-specific cyber-incident response readiness on examination days, with elevated SOC monitoring and rapid-response capability.

5.8 Third-Party Risk and Supply-Chain Security

- Establish a structured Third-Party Risk Management (TPRM) programme covering all technology vendors, MSSPs, BPO partners, hosting providers and SaaS partners that have access to NTA systems or data.
- Define security requirements for vendor contracts and run pre-onboarding security assessments for all material vendors, in coordination with NTA's finance and legal function.
- Run continuous monitoring of high-risk vendors through audits, security questionnaires, attestations and vulnerability disclosures.
- Define standards for software supply-chain security including software bill of materials (SBOM), open-source component governance and code-signing.

- Maintain incident-coordination protocols with major vendors so that vendor-side incidents impacting NTA are escalated and managed in line with NTA's response framework.

5.9 Security Awareness, Culture and Capability Building

- Build a security-aware culture across NTA - through structured training, simulations, policy enforcement and recognition.
- Run mandatory security-awareness training for all NTA staff, contractors and field workforce (Centre Superintendents, City Coordinators, Observers, Invigilators), in coordination with NTA's HR and capacity-building function.
- Run periodic phishing simulations and similar awareness exercises, and use the data to drive targeted improvements.
- Build and lead a high-performing in-house Information Security team covering governance, security operations, application security, identity, cloud security and DevSecOps.
- Manage relationships with empanelled security agencies, MSSPs, audit firms and technology vendors with strong SLA, quality and confidentiality discipline.
- Plan and manage the function's budget and contracts in compliance with GFR and NTA financial norms; define and track security KPIs and dashboards, and report progress to the Director General and Governing Body.

6. Key Result Areas (KRAs)

- Demonstrably strong cyber-security posture across NTA's technology stack, with measurable improvements in vulnerability remediation timelines, control coverage and audit ratings.
- Zero major cyber-incidents impacting confidentiality, integrity or availability of examination-critical systems; for any incidents, rapid detection, containment and recovery within published SLAs.
- Full compliance with CERT-In directions, the Digital Personal Data Protection Act 2023, MeitY guidelines and other applicable standards, with timely regulatory submissions.
- An operational 24x7 SOC capability with comprehensive log coverage, threat-hunting practice and metrics-driven continuous improvement.
- A robust third-party risk management programme covering all material vendors and partners, with documented assessments and continuous monitoring.
- A measurable security-aware culture across NTA, with training coverage, phishing-simulation results and reporting metrics on an upward trajectory.
- A capable, motivated and professionally strong Information Security team within NTA.

7. Selection Process

Shortlisting will be done on the basis of qualifications, experience and suitability of the candidate for the position. Shortlisted candidates will be invited for a personal interview (with the option of a presentation on cyber-security strategy and operations excellence for NTA) before a Selection Committee constituted by the competent authority. The Selection Committee may include senior cyber-security experts. NTA reserves the right to fix suitable criteria for shortlisting and to limit the number of candidates called for interview. Given the sensitive nature of the role, comprehensive background verification will be undertaken before any offer is made. The decision of the Selection Committee will be final and binding.

8. How to Apply

- Eligible candidates may submit their applications in the format provided at Annexure-I, along with a detailed CV, a brief (maximum 2-page) write-up on their vision for information security and cyber resilience at NTA, and self-attested copies of certificates in support of qualifications, experience and professional certifications.
- Applications may be submitted by e-mail to the address notified on the NTA website, with the subject line "Application for the Post of GM - Information Security (CISO), NTA".
- Applications must reach NTA within 30 days from the date of publication of this advertisement on the NTA website. Applications received after the last date or in any form other than prescribed shall not be entertained.
- Candidates already employed in Government / PSU / Autonomous Bodies must route their applications through proper channel or submit a No Objection Certificate (NOC) at the time of interview.
- Mere fulfilment of the minimum qualifications and experience does not entitle a candidate to be called for interview. NTA reserves the right not to fill this post or to cancel the recruitment process at any stage without assigning any reason.

9. General Conditions

- The engagement will be purely on contractual basis and will not confer any right for regular appointment or absorption in NTA.
- Given the sensitive nature of the role, the selected candidate will be required to sign a comprehensive non-disclosure agreement and submit to periodic background verification.
- Canvassing in any form will lead to disqualification.
- Incomplete applications, or applications not accompanied by the required supporting documents, are liable to be summarily rejected.
- In case of any dispute, the decision of the Director General, NTA shall be final.

ANNEXURE - I

APPLICATION FORM

Engagement of General Manager - Information Security (CISO), National Testing Agency

Paste recent passport-size photograph
(self-attested)

To,

The Director General
National Testing Agency
(Ministry of Education, Government of India)
New Delhi

Subject: Application for the Post of General Manager - Information Security (CISO), NTA.

Reference: Advertisement dated _____

Sir/Madam,

With reference to the above-mentioned advertisement, I wish to apply for the post of General Manager - Information Security (CISO), National Testing Agency. My details are furnished below for kind consideration:

A. Personal Details

1. Full Name (in block letters)	
2. Father's / Husband's Name	
3. Date of Birth (DD/MM/YYYY)	
4. Age (as on last date of application)	
5. Gender	
6. Nationality	
7. Category (Gen / OBC / SC / ST / EWS / PwBD)	
8. Aadhaar Number	
9. PAN Number	

10. Mobile Number	
11. Alternate Contact Number	
12. E-mail Address	
13. Present / Correspondence Address	
14. Permanent Address	

B. Educational Qualifications

(Starting from the highest qualification. Attach self-attested copies of certificates.)

S. No.	Qualification / Degree	University / Institution	Year of Passing	% / CGPA	Division / Class
1					
2					
3					
4					
5					

C. Employment History / Work Experience

(In chronological order, starting with the most recent. Attach additional sheet in the same format, if required.)

S. No.	Organisation / Employer	Designation	Period (From - To)	Last Pay Drawn / CTC	Brief Description of Role & Responsibilities
1					
2					
3					

S. No.	Organisation / Employer	Designation	Period (From - To)	Last Pay Drawn / CTC	Brief Description of Role & Responsibilities
4					
5					
6					

Total Post-Qualification Experience (Years / Months)	
Experience at CISO / Head of Information Security level (Years / Months)	
Experience in Information Security / Cyber Security (Years)	
Experience in running 24x7 SOC operations (Years, if any)	
Largest user / data / transaction base secured (scale)	
Experience in Government / PSU / Autonomous Body (if any)	

D. Professional Certifications and Training

(Include relevant certifications such as CISSP, CISM, CISA, CRISC, CGEIT, CCISO, OSCP, GIAC tracks, ISO 27001 Lead Auditor / Implementer, certifications in cloud security (AWS / Azure / GCP), AI / ML security, or allied areas.)

S. No.	Certification / Training	Issuing Body / Organisation	Date / Year	Validity / Expiry
1				
2				
3				

S. No.	Certification / Training	Issuing Body / Organisation	Date / Year	Validity / Expiry
4				
5				

E. Key Achievements / Major Information Security Initiatives Led

(Briefly describe up to five major information-security / cyber-security / incident-response / transformation initiatives led by you, indicating scale, role played and measurable outcomes. May attach separate sheet. Do NOT include any classified or sensitive details that would breach prior employer confidentiality.)

1	
2	
3	
4	
5	

F. References

(Two professional references, preferably from senior positions, who can be contacted.)

Name and Designation	Organisation and Address	Contact Number and E-mail

G. Additional Information

1. Current Employer and Designation	
2. Current Gross Remuneration / CTC (per annum)	
3. Expected Remuneration (per annum)	
4. Notice Period / Earliest Date of Joining	
5. Whether any criminal case / departmental enquiry / vigilance proceeding is pending against you? (Yes / No - if yes, give details)	
6. Disclosure of any current or recent engagements with security vendors / MSSPs / audit firms that may bear on the role at NTA (Yes / No - if yes, give details)	
7. Languages Known (Read / Write / Speak)	

H. List of Enclosures

- Detailed Curriculum Vitae (CV / Resume).
- Vision Statement (maximum 2 pages) on information security and cyber resilience at NTA.
- Self-attested copies of certificates of educational qualifications.
- Self-attested copies of experience certificates / appointment letters.
- Copies of professional certifications (CISSP, CISM, CISA, etc.) with current validity.
- Copy of latest salary slip / Form 16 (for verification of CTC).
- Copy of a Government-issued photo identity (Aadhaar / PAN / Passport).
- No Objection Certificate (NOC), if employed in Government / PSU / Autonomous Body.
- Any other document in support of the candidature (please specify): _____.

Declaration

I hereby solemnly declare that all the statements made and information furnished in this application are true, complete and correct to the best of my knowledge and belief. I understand that in the event of any information being found false, incorrect or incomplete, or ineligibility being detected before or after the selection / appointment, my candidature / appointment is liable to be cancelled / terminated without any notice or compensation, and appropriate action may be initiated against me. I further declare that I have no objection to any verification of the particulars

furnished by me, including comprehensive background and security verification. I also undertake to disclose proactively any actual, potential or perceived conflict of interest with security vendors, MSSPs, audit firms or other entities that may bear on my role at NTA.

Place: _____

Date: _____

_____

(Signature of the Applicant)

Name: _____