File No.:11-33/12/2024-COMP - DGS **Date:26.10.2026**

ORDER

Subject: Termination of the Contract dated 27.03.2026 for "Cybersecurity & Data Privacy Staff Augmentation and Managed Support Services" with M/s A3S Tech and Company, following show-cause proceedings.

A. Introduction and summary of decisions:

1. The Directorate General of Maritime Administration (DGMA), Mumbai (the "Client"), engaged MIS A3S Tech and Company (the "Consultant"), a partnership firm, under the Contract dated 27.03.2026 (the "Contract") for Cybersecurity & Data Privacy Staff Augmentation and Managed Support Services. The engagement covers six dedicated cybersecurity and data privacy resources deployed on-site for twelve months at a Contract Price of I per month), excluding GST

2. The Consultant is an execution and implementation partner working under the supervision of the DGMA PMU and the CISO Office. Its personnel were entrusted with access to DGMA premises, systems, information, vendors and operational processes. The nature of the engagement required strict integrity, confidentiality, discipline, authorised access and faithful protection Of DGMA 's interests.

3. Serious concerns regarding the conduct of a resource deployed by the Consultant (the "Concerned Resource") came to the notice of DGMA. A Show-Cause Notice ("SCN") was issued on 03.10.2026 and required a signed, point-wise reply, supported by records, within five working days. By communication dated 06.10.2026, the Consultant acknowledged receipt of the SCN, proposed to conduct an internal investigation, requested access to the evidence relied upon, and assured its cooperation. That communication was preliminary in nature and did not constitute the complete signed, point-wise reply required by the SCN. It also did not curtail the balance of the original five-working-day opportunity. Thereafter, to ensure a full and reasonable opportunity, a separate additional period of five days was permitted for submission of a complete response, supplementary explanation, or supporting material. During that extended Opportunity, DGMA independently retrieved and reviewed concrete electronic evidence, including official intercom recordings and the corresponding transcripts. The communication dated 06.10.2026, any subsequent response or material received, the independently retrieved electronic evidence, and the available record have been considered by the Competent Authority.

4. Upon consideration of the SCN, the Consultant's communication dated 06.10.2026, any subsequent response Or material received, the available documentary and electronic material, the prior

communications, applicable contractual duties and the Government procurement framework, the Competent Authority has determined that continuation of the engagement is incompatible with DGMA's security, integrity and operational requirements. The Contract is therefore terminated for default with effect from 17.10.2026 under paragraph 10.8.3 Of the Manual for Procurement of Consultancy Services, Second Edition, 2025, read with the Contract and the findings recorded in this Order.

B. Background and chronology

Date	Event
12.11.2024	GeM Bid No. GEM/2024/B/5587457 floated for a CERT-In empanelled agency for cybersecurity framework, infrastructure audit and compliance audit.
17.03.2025 / 15.04.2025	Letter of Intent and GeM Contract No. GEMC-511687724540159 issued for the earlier engagement.
22.04.2025 to 22.09.2025	Initial service period completed for cybersecurity framework, assessment and compliance support, including risk-assessment methodology, policy/SOP development, cyber-resilience and disaster-recovery inputs, regulatory compliance assessment, awareness and continuity planning.
27.03.2026	A3S Tech and Company was re-engaged for the next stage under the Contract dated 27.03.2026 for Cybersecurity & Data Privacy Staff Augmentation and Managed Support Services. The scope moved from assessment/framework development to implementation and sustained support, including compliance remediation, policy operationalisation, application and infrastructure security, monitoring, incident response, vendor governance, data privacy and awareness support.
06.02.2026	Letter of Intent for the present engagement; accepted by the Consultant on 19.02.2026.
27.02.2026	Performance Bank Guarantee No. 0201IGP261133880 for ₹3,61,080/- issued by Kotak Mahindra Bank Ltd.
27.03.2026	Present Contract executed at Mumbai.
Prior to SCN	Concerns arose regarding alleged solicitation of percentage/consideration, unauthorised vendor interaction, conflict of interest, information-security practices, attendance and misuse of official facilities. Prior warnings and corrective

	communications had also been issued.
03.10.2026	DGMA issued the SCN and protective directions. The SCN required a signed, point-wise reply with supporting records within five working days.
06.10.2026	Consultant's communication received acknowledging the SCN, proposing an internal investigation, requesting access to evidence, and assuring cooperation; it was not a complete signed, point-wise reply.
After expiry of the original response period	The preliminary communication dated 06.10.2026 did not constitute the complete point-wise reply and did not curtail the original five-working-day opportunity. A separate additional five-day opportunity was thereafter permitted for a complete response, supplementary clarification, or supporting material, without prejudice to DGMA's protective directions. During this extended opportunity, DGMA independently retrieved and reviewed concrete electronic evidence, including official intercom recordings and the corresponding transcripts.
26.10.2026	Speaking Order issued; termination effective.

C. Contractual and regulatory framework

Provision	Relevant obligation
GCC 1.9	Code of Integrity under GFR Rule 175; disclosure of commissions, gratuities or fees; contractual consequences for breach.
GCC 3.1	Due diligence, sound management and faithful protection of the Client's interests.
GCC 3.2.1, 3.2.3, 3.2.5 and 3.2.6	Client's interest paramount; prohibition on trade commission or similar payment; prohibition of conflicting activities; duty to disclose actual or potential conflicts.
GCC 3.3	Confidentiality obligations, surviving termination.
GCC 3.7 and 3.8	Ownership, handover and protection of deliverables, information, logs, credentials and artefacts.

GCC 3.9 and 3.10	Audit/inspection rights and right to initiate debarment or blacklisting proceedings for material breach.
GCC 4.2	Control over deployment and replacement of Experts.
GCC 6.3, 6.4 and SCC 6.2	Payment subject to accepted outputs, verified deployment and exit compliance; performance security held until formal closure.
ToR: Deployment and Attendance	Full-time on-site deployment, 100% availability, prior approvals, attendance verification and replacement obligations.
ToR: Exit and Transition	Orderly handover, credential rotation, access revocation, return of property, deletion certification and CISO sign-off.

1. GFR 2017, Rule 175 (Code of Integrity).: Procuring entities, bidders, contractors and consultants are required to observe the highest standards of ethics during procurement and contract execution. The relevant prohibitions include solicitation or acceptance of an improper benefit, misrepresentation, improper use of information and non-disclosure of conflicts of interest.

2. GFR 2017, Rule 151 (Debarment from bidding), as amended by Department of Expenditure O.M. dated 08.05.2026. Rule 151(iii) permits a procuring entity to debar a bidder or its successors from procurement processes undertaken by that procuring entity, for a period not exceeding two years, upon determination of breach of the Code of Integrity. Rule 151(iv) requires a reasonable opportunity to represent before debarment. A ban across all Central Government Ministries/Departments requires a separate proposal by the concerned Ministry/Department, approval at the prescribed level and an order by the Department of Expenditure under the applicable Guidelines. The operative directions below therefore distinguish DGMA-level debarment from the proposal for Government-wide debarment.

3. GFR 2017, Rule 171 (Performance Security). Performance security secures due performance and may be dealt with in accordance with the Contract and the terms of the security instrument.

4. GFR 2017, Rules 144 and 173. These provisions embody transparency, fairness, integrity, accountability and standard contractual remedies in public procurement.

5. Manual for Procurement of Consultancy Services, Second Edition, 2025, paragraph 10.8.3 (Termination of Contract for Default). Where a Notice of Default remains unsatisfactorily resolved within two weeks of issue, the Procuring Entity may, by written Notice of Termination for Default, terminate the contract in whole or in part without compensation. Such termination does not prejudice accrued rights and remedies, does not extinguish liability for services already supplied, and permits further contractual remedies, including withholding payments, recovery of liquidated damages, encashment or forfeiture of performance security and legal proceedings. Legal advice may appropriately

be obtained before cancellation and further action.

6. Department of Expenditure Guidelines on Debarment of Firms from Bidding dated 02.11.2021, as amended on 08.05.2026. These govern entity-level and Government-wide debarment, including the requirement of due opportunity and the prescribed competent-authority process.

D. Show-cause proceedings and opportunity afforded

1. The SCN dated 03.10.2026 set out the prima facie matters requiring explanation, directed withdrawal of the Concerned Resource and suspension of access as protective measures, required preservation of records, and called for a signed, point-wise response supported by documents. The Commission/consideration allegation was specifically stated to include a reported percentage of 10%.

2. The Consultant's communication dated 06.10.2026 has been taken on record and considered. It acknowledged receipt of the SCN, proposed an internal investigation, requested access to the evidence relied upon, and assured cooperation. It did not, however, constitute the complete signed, point-wise reply with supporting records required by the SCN. During the extended opportunity afforded thereafter, DGMA independently retrieved and reviewed concrete electronic evidence, including official intercom recordings and the corresponding transcripts. The communication, any subsequent response or material received, the independently retrieved electronic evidence, and the available record have been assessed against the specific allegations, attendance material, access-related information, earlier communications and the Consultant's supervisory obligations. Mere denial, absence of a criminal adjudication, or attribution of the conduct solely to an individual does not by itself discharge the Consultant's contractual responsibility for deployed personnel.

3. The Consultant was allowed five working days from receipt of the SCN to submit a complete signed, point-wise response with supporting records. Its communication dated 06.10.2026 was an acknowledgment and preliminary procedural response, not the complete reply sought under the SCN; the remaining portion of the original opportunity was therefore not curtailed. After completion of the original five-working-day period, a separate additional opportunity of five days was permitted for submission of a complete response, supplementary clarification, or supporting material. During that extended opportunity, DGMA independently retrieved and reviewed concrete electronic evidence, including official intercom recordings and the corresponding transcripts. The Competent Authority has considered the communication dated 06.10.2026, any subsequent response or material received, the independently retrieved electronic evidence, and the material available on record. The principles of natural justice have accordingly been observed for the contractual determination recorded in this Order.

E. Material considered and standard applied

1. The SCN dated 03.10.2026 and proof of service;
2. The Consultant's communication dated 06.10.2026, acknowledging the SCN, proposing an internal investigation, requesting access to evidence and assuring cooperation, together with any subsequent response or documents furnished;
3. The transcript/material in which a percentage in relation to the procurement is mentioned;
4. The material concerning false, inconsistent or unauthorised representations and organisational affiliations;

5. The material concerning Seven-Star Solutions, indicating an association claimed or projected by the Concerned Resource, without independently establishing ownership, employment, beneficial interest or any formal legal relationship;
6. The Computer Cell/OTP transcript and related credential or after-hours access concern;
7. DGMA attendance and availability records, including prior approval/intimation records;
8. Official intercom recordings independently retrieved by DGMA during the extended opportunity, together with the corresponding transcripts;
9. Earlier warning/corrective communication issued under the direction of the CISO; and
10. The Contract, GCC, SCC, ToR, GFR 2017 and the Manual for Procurement of Consultancy Services, Second Edition, 2025.
11. The standard applied is the preponderance of probabilities appropriate to a contractual and administrative determination. This Order does not record criminal guilt and does not prejudice any vigilance, police, regulatory, civil or judicial process. Each finding is confined to the purpose of contractual, recovery, security and procurement action.

F. Issue-wise consideration and findings

Issue 1: Alleged demand for unauthorised commission or consideration

The record includes transcript material in which a percentage or consideration is mentioned in the context of procurement/vendor engagement. The transcripts support a concern regarding an unauthorised discussion of **Mr. Jainam Chopra, Consultant** from M/s A3S Tech & Co. of percentage-based consideration; however, they do not, by themselves, conclusively establish that the exact reported demand was 10% or that such an exact demand was made specifically in the cybersecurity-tools procurement. Accordingly, no conclusive finding is recorded on the precise percentage or the specific procurement linkage alleged in the SCN. Nevertheless, the discussion or solicitation of any unauthorised percentage or consideration with bidders/vendors, in the absence of an authorised basis, is incompatible with the Code of Integrity and the Consultant's duty to protect DGMA's interests. The Consultant has not produced material sufficient to satisfactorily dispel that broader contractual concern. The issue is therefore held established on the preponderance of probabilities only to the extent of unauthorised percentage-based consideration being discussed or solicited, without recording a finding on the exact 10% figure, its specific linkage to the cybersecurity-tools procurement, or any criminal guilt.

Issue 2: Unauthorised representation and vendor interaction

The Concerned Resource had no written authority to represent DGMA before bidders/vendors, to speak on behalf of DGMA, or to create an impression of influence over procurement outcomes. The available material concerning false, inconsistent or unauthorised representations and organisational affiliations demonstrates a serious breach of protocol, trust and governance. The Consultant's obligation extended to controlling how its personnel represented their role. This issue is held established for contractual purposes.

Issue 3: Conflict of interest and misuse of position or information

The material concerning Seven-Star Solutions indicates an association claimed or projected by the Concerned Resource in a vendor-facing context outside approved duties. That material does not, by itself, establish ownership, employment, beneficial interest or any formal legal relationship between the

Concerned Resource and Seven Star Solutions. Nevertheless, the claimed or projected association raises a concern that access, role or information obtained through the DGMA engagement may have been used, or appeared to be used, outside approved duties. The Consultant has not demonstrated prior disclosure, written authorisation, recusal or an effective conflict-control mechanism. The issue is therefore held established only to the extent of the undisclosed claimed or projected association and the resulting contractual concern regarding misuse of entrusted position or information; no finding of ownership, employment, beneficial interest or formal legal relationship is recorded.

Issue 4: Credentials, after-hours access and information security

The Computer Cell/OTP transcript indicates credential/OTP-related interaction and access activity outside ordinary controls. Credentials and one-time passwords are security-sensitive and must not be requested, obtained, shared or used except through recorded, authorised and auditable procedures. The Consultant has not satisfactorily established a documented business justification and prior authorisation sufficient to cure the concern. Given the privileged nature of the engagement, this is a material information-security and trust failure.

Issue 5: Attendance, availability and deployment discipline

DGMA attendance records and the available approval/intimation trail indicate deficiencies in attendance, availability and/or deployment discipline. The ToR required full-time on-site deployment, timely intimation, approved remote work and adequate continuity arrangements. The Consultant remained responsible for deployment control and alternates. The explanation does not satisfactorily reconcile the official records or demonstrate consistent compliance. This issue is held established to the extent reflected in DGMA's attendance and approval records.

Issue 6: Misuse of official communication facilities

The official intercom facility was required to be used only for authorised official purposes. Available records indicate use outside the approved purpose. Even where individual calls may appear minor in isolation, repeated unauthorised use by a deployed resource reflects disregard of workplace controls and compounds the pattern of indiscipline. The Consultant has not shown an adequate preventive or corrective control. This issue is held established for contractual purposes.

Issue 7: Supervision, prior communication and corrective action by the Consultant

The Consultant was responsible for supervision, governance, discipline and corrective control over its deployed resources. A prior warning had been given under the direction of the CISO concerning conduct and protocol. The recurrence and breadth of the present issues demonstrate that supervision and corrective action were ineffective. The Consultant cannot avoid contractual responsibility by treating the conduct as solely personal to the Concerned Resource. This issue is held established.

Issue 8: Attribution to the Consultant

The Concerned Resource was deployed by the Consultant to perform the Contract and operated within the access and opportunity created by that deployment. The Consultant was contractually responsible for selection, background verification, supervision, conduct, attendance, access discipline and replacement of its Experts. The established defaults are therefore attributable to the Consultant for contractual purposes, without prejudice to separate individual responsibility.

G. Grounds for termination

1. On the basis of Issues 1 to 8, read cumulatively and not in isolation, the Competent Authority finds material and fundamental defaults involving integrity, unauthorised representation, conflict of interest, misuse of entrusted access/information, information-security discipline, official-facility use and inadequate supervision. The defaults strike at the foundation of a cybersecurity and data-privacy engagement, where trust, controlled access and faithful conduct are essential and cannot be restored merely through substitution of one resource.

2. SCN functioned as the Notice of Default and the Consultant's explanation did not satisfactorily resolve the defaults within the opportunity afforded. DGMA is therefore entitled to terminate for default under paragraph 10.8.3 of the Manual, read with the Contract, without compensation and without prejudice to accrued rights, recovery, performance-security, confidentiality, data-protection, vigilance and debarment remedies.

3. The decision is proportionate to the nature of the engagement and the cumulative risk. Lesser measures would require DGMA to continue a privileged cybersecurity engagement despite unresolved integrity and access-control concerns. Public interest, operational continuity and protection of DGMA systems and information require immediate cessation coupled with controlled exit obligations.

H. Operative orders

l. Termination: The Contract dated 27.03.2026 between DGMA and MIS A3S Tech and Company is hereby terminated for default under paragraph 10.8.3 of the Manual for Procurement of Consultancy Services, Second Edition, 2025, read with the applicable provisions of the Contract and the findings in this Order. This Order constitutes the written Notice of Termination for Default. NO compensation, termination charge, loss of profit or expectancy claim shall be payable merely by reason of termination.

2. Effective date: The termination shall take effect from the issuance of this letter, the Consultant shall cease representing itself as an authorised DGMA consultant, except solely for the limited purpose of completing written exit directions.

3. Cessation Of Phase 2 / scope expansion: Any proposed Phase 2 onboarding or scope expansion is withdrawn/closed and shall not be acted upon. NO further resource shall be onboarded, and no additional scope shall be assigned under or in continuation of the terminated Contract.

4. Immediate access control : All physical, logical, remote, VPN, cloud, API, application, infrastructure, email, collaboration, repository and administrative access of all Consultant personnel shall be suspended/revoked immediately, unless a named account is temporarily retained by written CISO approval solely for controlled handover. All credentials shall be rotated and revocation evidence placed On record.

5. Exit and transition. : The Consultant shall comply with the TOR and a written exit plan issued by DGMA. Handover shall include all deliverables, source code, scripts, configurations, inventories, dashboards, reports, risk registers, logs, credentials, licences, repositories, working papers and pending action trackers. DGMA may prescribe a shorter, security-controlled handover schedule notwithstanding any general exit period.

6. Data, records and property. All DGMA data and materials shall be returned against an inventory. The Consultant and its personnel shall preserve relevant electronic and physical records and shall not delete, alter, conceal or destroy them. After verified transfer, the Consultant shall issue a signed

certificate confirming deletion Of DGMA data from its 11-33/12/2024-COMP - DGS systems, backups and personnel devices, subject to lawful retention directions.

7. Confidentiality and non-representation: Confidentiality, data protection, intellectual property, audit, indemnity, limitation-of-liability and dispute-resolution obligations shall survive termination. The Consultant and its personnel shall not disclose DGMA information or hold themselves Out as representing DGMA.

8. Payments: Payment, if any, shall be limited to services actually rendered, verified and accepted up to the Effective Date, subject to attendance, SLA, deductions, tax, set-off, recovery and exit compliance. NO payment shall be due for unauthorised absence, non- deployment, suspended access or unaccepted deliverables. Final payment shall be considered only after CISO/competent-authority exit sign-off.

9. Deductions, recovery and other remedies: DGMA may assess and recover contractual deductions, penalties, liquidated damages, loss, replacement/transition cost and other sums lawfully due, after computation and opportunity where required. Termination shall not prejudice accrued rights or liability for services already supplied.

10. Audit, vigilance and legal action.: DGMA reserves the right to conduct or require audit/forensic review and to refer the matter to the CVO, vigilance authorities, police, regulators, GeM, the administrative Ministry or any Other competent authority. NO finding in this Order shall preclude independent action under applicable law.

11. Performance Bank Guarantee.: DGMA shall retain Performance Bank Guarantee NO. 0201 IGP261133880 dated 27-02.2026 for 3,61,080 /- issued by Kotak Mahindra Bank Ltd. It shall not be released until all obligations, including exit completion, are formally closed (SCC 6.2(1)). The Consultant shall keep it valid, and shall extend its validity if required, until closure. DGMA may invoke and appropriate it, in accordance with its terms and after determination of recoverable amounts, towards any Sum due or recoverable from the Consultant, including penalties, deductions, loss and damage, and consequences of non- compliance with exit obligations.

12. Compliance report.: The Consultant shall submit a signed closure and compliance report, together with inventories and certificates by DGMA, within the timeline communicated by the CISO Office. Failure shall be recorded as continuing non-compliance and may trigger recovery, security invocation and further proceedings.

13. Debarment and Government-wide blacklisting.: In view of the findings and after consideration of the opportunity already afforded on the Code-of-Integrity allegations, M/s A3S Tech and Company and its successors are debarred for two years from participating in procurement processes undertaken by DGMA, under GFR 2017 Rule 151(iii), read with Rule 151(iv) and the Department of Expenditure Guidelines dated 02.11.2021 as amended on 08.05.2026. This firm may be debarment or blacklisted. For debarment across all Central Government Ministries/Departments, the matter shall be forwarded through the administrative Ministry, with approval of the competent Secretary and a self-contained note with the complete record, to the Department of Expenditure and Ministry of Electronics and Information Technology for decision under the amended Guidelines. Until such Government-wide order is Issued by the competent authority, this Order shall not be represented as an all-Government debarment.

14. Communication and publication.: This Order shall be issued upon the Consultant by official email and Other approved mode, placed on the procurement/contract file, and communicated to the concerned DGMA divisions, GeM and the administrative Ministry to the extent prescribed by applicable rules and instructions.

15. Right to remedies: Any contractual dispute may be pursued strictly in accordance with the dispute-resolution provisions Of the Contract. The filing of any representation or dispute shall not, by itself, Stay the access-control, record-preservation, confidentiality, exit or security directions in this Order.

This Order is issued with the approval of the Competent Authority and shall be implemented with effect from the Effective Date of Termination. The matters recorded herein stand concluded for the purpose of this contractual determination; no further reply is invited. Any representation or proceeding, if made or initiated under the applicable contractual or legal provisions, shall not by itself operate as a stay of this Order or of the access-control, record-preservation, confidentiality, exit and security directions contained herein.

This issue with approval of competent authority.

26 Oct. 26

(Deependra Singh Bisen)
Chief Information Security Officer(CISO)
Directorate General Of Maritime Administration

To,
M/S
A3S Tec & co.
13/14, Devika Tower,
Nehru Place,
New Delhi-110019

Copy to:
1. DG's Secretariat
2. Office Of the Additional Director General
3. Chief Vigilance Officer / Vigilance Section
4. DDG, IT & e-Governance
5. DDG, Finance / Accounts
6. DDG, Heading all branches in DGMA
7. Contract Management Committee
8. Computer Cell for uploading on the DGMA website
9. GeM / Administrative Ministry, as applicable
10. Ministry of Electronics and Information Technology
11. Guard file.