Government eProcurement System

eProcurement System Government of India

Tender Details

Date : 16-Oct-2025 05:03 PM

Print

Basic Details

Organisation Chain	Directorate General of Shipping		
Tender Reference Number	25-63011/39/2024-NT-DGS(comp. no.31713)		
Tender ID	2025_DGS_881682_1	**Withdrawal Allowed**	Yes
Tender Type	Open Tender	**Form of contract**	QCBS
Tender Category	Services	**No. of Covers**	2
General Technical Evaluation Allowed	Yes	**ItemWise Technical Evaluation Allowed**	No
Payment Mode	Offline	**Is Multi Currency Allowed For BOQ**	No
Is Multi Currency Allowed For Fee	No	**Allow Two Stage Bidding**	No

Payment Instruments

	S.No	Instrument Type
Offline	1	Demand Draft

Cover Details, No. Of Covers - 2

Cover No	Cover	Document Type	Description
1	Fee/PreQual/Technical	.pdf	Technical Qualification Documents
		.pdf	Eligibility Criteria Documents
2	Finance	.xls	BOQ

Tender Fee Details, [Total Fee in ₹ * - 0.00]

Tender Fee in ₹	0.00		
Fee Payable To	Nil	**Fee Payable At**	Nil
Tender Fee Exemption Allowed	No		

EMD Fee Details

EMD Amount in ₹	23,45,840	**EMD Exemption Allowed**	Yes
EMD Fee Type	fixed	**EMD Percentage**	NA
EMD Payable To	Directorate General of Shipping	**EMD Payable At**	Mumbai

Click to view modification history

Work /Item(s)

Title	Request for Proposal (RFP) for Selection of System Integrator for development of Platform for the Indian Global Maritime Safety Platform (IGMSP) for Directorate General of Shipping, the Ministry of Ports, Shipping and Waterways (MoPSW), Govt. of Ind				
Work Description	Request for Proposal (RFP) for Selection of System Integrator for development of Platform for the Indian Global Maritime Safety Platform (IGMSP) for Directorate General of Shipping, the Ministry of Ports, Shipping and Waterways (MoPSW), Govt. of Ind				
Pre Qualification Details	Please refer Tender documents.				
Independent External Monitor/Remarks	NA				
Show Tender Value in Public Domain	Yes				
Tender Value in ₹	11,72,92,000	**Product Category**	Miscellaneous Services	**Sub category**	NA
Contract Type	Tender	**Bid Validity(Days)**	180	**Period Of Work(Days)**	NA
Location	Directorate General of Shipping	**Pincode**	400042	**Pre Bid Meeting Place**	Online
Pre Bid Meeting Address	Meeting Link has been provided on the RFP	**Pre Bid Meeting Date**	06-Nov-2025 03:00 PM	**Bid Opening Place**	Online

Should Allow NDA Tender	No	**Allow Preferential Bidder**	No	

Critical Dates

Publish Date	16-Oct-2025 05:10 PM	**Bid Opening Date**	25-Nov-2025 03:00 PM
Document Download / Sale Start Date	16-Oct-2025 05:10 PM	**Document Download / Sale End Date**	24-Nov-2025 03:00 PM
Clarification Start Date	17-Oct-2025 10:00 AM	**Clarification End Date**	06-Nov-2025 06:00 PM
Bid Submission Start Date	07-Nov-2025 02:00 PM	**Bid Submission End Date**	24-Nov-2025 03:00 PM

Tender Documents

NIT Document

S.No	Document Name	Description	Document Size (in KB)
1	Tendernotice_1.pdf	Notice Inviting RFP	351.99

Work Item Documents

S.No	Document Type	Document Name	Description	Document Size (in KB)
1	BOQ	BOQ_926909.xls	BOQ	319.50
2	Tender Documents	RFP.pdf	RFP Document	2073.44

View GTE /QCBS Details - Indian Global Maritime Safety Platform

S.No	Particulars	Expected Value	Mandatory	Points(Weightage)
1.0	**Indian Global Maritime Safety Platform - [Request for Proposal (RFP) for Selection of System Integrator for development of Platform for the Indian Global Maritime Safety Platform (IGMSP) for Directorate General of Shipping, the Ministry of Ports, Shipping and Waterways (MoPSW), Govt. of Ind]**		Yes	
1.01	Bidder Experience-Cloud Experiences - [Bidder Experience-Cloud Experiences]	Yes	Yes	5
1.02	Bidder Experiences-Certification - [Bidder Experiences-Certification]	Yes	Yes	5
1.03	Bidder Experience-System Integration Experience in Specific sectors - [Bidder Experience-System Integration Experience in Specific sectors]	Yes	Yes	7
1.04	Bidder Experience-System Integration Experiences - [Bidder Experience-System Integration Experiences]	Yes	Yes	10
1.05	Resource Requirement-Business Analyst (01) - [Resource Requirement-Business Analyst (01)]	Yes	Yes	5
1.06	Resource Requirement-Change Management Specialist /Trainer (01) - [Resource Requirement-Change Management Specialist /Trainer (01)]	Yes	Yes	5
1.07	Resource Requirement-Cloud Infrastructure specialist (01) - [Resource Requirement-Cloud Infrastructure specialist (01)]	Yes	Yes	5
1.08	Resource Requirement-Database Administrator (01) - [Resource Requirement-Database Administrator (01)]	Yes	Yes	5
1.09	Resource Requirement-Domain Expert (01) - [Resource Requirement-Domain Expert (01)]	Yes	Yes	5
1.1	Resource Requirement-Project Manager (01) - [Resource Requirement-Project Manager (01)]	Yes	Yes	10
1.11	Resource Requirement-Solution Architect (01) - [Resource Requirement-Solution Architect (01)]	Yes	Yes	5
1.12	Technical Solutions-Compliance to Functional and Technical Requirements - [Technical Solutions-Compliance to Functional and Technical Requirements]	Yes	Yes	3
1.13	Technical Solutions-Solution Design and Approach - [Technical Solutions-Solution Design and Approach]	Yes	Yes	20
1.14	Technical Solutions-Technical Presentation - [Technical Solutions-Technical Presentation]	Yes	Yes	10

Bid Openers List

S.No	Bid Opener Login Id	Bid Opener Name	Certificate Name
1.	sumit-dgs@nic.in	Sumit Kumar	SUMIT KUMAR
2.	rjadhav-dgs@gov.in	Ritesh Suresh Jadhav	RITESH SURESH JADHAV
3.	madhavpatil.dgs@gov.in	Madhav Patil	MADHAV DAMODAR PATIL

GeMARPTS Details

GeMARPTS ID	BP3LWRI8O3ZG
Description	Not available
Report Initiated On	16-Oct-2025
Valid Until	15-Nov-2025

Tender Properties

Auto Tendering Process allowed	No	**Show Technical bid status**	Yes
Show Finance bid status	Yes	**Stage to disclose Bid Details in Public Domain**	Technical Bid Opening
BoQ Comparative Chart model	Normal	**BoQ Compartive chart decimal places**	2
BoQ Comparative Chart Rank Type	L	**Form Based BoQ**	No

TIA Undertaking

S.No	Undertaking to Order	Tender complying with Order	Reason for non compliance of Order
1	PPP-MII Order 2017	Agree	
2	MSEs Order 2012	Agree	

Tender Inviting Authority

Name	Dy. Nautical Advisor
Address	9th Floor Beta Building, i-Think Techno Campus, Kanjurmarg East, Mumbai, Maharashtra 400042

Tender Creator Details

Created By	Madhav Patil
Designation	Assistant
Created Date	16-Oct-2025 03:34 PM

नौवहन महानिदेशालय, मुंबई
DIRECTORATE GENERAL OF SHIPPING, MUMBAI

QUALITY & COST BASED SELECTION (QCBS)

(Using E-Procurement mode on Central Public Procurement Portal)

Request for Proposals (RFP)
for
Selection of vendor to establish the Indian Global Maritime Safety Platform (IGMSP) for Directorate General of Shipping Kanjurmarg(E), Mumbai

Tender Ref. No.: 25-63011/39/2024-NT-DGS(comp. no.31713)

Date of Issue: 16.10.2025

ISSUING AUTHORITY:
DIRECTORATE GENERAL OF SHIPPING, MUMBAI
Postal Address: 9th Floor Beta Building, I-Think Techno Campus, Kanjurmarg (East),
Mumbai - 400 042 (India)

E-Mail: dgship-dgs[at]nic[dot]in
Tel. No.: 91-22-25752040/41/42/43/45
(From 9:30 A.M. to 6:00 P.M.)

Disclaimer

The information contained in this Request for Proposal (RFP) document or subsequently provided to Applicants/Consultants whether verbally or in documentary or any other form by or on behalf of the Directorate General of Shipping (DGS) is provided on the terms and conditions set out in this RFP and any other terms and conditions subject to which such information is provided.

This RFP is not an agreement and does not constitute an offer or invitation by client to the prospective Applicants or any other party. Its purpose is solely to provide information that may assist Applicants in preparing their Proposals.

This RFP contains assumptions, assessments, statements, and information made by DGS in relation to the proposed consultancy. These are provided for reference purposes only and may not be complete, accurate, adequate, or correct. Each Applicant should conduct its own independent assessment, investigation, and analysis and obtain independent advice as it may deem necessary before submitting any Proposal.

The information provided herein is not intended to be an exhaustive account of applicable legal or regulatory requirements and should not be considered a complete or authoritative statement of law. DGS shall not be responsible for the accuracy or interpretation of legal provisions contained in this document.

DGS, its employees, and advisors make no representation or warranty and shall have no liability to any person including any Applicant under any law or contract for any loss, damage, cost, or expense arising from any aspect of this RFP, including its accuracy, completeness, reliability, or suitability for any particular purpose.

DGS reserves the right to amend, revise, update, or withdraw the RFP at any stage, to accept or reject any or all Proposals, and to cancel or annul the bidding process, without assigning any reason and without incurring any liability whatsoever. The issue of this RFP does not imply that client is bound to select any Applicant or to appoint the selected Consultant.

All costs associated with the preparation and submission of the Proposal, including but not limited to documentation, travel, presentations, and other expenses, shall be borne solely by the Applicant. client shall not be liable in any manner for such costs, regardless of the outcome of the selection process.

Key information at a glance

SN	Item	Description
1	Tender Ref. No.	
2	Tender Title	Selection of vendor to establish the Indian Global Maritime Safety Platform (IGMSP) for Directorate General of Shipping Kanjurmarg(E), Mumbai
3	Cost of Request for Proposals	Request for Proposals can be downloaded **free of cost** from the following websites: https://eprocure.gov.in/epublish/app https://www.dgshipping.gov.in/Content/TenderNotices.aspx
4	Date of Tender Publishing	16/10/2025; 17:00 Hrs.
5	Seek Clarification Start Date	17/10/2025; 10:00 Hrs.
6	Seek Clarification End Date	06/11/2025; 18:00 Hrs.
7	Date and time of Pre-Proposal Meeting	06/11/2025; 15:00 Hrs.
8	Start date and time for Submission of Proposals (Technical + Financial Proposals)	07/11/2025; 14:00 Hrs.
9	Last date and time for Submission of Proposals (Technical + Financial Proposals)	24/11/2025; 15:00 Hrs.
10	Date and time of opening of Technical Proposals	25/11/2025; 15:00 Hrs.
13	Help Desk No. (For E - Procurement)	E-Mail: dgship-dgs[at]nic[dot]in Tel. No.: 91-22-25752040/41/42/43/45 Primary Custodian number: 8652690051 madhavpatil.dgs@gov.in eProcurement Helpdesk no.s (New Delhi)

		0120-4200462, 0120-4001002, 0120-4001005
14	Link for accessing training schedule regarding use of e-procurement portal by Bidders may be found at:	https://eprocure.gov.in/cppp/trainingdisp
15	Authority to be contacted in case of any clarification / request for entry permission for physical visit	Name: - Capt. Harinder Singh Designation: Deputy Director General, Casualty Branch Email: - singh.harinder@gov.in

Table of Contents

Section 1 – Letter of Invitation

Proposal Reference No.:25-63011/39/2024-NT-DGS(comp. no.31713) Date: 15/10/2025

Tender Title: Request for Proposal (RFP) for Selection of System Integrator for development of Platform for the Indian Global Maritime Safety Platform (IGMSP) for Directorate General of Shipping, the Ministry of Ports, Shipping and Waterways (MoPSW), Govt. of India

1. The DGS invites online Proposals from eligible Bidders for Selection of vendor to establish the Indian Global Maritime Safety Platform (IGMSP) for Directorate General of Shipping Kanjurmarg(E), Mumbai.
2. More details pertaining to the scope of work may be seen under the Terms of Reference
   (Section V).
3. The process of Quality & Cost Based Selection (QCBS) shall be followed for selection of suitable Bidder. The Bidding process shall be conducted in an online mode on the Central Public Procurement Portal (CPPP) which is publicly accessible using the following web address: https://eprocure.gov.in/eprocure/app. Bidders can download the Request for Proposals free of cost from this portal.
4. Interested Bidders must register on the e-procurement portal and upload their technical and financial proposals separately within the stipulated time and date i.e.<enter date and time>.
5. Detailed instructions regarding online submission of proposals may be seen under Annexure I.
6. Joint ventures or consortiums are permitted to submit a proposal for this assignment.

7. The Bidder is solely responsible for timely uploading of Proposals on the e-procurement portal. DGS shall not be liable for resolving any queries / issues raised on the day of Proposal submission.
8. Technical Proposals shall be opened online at 15:00 Hrs. on 25th Nov 2025. Bidders can see the tender opening status by logging on to the e-procurement portal using their registered IDs.
9. Financial Proposals of only technically qualified Bidders shall be opened at a date which shall be pre-disclosed on the e-procurement portal.
10. DGS reserves the right to accept or reject any or all of the Proposals at any time during the Bidding process.

Deputy Director General

Section 2 – Instructions to Bidders (ITB)

1. General

1.1. Introduction

a) This Section provides the relevant information as well as instructions to assist prospective Bidders in preparation and submission of Proposals. It also includes the mode and procedure to be adopted by the DGS (hereinafter referred to as the 'Client') for receipt and opening as well as scrutiny and evaluation of Proposals and subsequent placement of award of contract.

b) The Client named in the **Data Sheet** will select an eligible consulting firm / organization (the Bidder), in accordance with the method of selection specified in the **Data Sheet**.

c) Before preparing the Proposal and submitting the same to the Client, the Bidder should read and examine all the terms & conditions, instructions etc. contained in the Request for Proposals. Failure to provide required information or to comply with the instructions incorporated in this Request for Proposals may result in rejection of Proposals submitted by Bidders.

d) The successful Bidder will be expected to complete the Services by the Intended Completion Date as provided in the **Data Sheet** and communicated in the services contract.

1.2. Language of Proposals

Proposal submitted by the Bidder and all subsequent correspondences and documents relating to the Proposal exchanged between the Bidder and the Client, shall be written in English language. However, the language of any printed literature furnished by the Bidder in connection with its Proposal may be written in any other language, provided the same is accompanied by a self-certified English translation and, for purposes of interpretation of the Proposal, the English translation shall prevail.

1.3. Code of Integrity

a) The Client and all officers or employees of the Client, whether involved in the procurement process or otherwise, or Bidders and their representatives or employees participating in a procurement process or other persons involved, directly or indirectly in any way in a procurement process shall maintain an unimpeachable standard of integrity in accordance with the code of integrity prescribed under GFR 175.

b) In case of breach of the code of integrity by a Bidder or a prospective Bidder, the DGS, after giving a reasonable opportunity of being heard, may take appropriate measures including –

i. exclusion of the Bidder from the procurement process.
ii. calling off of pre-contract negotiations and forfeiture or encashment of Proposal security;
iii. forfeiture or encashment of any other security or bond relating to procurement;
iv. recovery of payments made by the Client along with interest thereon at bank rate;
v. cancellation of the relevant contract and recovery of compensation for loss incurred by the Client;
vi. debarment of the Bidder from participation in any future procurements of any Client for a period of up to three years.

1.4. Eligibility

a) This Request for Proposals is open to all Bidders eligible as described in the instructions to Bidders. DGS employees, Committee members, Board members and their relatives (Spouse or Children) are not eligible to participate in the tender. Bidders involved in corrupt and fraudulent practices or debarred from participating in Public Procurement by any state government or any procuring entity of the central government shall not be eligible.

b) The specific eligibility conditions shall be as prescribed under the **Data Sheet**.

c) Bidders shall submit a declaration regarding its eligibility vis-à-vis all the criteria mentioned under the instructions to Bidders and the Proposal data sheet.

1.5. Online Proposal Submission Process

The e-tender is available on CPPP portal, https://eprocure.gov.in/eprocure/app as mentioned in the tender. The tenders duly filled in should be uploaded and submitted online on or before the end date of submission. More details regarding the online Proposal submission process may be found under Annexure-II attached to this Request for Proposals.

2. Request for Proposals

2.1. Contents of Request for Proposals

a) The Request for Proposals include the following Sections, which should be read in conjunction with any amendment issued in accordance with ITB.

➢ Section 1	Invitation for Bidders
➢ Section 2	Instructions to Bidders (ITB)
➢ Section 3	Data Sheet
➢ Section 4	Evaluation Criteria
➢ Section 5	Terms of Reference
➢ Section 6	Service Level Agreement
➢ Section 7	Bidding Forms
➢ Section 8	General Conditions of Contract (GCC)
➢ Section 9	Special Conditions of Contract (SCC)
➢ Section 10	Contract Forms
➢ Financial Proposal Template in MS Excel format	

b) Unless downloaded directly from the DGS website (https://www.dgshipping.gov.in) or the e-procurement portal https://eprocure.gov.in/eprocure/app as specified in the **Data Sheet**, Client shall not be responsible for the correctness of the Request for Proposals, responses to requests for clarification, the Minutes of the Pre-Proposal meeting, if any, or Amendment(s) to the Request for Proposals in accordance with ITB.

c) Bidders are expected to examine all instructions, forms, terms, and specifications in the Request for Proposals and to furnish with its Proposal all information or documentation as is required by the Request for Proposals.

2.2. Clarification of Request for Proposals

a) A Bidder requiring any clarification of the Request for Proposals shall contact the DGS in writing / email at the Client's address specified in the D**ata Sheet**.

b) The Client will respond in writing / email / through the e-procurement portal to any request for clarification, provided that such request is received prior to the deadline for submission of Proposals within a period specified in the **Data Sheet**. The Client shall also promptly publish brief description of the enquiry but without identifying its source and its response at its website or on the e-procurement portal.

c) Should the clarification result in changes to the essential elements of the Request for Proposals, the Client shall amend the Request for Proposals following the procedure given under ITB.

d) The queries should necessarily be submitted in the following format

Name of	Designation	Email ID(s)	Tel. Nos. & Fax Nos.

S. No	RFP Document Reference (s) (Page Number and Section Number)	Content of RFP Requiring Clarification	Points of Clarification
1.			
2.			
3.			
4.			
5.			

e) DGS shall not be responsible for ensuring that the bidders' queries have been received by them. Any requests for clarifications after the indicated date and time may not be entertained by the DGS.

f) Queries must be strictly submitted only in the prescribed format (.XLS/.XLSX). Queries not submitted in the prescribed format will not be considered/ responded at all by the procuring entity.

2.3. Pre-Proposal Meeting

a) In order to provide response to any doubt regarding Request for Proposals, or to clarify issues, a pre-Proposal meeting may be scheduled, as specified in the **Data Sheet**.

b) During the pre-Proposal meeting, the clarification sought by representative of prospective Bidders shall be responded appropriately. However, they shall be asked to submit their written request by close of office next day or by e-mail for electronic record thereof. The Client shall publish written response to such requests for clarifications, without identifying its source. In case required, amendment(s), in terms of ITB below shall be issued, which shall be binding on all prospective Bidders.

2.4. Amendments to Request for Proposals

a) At any time prior to the deadline for submission of Proposals, the DGS may, for any reason deemed fit by it, amend or modify the Request for Proposals by issuing Amendment(s)/corrigendum.

b) Such Amendment(s)/corrigendum will be published on DGS's website or on the e-procurement portal and the same shall be binding on all prospective Bidders.

c) To provide prospective Bidders reasonable time for taking the corrigendum into account, DGS may, at its discretion, extend the last date for the receipt of Proposals. Notifications regarding extensions, corrigendum, will be published on the website mentioned in the tender schedule and there shall be no paper advertisement.

Bidder

d) Any Bidder who has downloaded the Request for Proposals should check the Amendment(s), if any, issued on the DGS website and on the e-procurement portal.

3. Preparation of Proposals

3.1. Documents Comprising Proposal

a) Technical Bid: The list of Documents to be submitted as part of Technical Bid is provided below.

Covering Letter – Technical Bid	Please refer Tech 3
Checklist of documents comprising Proposal	Please refer Tech 2
Letter of Proposal	Please refer Tech 1
Prequalification compliance sheet	Please refer Tech 19
Particulars of the Bidder	Please refer Tech 4
Financial Capabilities	Please refer Tech 5
Profile of Resource	Please refer Tech 6
Certificate from HR demonstrating its Organization Strength	Please refer Tech 7
Technical Solution	Please refer Tech 8
Unpriced Bill of Material	Please refer Tech 18
Approach and Methodology	Please refer Tech 9
Project Plan and development	Please refer Tech 10
Deployment of Personnel	Please refer Tech 11
Details of Experience of Bidder in Various Projects	Please refer Tech 12
List of Sub-Contractors and OEMs and their details	Please refer Tech 13
Black-listing Certificate	Please refer Tech 14
Format of Consortium Agreement	Please refer Tech 15
Bank Guarantee for Earnest Money Deposit	Please refer Tech 16
Certificate of Conformity / No Deviation	Please refer Tech 17
Declaration for No Conflict of Interest	Please refer Tech 18
Bid Security Declaration	Please refer Tech Form 20:
Compliance sheet for Functional Requirements	Please refer Annexure
Compliance sheet for Technical Requirements	Please refer Annexure

Bidder’s financial Proposal shall comprise the financial quote submitted in the excel template published along with these Request for Proposals. The Bidder shall use the financial proposal template uploaded along with this RFP for preparation of their financial proposal. The Bidder shall enter the remuneration and reimbursable rates along with applicable taxes. The Bidder shall quote the price in INR only.

3.2. Bid Security

a) Consultant who are not exempted from submission of bid security/EMD, shall furnish bid security as specified in the ***Data Sheet***. Any proposal not accompanied by Bid Security other than exempted consultant shall be rejected as non-responsive.

b) **Consultants mentioned in the *Data Sheet* are exempted from payment of EMD.**

c) Unless otherwise specified in ***Data Sheet***, the earnest money shall be valid for a period of forty-five days beyond the final bid validity period. Document for establishing submission or waiver of EMD must be uploaded.

d) The **Bid Security shall be forfeited** / Bid security declaration shall be executed under the following circumstances:

1) If the Consultant is found to have violated the Code of Integrity.
2) If the Consultant withdraws, amends, or modifies its proposal during validity period or any extension agreed by the consultant thereof.
3) If the successful Consultant fails to sign the Contract Agreement within the stipulated time after being notified of the award.
4) If the successful Consultant fails to furnish the required Performance Security within the specified time frame.
5) If the Consultant is found to have submitted false, incorrect, or misleading information or documents in support of its proposal.
6) If the Consultant engages in corrupt, fraudulent, coercive, or collusive practices in competing for the contract.

e) The Bid Security of unsuccessful consultant shall be returned without interest after expiry of the final Bid validity and latest on or before the 30th day after the signing of the Contract with the successful consultant and the furnishing of the required Performance Security.

f) The Bid Security of the successful consultant shall be returned /bid-Securing Declaration stand expired upon signing of the Contract and submission of the required Performance Security.

3.3. Cost of Preparation of Proposal:

The Consultant(s) shall bear all direct or consequential costs, losses and expenditures associated with or relating to the preparation, submission, and subsequent processing of their Proposals, including but not limited to preparation, copying, postage, delivery fees, expenses associated with any submission of samples, demonstrations, or presentations which the client may require, or any other costs incurred in connection with or relating to their Proposals. All such costs, losses and expenses shall remain with the Consultant(s), and the client shall not be liable in any manner whatsoever for the same or any other costs, losses and expenses incurred by a Consultant(s) for participation in the Procurement Process, regardless of the conduct or outcome of the Procurement Process.

3.4. Only One Proposal:

A Consultant, including any member of a joint venture, shall submit only one proposal, either independently or as part of a joint venture. If a Consultant or joint venture member participates in more than one proposal, all such proposals shall be disqualified. However, a sub-consultant or a consultant's personnel may be included as Key Experts or Non-Key Experts in multiple proposals only if the circumstances justify it and the ***Data Sheet*** permits it.

3.5. Period of Validity of Proposals

a) Proposals shall remain valid for a period of 180 days from the deadline of submission of Proposals unless otherwise specified in the **Data Sheet**.

b) In exceptional circumstances, prior to the expiration of the Proposal validity period, the Client may request Bidders to extend the period of validity of their Proposals. The request and the responses shall be made in writing. A Bidder may refuse the request without any penal repercussions. A Bidder granting the request shall not be required or permitted to modify its Proposal.

3.6. Format and Signing of Proposals

a) Documents establishing Bidder’s eligibility shall be compiled into a single PDF file. All pages in the document should be serially numbered and an index specifying contents of the Proposal should be populated at the beginning of the document.

b) The technical Proposals comprising all documents specified under ITB Clause 10 a) may be compiled into a single PDF document. All pages in the document should be serially numbered and an index specifying contents of the Proposal should be populated at the beginning of the document.

c) Authorized signatory of the Bidder shall sign, either physically or digitally, on each page of the Proposal. This signature should be accompanied by Bidder’s official seal.

d) The financial Proposal must be submitted in the MS excel template provided with the Request for Proposals. Any financial quotation in Request for Proposal (RFP) will result in disqualification of the bid.

4. Submission and Opening of Proposals

4.1. Sealing, Marking and Submission of Proposals

a) Bidders shall submit their pre-qualification (eligibility) documents as well as the technical and financial proposals online.
b) Online submission of Proposals shall be carried out in accordance with the instructions given under Annexure I.

4.2. Deadline for Submission of Proposals

a) Proposals must be received by the Client online on the e-procurement portal no later than the date and time specified in the **Data Sheet**.

b) The date of submission and opening of Proposals shall not be extended except when:
   - ➢ sufficient number of Proposals have not been received within the given time and the Client is of the opinion that further Proposals are likely to be submitted if time is extended; or
   - ➢ the Request for Proposals are required to be substantially modified as a result of discussions in pre-Proposal meeting or otherwise and the time for preparations of Proposals by the prospective Bidders appears to be insufficient for which such extension is required.

c) In cases where the time and date of submission of Proposals is extended, an amendment to the Request for Proposals shall be issued.

4.3. Late Proposals

The e-procurement portal does not permit late submission of Proposals.

4.4. Opening of Proposals

a) The pre-qualification (eligibility) documents and the technical proposals shall be opened online on the date and time stipulated in the **Data Sheet**.

b) After due evaluation of the technical Proposals, the Client shall notify the technically qualified Bidders regarding the date of financial Proposal opening by giving at least 3 days' advance notice on the e-procurement portal.

c) The financial Proposals of only technically qualified Bidders shall be opened.

5. Evaluation and Comparison of Proposals

5.1. Confidentiality

a) Information relating to the evaluation of Proposals and recommendation of contract award, shall not be disclosed to Bidders or any other persons not officially concerned with the bidding process until the same is published officially on the e-procurement portal for information of all Bidders.

b) Any effort by a Bidder to influence the Client in the evaluation or contract award decisions may result in the rejection of its Proposal.

5.2. Preliminary Examination of Proposals

a) The Proposal Evaluation Committee constituted by the Client shall conduct a preliminary scrutiny of the opened Proposals at the beginning to assess the prima-facie responsiveness and record its findings thereof particularly in respect of the following:
   - ➢ that the Proposal is complete and duly signed by authorized signatory;
   - ➢ that the Proposal is valid for the period, specified in the Request for Proposals;
   - ➢ that the Proposal is unconditional and that the Bidder; and
   - ➢ any other specific requirements put forth in the Request for Proposals.

b) Proposals failing to meet these preliminary requirements shall be treated as non-responsive and shall not be considered further for evaluation.

5.3. Immaterial non-conformities

a) The Proposal Evaluation Committee may waive non-conformities in the Proposal that do not constitute a material deviation, reservation or omission and deem the Proposal to be responsive;

b) The Proposal Evaluation Committee may request the Bidder to submit necessary information or documents which are historical in nature like audited statements of accounts, tax clearance certificate, PAN, etc. within a reasonable period of time. Failure of the Bidder to comply with the request within the given time shall result in the rejection of its Proposal;

c) The Proposal Evaluation Committee may rectify immaterial non-conformities or omissions on the basis of the additional information or documentation received from the Bidder.

5.4. Determination of Responsiveness

a) The Proposal Evaluation Committee constituted by the Client shall determine the responsiveness of a Proposal to the Request for Proposals based on the contents of the Proposal submitted by the Bidder;

b) A Proposal shall be deemed to be substantially responsive if it meets the requirements of the Request for Proposals without any material deviation, reservation, or omission where: -

   i. "deviation" is a departure from the requirements specified in the Request for Proposals;
   ii. "reservation" is the setting of limiting conditions or withholding from complete acceptance of the requirements specified in the Request for Proposals; and
   iii. "omission" is the failure to submit part or all of the information or documentation required in the Request for Proposals.

c) A "material deviation, reservation, or omission" is one that, if accepted, shall:-

   i. Effect in any substantial way the scope, quality, or performance of the subject matter of procurement specified in the Request for Proposals; or
   ii. Limit in any substantial way, inconsistent with the Request for Proposals, the rights of the Client or the obligation of the Bidder under the proposed contract; or
   iii. If rectified shall unfairly affect the competitive position of other Bidders presenting responsive Proposals;

d) The Proposal Evaluation Committee shall examine the technical aspects of the Proposal in particular to confirm that all requirements of Request for Proposals have been met without any material deviation, reservation or omission;

e) The Proposal Evaluation Committee shall regard a Proposal as responsive if it conforms to all requirements set out in the Request for Proposals, or contains minor deviations that do not materially alter or depart from the characteristics, terms, conditions and other requirements set out in the Request for Proposals, that is, there is no material deviation, or if it contains errors or oversights that can be corrected without any change in the substance of the Proposal;

f) Proposals that are not responsive or contain any material deviation shall be rejected. Proposals declared as non-responsive shall be excluded from any further evaluation.

5.5. Non-conformities, Errors and Omissions

a) Provided that a Proposal is substantially responsive, the Proposal Evaluation Committee may waive any nonconformity in the Proposal.

b) Provided that a Proposal is substantially responsive, the Client, being DGS or authorized representative may request that the Bidder submit the necessary information or documentation, within a reasonable period of time, to rectify nonmaterial nonconformities or omissions in the Proposal related to documentation requirements. Such omission shall not be related to any aspect of the price of the Proposal. Failure of the Bidder to comply with the request may result in the rejection of its Proposal.

c) Provided that a Proposal is substantially responsive, the Proposal Evaluation Committee shall rectify quantifiable nonmaterial nonconformities related to the Proposal Price. To this effect, the Proposal Price shall be adjusted, for comparison purposes only, to reflect the price of a missing or non- conforming item or component.

5.6. Evaluation of Proposals

a) Technical evaluation of proposals shall be carried out based on the criteria stipulated under 'Section 4 – Evaluation Criteria'. The evaluation committee shall not adopt any other criteria other than the ones already stipulated in the Request for Proposals.

b) The evaluation of financial Proposal will shall be including GST.

c) The Client's evaluation of a proposal may require the consideration of other factors, in addition to the Bidder's financial offer. These factors may be related to the characteristics, performance, and terms and conditions of Consultancy Services. The effect of the factors selected, if any, shall be expressed in monetary terms to facilitate comparison of Proposals, shall be specified in 'Section 4 - Evaluation Criteria'.

d) Bidders shall be asked to deliver presentation on their technical proposals as per the details provided in the **Data Sheet**. This presentation shall only cover contents of the technical proposals submitted by the Bidder. No marks shall be assigned to the presentation. The objective of the presentation round is to summarize the contents of Bidder's technical proposal for better understanding of the evaluation committee.

5.7. Right to Accept Any Proposal and to Reject Any or All Proposals

The Client reserves the right to accept or reject any Proposal, and to cancel / annul the Bidding process and reject all Proposals at any time prior to contract award, without thereby incurring any liability to the Bidders for which the Client shall keep record of clear and logical reasons properly for any such action / recall of Bidding process. In case of cancellation / annulment, all Proposals submitted and specifically, Proposal securities, shall be promptly returned to the Bidders

6. Award of Contract

6.1. Award Criteria

The Bidder obtaining the highest combined evaluation score i.e. sum of weighted technical and financial scores shall be considered for award of contract (in case of QCBS evaluation)

6.2. Notification of Award

a) Prior to the expiration of the period of Proposal validity, the Client shall notify the successful Bidder, in writing, that its Proposal has been accepted. The notification letter (hereinafter and in the Conditions of Contract and Contract Forms called the "Letter of Acceptance") shall specify the accepted contract price. The expected date of award of contract is as stipulated under **Data Sheet**.

b) Until a formal Contract is prepared and executed, the Letter of Acceptance shall constitute a binding Contract.

6.3. Other Statutory Requirements

Successful Bidder shall be required to fulfill insurance and other statutory requirements including submission of signed undertakings assuring compliance with the various standards stipulated in the conditions of contract. Failure of the successful Bidder to submit the same shall constitute sufficient grounds for the annulment of the award. In that event the Client may award the Contract to the next highest evaluated Bidder, whose Proposal is substantially responsive and is determined by the Client to be qualified to perform the Contract satisfactorily.

6.4. Signing of Contract

Promptly after notification of Award, the Client shall send the successful Bidder the Contract Agreement. Within twenty-eight days of receipt of the Contract Agreement, the successful Bidder shall sign, date, and return it to the Client.

6.5. Performance Security

a) Within twenty-eight (28) days of receiving the Letter of Award, the successful Consultant shall furnish the Performance Security as specified in the ***Data Sheet.***

b) The Performance Security shall be submitted in the form of a Bank Guarantee or Fixed Deposit Receipt (FDR) issued by a Scheduled Commercial Bank in India, in favour of the client.

c) The Performance Security shall remain valid for a period of six (6) months beyond the completion of all contractual obligations, including any extensions, if applicable.

d) Failure of the successful Consultant to submit the required Performance Security or to sign the Contract Agreement within the stipulated time shall constitute sufficient grounds for annulment of the award and forfeiture of the Bid Security. In such a case, the client reserves the right to award the contract to the next most advantageous Consultant.

e) Upon signing of the Contract Agreement and submission of the required Performance Security by the successful Consultant, the client shall promptly release the BidSecurities of both the successful and unsuccessful Consultants.

f) The Consultant shall be solely responsible for **renewing or extending** the validity and claim period of the PBG in case of non-completion of the project

g) client reserves the right to invoke the Performance Bank Guarantee in case the Consultant:

i) Fails to discharge contractual obligations during the Contract Period, or

ii) Causes any loss to client due to negligence or non-performance in project implementation as per agreed terms and conditions.

6.6. Grievance Redressal/ Complaint Procedure

a) The consultant has the right to submit a complaint or seek de-briefing regarding the rejection of his proposal, in writing or electronically, within 10 days of the declaration of techno-commercial or financial evaluation results. The complaint shall be addressed to the authority mentioned in ***Data Sheet.***

b) Within 5 working days of receipt of the complaint, the client shall acknowledge the receipt in writing to the complainant, indicating that it has been received, and the response shall be sent in due course after a detailed examination.

c) The client /authority shall convey the final decision to the complainant within 15 days of receiving the complaint. No response shall be given regarding the confidential process of evaluating Proposals and awarding the contract before the award is notified, although the complaint shall be kept in view during such a process. However, no response shall be given regarding the following topics explicitly excluded from such complaint process:

   1) Only a consultant who has participated in the procurement process, i.e., pre-qualification, Consultant registration or bidding, as the case may be, can make such representation.

   2) Only a directly affected Consultant can represent in this regard.

   3) In the case of EOI, before the submission of Technical/ financial Proposals, an application for review concerning the technical/ financial Proposal may be filed only by a consultant who has qualified in the EOI;

   4) If a technical Proposal has been evaluated before the opening of the financial Proposal, an application for review concerning the financial Proposal may be filed only by a consultant whose technical Proposal is found to be acceptable.

d) No third-party information (RFPs, evaluation results) can be sought or included in the response.

e) The following decisions of the client shall not be subject to review:

1. Determination of the need for procurement.
2. Complaints against Terms of Reference except under the premise that they are either vague or too specific to limit competition
3. Selection of the mode of procurement or RFP system.
4. Choice of the selection procedure.
5. Provisions limiting the participation of Consultants in the Procurement Process, in terms of policies of the Government
6. Provisions regarding purchase preferences to specific categories of consultants in terms of policies of the Central Government
7. Cancellation of the Procurement Process except where it is intended to subsequently re- tender the same Services.

Section 3 – Data Sheet

The following specific data for the Selection of the System Integrator to be procured shall complement, supplement, or amend the provisions in the Instructions to Bidder (ITB). Whenever there is a conflict, the provisions herein shall prevail over those in ITB

ITB Para Reference	Particulars
ITB 1.1 b)	The Client is: DGS, Address: Kanjur village Rd, 9th Floor Beta Building, i-Think Techno Campus, Kanjurmarg East, Mumbai, Maharashtra 400042 The Method of Selection of Bidder is: Quality & Cost Based Selection (QCBS)
ITB 1.1 d)	The intended completion date is <enter date>
ITB 1.4 b	In order to be considered for technical evaluation, the Bidder must satisfy the eligibility requirements stipulated under Section 4.
ITB 2.1 b)	The official website of DGS is: https://www.dgshipping.gov.in/ The e-procurement portal is: https://eprocure.gov.in/eprocure/app
ITB 2.2 a)	The Client's address for seeking clarifications is: Directorate General of Shipping, 9th Floor Beta Building,i-Think Techno Campus, Kanjurmarg (East), Mumbai - 400 042 (India) Tel. No. : 91-22-25752040/41/42/43/45 Fax.No. :91-22-25752029/35; Email: dgship-dgs[at]nic[dot]in Name: - Capt. Harinder Singh Designation: Deputy Director General, Casualty Branch Email: - singh.harinder@gov.in Queries may also be raised by using the 'seek clarifications' option available on the e-procurement portal.
ITB 2.2 b)	The Bidders may submit their requests for clarification before the seek clarification end date as will be mentioned in the E-Procurement portal.
ITB 2.3 a)	The pre-Proposal meeting shall be held electronically at 15.00 Hrs. on 06th Nov 2025.

	The web-link to attend the pre-Proposal meeting is as follows: https://teams.microsoft.com/l/meetup-join/19%3ameeting_NWU4ZjA3MzItYjVmNi00MjJkLTg4ZjgtZjczYjUyZmIxMGE3%40thread.v2/0?context=%7b%22Tid%22%3a%22cb5a1016-54aa-436e-9000-56e0cd62fa91%22%2c%22Oid%22%3a%222d27b929-b944-4a23-81de-2cfef5ce5ebd%22%7d
ITB 3.2 a)	No change. Proposals shall remain valid for a period of 180 days from the deadline of submission of Proposals.
ITB 3.2 a)	Bid Security / Earnest Money Deposit of INR 23,45,840 (Rupees Twenty Three Lakhs Forty Five Thousand ,Eight Hundred and Forty Only) valid for 90 days in the form of Demand Draft from the date of submission of bid as mentioned in the Scope of Work. Or if the Bidder is exempted from submission of EMD Bid Security Declaration shall be submitted duly signed on the letterhead of the bidder, in pursuance of Govt. of India O.M. No. F.9/4/2020-PPD dated 12/11/2020, as per the format provided. The demand draft shall be drawn in favor of "**Directorate General of Shipping Mumbai**," and shall be payable at Mumbai.
ITB 3.2 b)	Exemption from EMD: Consultants registered as: Micro and Small Enterprises (MSEs) under the MSME Act, or Start-ups recognized by the Department for Promotion of Industry and Internal Trade (DPIIT), or Consultants registered with Central Purchase Organizations (CPOs) for the services under this RFP, are exempted from payment of EMD upon submission of valid supporting documents. Bid Security Declaration (Mandatory for Exempted Consultants): Consultants claiming exemption from EMD payment must mandatorily submit a signed Bid Security Declaration in the format provided in Section 6. Failure to submit the declaration shall result in disqualification of the bid.
ITB 3.5 a)	Proposals shall be valid for 180 calendar days from the last date of submission of proposal
ITB 4.2 a)	The client shall use the following electronic-procurement system to manage this Request for Proposal (RFP) process: Central Public Procurement Portal (CPPP) https://eprocure.gov.in/eprocure/app The Proposals must be uploaded on the e-procurement portal specified in ITC 1(m) no later than: Date: 24/11/2025 Time: 15:00 Hrs.
ITB 4.4 a)	Technical proposal will be opened on the e-procurement portal by the client's Evaluation Committee at the date and time indicated below. Date: 25/11/2025 Time: 15:00 Hrs.
ITB	The presentations shall be held online using Microsoft Teams / offline within a week after

5.6 d)	opening of the technical proposals. The specific dates, time and meeting links shall be notified by the client on its website i.e. https://www.dgshipping.gov.in/ and also will be communicated via respective emails.
ITB 6.2 a)	The expected date of award of contract is .
ITB 6.5	The Performance Security shall be 3%..of the total contract value

7. Annexure I - Instructions for Online Proposal Submission

Bidders are required to submit soft copies of their Proposals electronically on the CPP Portal, using valid Digital Signature Certificates. The instructions given below are meant to assist the Bidders in registering on the CPP Portal, prepare their Proposals in accordance with the requirements and submitting their Proposals online on the CPP Portal.

7.1. Registration

i. Bidders are required to enroll on the e-Procurement module of the Central Public Procurement Portal (URL: https://eprocure.gov.in/eprocure/app) by clicking on the link “Online Bidder Enrollment” on the CPP Portal which is free of charge.

ii. As part of the enrolment process, the Bidders will be required to choose a unique username and assign a password for their accounts.

iii. Bidders are advised to register their valid email address and mobile numbers as part of the registration process. These would be used for any communication from the CPPP.

iv. Upon enrolment, the Bidders will be required to register their valid Digital Signature Certificate (Class III Certificates with signing key usage) issued by any Certifying Authority recognized by CCA India (e.g. Sify / nCode / eMudhra etc.), with their profile.

v. Only one valid DSC should be registered by a Bidder. Please note that the Bidders are responsible to ensure that they do not lend their DSC’s to others which may lead to misuse.

vi. Bidder then logs in to the site through the secured log-in by entering their user ID / password and the password of the DSC / e-Token.

7.2. Searching for Tender Documents

i. There are various search options built in the CPP Portal, to facilitate Bidders to search active tenders by several parameters. These parameters could include Tender ID, Organization Name, Location, Date, Value, etc. There is also an option of advanced search for tenders, wherein the Bidders may combine a number of search parameters such as Organization Name, Form of Contract, Location, Date, Other keywords etc. to search for a tender published on the CPP Portal.

ii. Once the Bidders have selected the tenders they are interested in, they may download the required documents / tender schedules. These tenders can be moved to the respective ‘My Tenders’ folder. This would enable the CPP Portal to intimate the Bidders through SMS / e-mail in case there is any corrigendum issued to the tender document.

iii. The Bidder should make a note of the unique Tender ID assigned to each tender, in case they want to obtain any clarification / help from the Helpdesk.

7.3. Preparation of Proposals

i. Bidder should take into account any corrigendum published on the tender document before submitting their Proposals.

ii. Please go through the tender advertisement and the tender document carefully to understand the documents required to be submitted as part of the Proposal. Please note the number of covers in which the Proposal documents have to be submitted, the number of documents - including the names and content of each of the document that need to be submitted. Any deviations from these may lead to rejection of the Proposal.

iii. Bidder, in advance, should get ready the Proposal documents to be submitted as indicated in the tender document / schedule and generally, they can be in PDF / XLS / RAR / DWF/JPG formats. Proposal documents may be scanned with 100 dpi with black and white option which helps in reducing size of the scanned document.

iv. To avoid the time and effort required in uploading the same set of standard documents which are required to be submitted as a part of every Proposal, a provision of uploading such standard documents (e.g. PAN card copy, annual reports, auditor certificates etc.) has been provided to the Bidders. Bidders can use "My Space" or "Other Important Documents" area available to them to upload such documents. These documents may be directly submitted from the "My Space" area while submitting a Proposal, and need not be uploaded again and again. This will lead to a reduction in the time required for Proposal submission process.

Note: My Documents space is only a repository given to the Bidders to ease the uploading process. If Bidder has uploaded his Documents in My Documents space, this does not automatically ensure these Documents being part of Technical Proposal.

7.4. Submission of Proposal

i. Bidder should log into the site well in advance for Proposal submission so that they can upload the Proposal in time i.e. on or before the Proposal submission time. Bidder will be responsible for any delay due to other issues.

ii. The Bidder has to digitally sign and upload the required Proposal documents one by one as indicated in the tender document.

iii. Bidder has to select the payment option as "offline" to pay the tender fee / EMD as applicable and enter details of the instrument.

iv. Bidder should prepare the EMD as per the instructions specified in the tender document. The original should be posted/couriered/given in person to the concerned official, latest by the last date of Proposal submission or as specified in the tender documents. The details of the DD/any other accepted instrument, physically sent, should tally with the details available in the scanned copy and the data entered during Proposal submission time, otherwise the uploaded Proposal will be rejected.

v. Bidders are requested to note that they should necessarily submit their financial Proposals in the format provided and no other format is acceptable. If the price Proposal has been given as a standard BoQ format with the tender document, then the same is to be downloaded and to be filled by all the Bidders. Bidders are required to download the BoQ file, open it and complete the white coloured (unprotected) cells with their respective financial quotes and other details (such as name of the Bidder). No other cells should be changed. Once the details have been completed, the Bidder should save it and submit it online, without changing the filename. If the BoQ file is found to be modified by the Bidder, the Proposal will be rejected.

vi. The server time (which is displayed on the Bidders' dashboard) will be considered as the standard time for referencing the deadlines for submission of the Proposals by the Bidders, opening of Proposals etc. The Bidders should follow this time during Proposal submission.

vii. All the documents being submitted by the Bidders would be encrypted using PKI encryption techniques to ensure the secrecy of the data. The data entered cannot be viewed by unauthorized persons until the time of Proposal opening. The confidentiality of the Proposals is maintained using the secured Socket Layer 128-bit encryption technology. Data storage encryption of sensitive fields is done. Any Proposal document that is uploaded to the server is subjected to symmetric encryption using a system generated symmetric key. Further this key is subjected to asymmetric encryption using buyers/Proposal opener's public keys. Overall, the uploaded tender documents become readable only after the tender opening by the authorized Proposal openers.

viii. The uploaded tender documents become readable only after the tender opening by the authorized Proposal openers.

ix. Upon the successful and timely submission of Proposals (i.e. after Clicking "Freeze Proposal Submission" in the portal), the portal will give a successful Proposal submission message & a Proposal summary will be displayed with the Proposal no. and the date & time of submission of the Proposal with all other relevant details.

x. The Proposal summary has to be printed and kept as an acknowledgement of the submission of the Proposal. This acknowledgement may be used as an entry pass for any Proposal opening meetings.

7.5. Assistance to Bidders

i. Any queries relating to the tender document and the terms and conditions contained therein should be addressed to the Tender Inviting Authority for a tender or the relevant contact person indicated in the tender.

ii. Any queries relating to the process of online Proposal submission or queries relating to CPP Portal in general may be directed to the 24x7 CPP Portal Helpdesk.

Bidders may avail the free training on the use of e-procurement system as per the schedule published at the following link: https://eprocure.gov.in/cppp/trainingdisp. In case of any further queries, please contact Shri Vikram Satre at +91-82865-87409 during office hours i.e. between 10 AM till 6 PM on weekdays.

Section 4 – Evaluation Criteria

This Section contains all the criteria that the DGS shall use to evaluate Proposals and qualify the Bidders. No other factors, methods or criteria shall be used for the purpose of evaluation.

i. The overall objective of this evaluation process is to select the capable and qualified firm in the business domain of developing and rolling out the integrated application, related hardware and other infrastructure, providing associated capacity building, training and handholding support as well as associated managed services and who will provide a comprehensive solution towards Supply, Installation, Integration, Commissioning, Development, Deployment, Operation & Management of the said system and hardware provisioning at DGS.

ii. First the Pre-Qualification Proposal will be evaluated and only those bidders who qualify the requirements will be eligible for next set of evaluations. Technical Proposal and Commercial Proposal of Bidders who do not meet the Pre-Qualification criteria shall not be evaluated.

iii. The technical score of all the bidders would be calculated as per the criteria mentioned below. All the bidders who achieve at least 70% marks in the technical evaluation would be eligible for the next stage, i.e., Financial Bid opening.

iv. Proposals of bidders would be evaluated as per Technical Evaluation Criteria.

8. Assessment of Eligibility

The Bidder's proposals shall be first assessed for eligibility based on the eligibility criteria stipulated below. Only those Bidders who are found to be eligible as per the stipulated criteria shall be considered for evaluation of technical proposals.

i. The prospective Bidders shall enclose documentary evidences in support of the Pre-Qualification Criteria along with the Bid.

ii. An indicative format for the Pre-Qualification Proposal is as follows [Please customize this list on the basis of Pre-Qualification Criteria Finalized below]

S. No	Criteria	Pre-qualification Criteria description	Supporting Document	Response (Yes / No)	Reference in Response to Pre-Qualification Bid (Section # and Page #)

EC#	Condition	Criteria	Supporting Documents (to be Included in the RFP)
EC1	**Legal Entity**	The Bidder/Lead bidder in case of consortium must be registered with the appropriate government authority as a pvt. ltd. company / ltd. company / LLP and shall be in the consulting services	Copy of the incorporation / registration certificate clearly indicating the nature of business. To be submitted for - • Single Bid – Bidder • Consortium Bid – Lead

EC#	Condition	Criteria	Supporting Documents (to be Included in the RFP)
		business for at least 5 years.	Bidder
EC2	**Registration Certification by the concerned authority/government**	The Bidder/Lead bidder in case of consortium must have valid registration regarding GSTIN, PAN, EPF, ESI, Labour, or equivalent registration certificate issued by the concerned authority/government as applicable to the subject Services.	Copy of certificate for Registration To be submitted for – • Single Bid – Bidder • Consortium Bid – Lead Bidder
EC3	**Declaration of Insolvency, Bankruptcy, etc.**	The Bidder/Lead bidder in case of consortium must not be insolvent, in receivership, bankrupt or being wound up, not have its affairs administered by a court or a judicial officer, not have its business activities suspended, and must not be the subject of legal proceedings for any of aforesaid reasons.	Self-Declaration on company letterhead by authorized signatory
EC4	**Conflict of Interest**	The Bidder/Lead bidder in case of consortium Must Not have a conflict of interest which substantially affects fair competition. No attempt should be made to induce any other Bidder to submit or not to submit bid to restrict competition.	Declaration by authorized signatory in Tech Form 18 In case of: • Single Bid – Bidder • Consortium Bid – All members
EC5	**Turnover**	The Bidder / lead bidder in case of consortium must have a minimum average annual turnover of INR 29 Cr. for the last three financial years ending	Copy of Audited Annual Balance sheet for last three years ending 31.03.2025 with Certificate from a CA stating Annual Turnover and the average turnover for similar projects for the last three

EC#	Condition	Criteria	Supporting Documents (to be Included in the RFP)
		31st March 2025 as evidenced by the audited accounts of the company. In case of consortium, consortium member (except Lead Bidder) must have a minimum turnover of INR 20 Crores	years. Tech Form: 5 In case of: Single Bid – Bidder Consortium Bid – Lead bidder and consortium members
EC6	**Financial: Net worth**	The bidder (for single firm) should have a positive net worth for 3 consecutive years i.e. 2022-23, 2023-24 and 2024-25 In case of a Consortium, the Lead Member must have positive net worth	Audited financial statements for the past 3 financial years. CA Certificate for 3 Years.
EC7	**Blacklisting by Govt.**	Must not be presently debarred / blacklisted by any procuring entity under the central government including PSUs and autonomous entities or by state/ UT/NCT of Delhi Governments including PSUs and its autonomous entities or by multilateral agencies such as The World Bank, Asian Development Bank, etc.	Self-declaration of not having been debarred / blacklisted by any of the entities mentioned in this criterion at present. Tech Form 14
EC8	**Technical Capability**	The Bidder (Single firm or any member of the consortium) must have System Integrator experience of successful Go-Live / completed project during the last FIVE years (from the last date of bid submission) in ONE IT/ITES project of	I. In case of completed bidder to submit Copy of work order / MSA / PO and bidder to submit Completion Certificate/Testimonial from the client. II. In case of ongoing projects bidder to submit Copy of work order / MSA / PO and proof of payment of the project(s) has

EC#	Condition	Criteria	Supporting Documents (to be Included in the RFP)
		amount not less than Rs. 5 crores OR TWO IT/ITES projects of amount not less than Rs. 2.5 crores each OR THREE IT/ITES projects of amount not less than Rs. 2 crores each Each of which includes Application Development, Software Support, training, support manpower & maintenance involving services to any state / central government organization in India and PSU in India or abroad during the last five financial years.	been received up to UAT or Proof of Go-Live of Project or Testimonial from the Client. III. The chartered accountant's certificate to the above extent indicating the name of the firm, name of the client, total value of the project and payment received as on date is to be submitted Bidder to provide project details as per Tech Form
EC9	**Certification**	The Bidder/Lead bidder in case of consortium in case of consortium must have been assessed for I. ISO 9001 for Quality Management II. ISO 27001 for Information Security Management III. CMMI Level 3 and above certification The certifications should be valid on the date of bid submission. In case the certification	Copy of valid certificate In case of: • Single Bid – Bidder • Consortium Bid – Lead bidder and Consortium members

EC#	Condition	Criteria	Supporting Documents (to be Included in the RFP)
		is under renewal, the Bidder shall provide the details of the previous certifications and the current assessment consideration in the Bid Process. Bidder to submit a valid certificate at the time of signing the contract (if selected) otherwise bidder will be disqualified. Bidder shall ensure that the certifications continue to remain valid till the end of the Agreement.	

9. Technical Evaluation Process

The evaluation committee shall carry out the preliminary examination of Proposals and shall determine the responsiveness of Proposals based as per the procedure stipulated under ITB.

1. Evaluation Criteria (QCBS)

The DGS shall evaluate the **technical proposals** on the basis of the following criteria:

#	Evaluation Criteria for the Proposed Solution	Max Marks
A	**Bidder Experience**	**27**
A.1	System Integration Experience	10
A.2	System Integration Experience in Specific sector	7
A.3	Cloud Experience	5
A.4	Certifications	5
B	**Resource Requirements**	**40**
B.1	Project Manager (01)	10
B.2	Solution Architect (01)	5

#	Evaluation Criteria for the Proposed Solution	Max Marks
B.3	Business Analyst (01)	5
B.4	Database Administrator (01)	5
B.5	Cloud Infrastructure specialist (01)	5
B.6	Domain Expert (01)	5
B.7	Change Management Specialist / Trainer (01)	5
C	**Technical Solution**	**33**
C.1	Solution Design and Approach	20
C.2	Technical Presentation	10
C.3	Compliance to Functional and Technical Requirements	3
	TOTAL	**100**

#	PARAMETER	MAX. MARKS	EVIDENCE TO BE SUBMITTED
TOTAL		**100**	
A	**Bidder Experience**	**27**	
A.1	***System Integration Experience*** The Bidder / Lead bidder in case of consortium must have system integrator experience of executing IT project for a client in last 5 years. The implementation must include IT/ITeS development/ application development/ customization and any 2 of the following: • Third Party Data center setup and operations • Training & Capacity Building • Providing Technical Manpower Support	**10**	Completed Projects: Copy of work order / MSA / PO and Completion Certificate from the client. IV. In case of completed bidder to submit Copy of work order / MSA / PO and bidder to submit Completion Certificate/Testimonial from the client. V. In case of ongoing projects bidder to submit Copy of work order / MSA / PO and proof of payment of the project(s) has been received up to UAT or Proof of Go-Live of Project or Testimonial from the Client. VI. The chartered accountant's certificate to the above extent indicating the name of

#	PARAMETER	MAX. MARKS	EVIDENCE TO BE SUBMITTED
TOTAL		100	
	• Operation and maintenance services The implementation must include application development / customization, Operations and maintenance services, Training & Capacity Building, Providing Technical Man-power Support These work orders should be from any of the State/Central Government Departments /Organizations / Public Sector Undertakings. 3 marks per project will be allotted. The bidder can submit a maximum of 4 projects. Maximum 12 marks will be awarded. **Additionally, marks will be awarded as follows for the above considered projects:** • In case the above said experience is for an Indian Government / Indian PSU client – 1 Additional Marks per project. The bidder can submit a maximum of 4 projects. Maximum 4 marks will be awarded. • In case the value of the above cited experience is > 5 Crores each – 1 Additional Marks per project. The bidder can submit a maximum of 4 projects. Maximum 4 marks will be awarded The additional criteria shall be evaluated only for the submitted projects (maximum 4).		the firm, name of the client, total value of the project and payment received as on date is to be submitted VII. In case of the project under Non - Disclosure Agreement (NDA), Company Secretary of the bidder or certifying authority of bidder should provide the certificate of completion + completion certificate from the client. Bidder to provide project details as per Tech Form 12
A.2	***Domain Experience*** The Bidder / Any member of consortium must have System Integrator experience of	**7**	Completed Projects: Copy of work order / MSA / PO and Completion Certificate from the client.

#	PARAMETER	MAX. MARKS	EVIDENCE TO BE SUBMITTED
TOTAL		**100**	
	successful Go-Live / completed project during the last FIVE years (as on the last date of bid submission) ***having Platform/ application development/ customization, Operations, and maintenance services, Training and Capacity Building, Providing Technical human resource/workforce Support*** . Each project must include implementation of any of the following: • **Maritime Regulatory and compliance platform** • **Port and logistics management system** • **Maritime safety, security and incident reporting system** • **Maritime education, certification and crew management system** • **Maritime environment and sustainable initiatives** • **Coastal and land management system** • **Integration with International maritime systems** • **Maritime Research analytics and decision support system** 4 marks per project will be allotted. A bidder can submit maximum of 2 projects. Maximum 8 marks will be awarded. **Additionally, marks will be awarded as follows for the above considered projects:** In case the above said experience is for a State/ Central Government / PSU / Autonomous Body (Under Any government law) – 1 Additional Marks per project. The bidder		I. In case of completed bidder to submit Copy of work order / MSA / PO and bidder to submit Completion Certificate/Testimonial from the client. II. In case of ongoing projects bidder to submit Copy of work order / MSA / PO and proof of payment of the project(s) has been received up to UAT or Proof of Go-Live of Project or Testimonial from the Client. III. The chartered accountant's certificate to the above extent indicating the name of the firm, name of the client, total value of the project and payment received as on date is to be submitted IV. In case of the project under Non - Disclosure Agreement (NDA), Company Secretary of the bidder or certifying authority of bidder should provide the certificate of completion + completion certificate from the client. Bidder to provide project details as per Tech Form 12

#	PARAMETER	MAX. MARKS	EVIDENCE TO BE SUBMITTED
TOTAL		100	
	can submit a maximum of 2 projects. Maximum 2 marks will be awarded.		
A.3	***Cloud Experience*** The Bidder / any consortium member should have experience in setting-up cloud solution in India during the last five years. Cloud Solution set-up would mean where the Bidder has, procured, installed, and commissioned Cloud Infrastructure (Hardware and Software). 50% marks per project will be allotted. A bidder can submit maximum of 2 projects.	5	Completed Projects: Copy of work order / MSA / PO and Completion Certificate from the client. I. In case of completed bidder to submit Copy of work order / MSA / PO and bidder to submit Completion Certificate/Testimonial from the client. II. In case of ongoing projects bidder to submit Copy of work order / MSA / PO and proof of payment of the project(s) has been received up to UAT or Proof of Go-Live of Project or Testimonial from the Client. III. The chartered accountant's certificate to the above extent indicating the name of the firm, name of the client, total value of the project and payment received as on date is to be submitted IV. In case of the project under Non - Disclosure Agreement (NDA), Company Secretary of the bidder or certifying authority of bidder should provide the certificate of completion + completion certificate from the client. Bidder to provide project details as per Tech Form 12
A.4	***Certifications**:* In case if bidder / Lead Bidder having CMMI Level 5 (DEV) certification maximum of 5 marks will be awarded OR	5	The certifications should be valid on the date of bid submission. In case of Service Providers where the CMMI certification is under renewal, the Bidder shall provide the details of the previous CMMI certification and the current assessment

#	PARAMETER	MAX. MARKS	EVIDENCE TO BE SUBMITTED
TOTAL		**100**	
	In case if bidder / Lead Bidder having CMMI Level 3 (DEV) certification maximum of 3 marks will be awarded		consideration in the Bid Process. Bidder to submit a valid CMMI certificate at the time of signing the contract (if selected) otherwise bidder will be disqualified. Bidder shall ensure that the certifications continue to remain valid till the end of the Agreement.
B	**Resource Requirements**	**40**	
B.1	***Project Manager (Full Time) (01 Nos)*** BE / BTech / MCA / MTech/ (preferable) MBA with at least 15 years of Total work experience **Award of marks will be as follows:** i. Experience of implementing end to end Projects as a Project Manager for scope as defined in the criteria A.1 • 4 – 5 Projects: 4 Marks • 2 – 3 Projects: 2 Marks • < 2 – 1 Marks ii. Experience of implementing end to end Projects as a Project Manager for scope as defined in the criteria A.2 • 4 – 5 Projects: 4 Marks • 2 – 3 Projects: 2 Marks • < 2: 1 Marks iii. Certifications: PMP / Prince2 Certification. Documentary proof to be submitted. • Certified: 2 Marks • Not Certified: 0 Marks	**10**	Signed Technical Bid Please provide resource details as per format of **“*Tech 6: Profile of Resource*”**
B.2	***Solution Architect (01 Nos.)*** BE / BTech / MCA / MTech / MBA with 10 years’ work experience **Award of marks will be as**	5	Signed Technical Bid Please provide resource details as per format of **“*Tech 6: Profile of Resource*”**

#	PARAMETER	MAX. MARKS	EVIDENCE TO BE SUBMITTED
TOTAL		**100**	
	follows: i. Experience as Solution Architect in Turnkey projects • > 5 Projects: 3 Marks • 2 to 5 Projects: 2 Marks • < 2 Projects: 1 Marks Additional 1 marks will be provided for a project with PSU / Government Bodies / Autonomous Organization (under any Indian Government law) in India to a maximum of 1 projects. ii. Certifications: TOGAF / Zachman Framework / any other relevant certification. Documentary proof to be submitted. • Certified: 1 Marks • Not Certified: 0 Marks		
B.3	***Business Analyst (01 Nos.)*** BE / BTech / MCA / MTech/ preferable MBA with at least 5 years of Total work experience **Award of marks will be as follows:** i. Total Number of Years of Experience working in India or abroad • >5 years: 3 Marks • 3 to 5 years: 2 Marks • < 3 years: 1 Marks ii. Experience of implementing end to end integrated projects as a business analyst: • 2 - 4 projects: 2 Marks • < 2 projects: 1 Marks	**5**	Signed Technical Bid Please provide resource details as per format of **“*Tech 6: Profile of Resource*”**
B.4	***Database Administrator (01***	**5**	Signed Technical Bid

#	PARAMETER	MAX. MARKS	EVIDENCE TO BE SUBMITTED
TOTAL		**100**	
	Nos) BE / BTech / MCA / MTech / MBA with at least 6 years of Total work experience **Award of marks will be as follows:** i. Number of Years of Experience working as Database Administrator (DBA) • > 6 years: 3 Marks • 3 to 6 years: 2 Marks • < 3 years: 1 Marks ii. Experience as DBA with full capability to setup and run proposed database solution independently: • >4 Projects: 2marks • 2 to 4 Projects: 1marks		Please provide resource details as per format of **“*Tech 6: Profile of Resource”***
B.5	***Cloud Infrastructure Expert (01 Nos.)*** Engineer with experience in Cloud Computing technologies (IAAS/ PAAS / SAAS) with at least 8 years of Total work experience **Award of marks will be as follows:** i. Experience in large scale Data Centre design and implementation. • >= 8years: 2 Marks • 4 to 8 years: 1 Marks • < 3 years: 0 Marks ii. Experience of managing projects where third-party cloud data center was integral part of the project scope of work • >=3 Projects: 2 Marks • 1 to 2 Projects: 1 Marks	**5**	Signed Technical Bid Please provide resource details as per format of **“*Tech 6: Profile of Resource”***

#	PARAMETER	MAX. MARKS	EVIDENCE TO BE SUBMITTED
TOTAL		100	
	• 0 Projects: 0 Marks iii. Cloud Certification from any leading Cloud OEMs • Certified: 1 Marks • Not certified; 0 Marks		
B.6	***Domain Expert (01 Nos.)*** BE / BTech / MCA / MTech/ MBA with at least 8 years of total work experience **Award of marks will be as follows:** i. Numbers of Years of Experience of implementing end to end Projects for scope as defined in the criteria A.2. • >= 8 years: 3 Marks • 4 to 8 years: 2 Marks • < 3 years: 1 Marks ii. Number of Years of Experience working in Shipping Management companies in India or abroad. • >= 5years: 2 Marks • < 5 years: 1 Marks	**5**	Signed Technical Bid Please provide resource details as per format of **“*Tech 6: Profile of Resource”***
B.7	***Change Management Specialist / Trainer (01 Nos.)*** Any graduation degree from recognized university / institute with at least 8 years of experience and at least 2 years of total work experience in all the following: a) Conducting large scale awareness, training, promotional programs.	**5**	Signed Technical Bid Please provide resource details as per format of **“*Tech 6: Profile of Resource”***

<table>
<tr><th>#</th><th>PARAMETER</th><th>MAX. MARKS</th><th>EVIDENCE TO BE SUBMITTED</th></tr>
<tr><td colspan="2"><b>TOTAL</b></td><td><b>100</b></td><td></td></tr>
<tr><td></td><td>b) Expertise in development of course material for training on technical area
c) Should have worked on at least one of project cited in criteria A1 / A2 or similar projects
<b>Award of marks will be as follows:</b>
Experience: Total Number of years as a change management expert / trainer
• > 8 years – 4 Marks
• 5 to 8 years – 3 Marks
• 2 – 4 Years – 2 Marks
• < 2 Years: 1 Marks
<b>Certificate:</b>
Providing training to government organizations: Certificate from client mentioning resource name for providing trainings.
Additional 1 mark for providing certification.</td><td></td><td></td></tr>
<tr><td><b>C</b></td><td><b>Technical Solution</b></td><td><b>33</b></td><td></td></tr>
<tr><td><b>C.1</b></td><td>Solution Design and Approach (as part of Bid Response Document)
<b>Marks will be awarded as below:</b>
○ Approach and Methodology for implementation and Operations and Maintenance - 4 Marks<table><tr><th>#</th><th>Description</th><th>Max. Marks</th></tr><tr><td>1.</td><td>Overall implementation</td><td>0.5</td></tr></table></td><td><b>20</b></td><td>Signed Technical Bid
Tech Form: 8 &amp; 9</td></tr>
</table>

<table>
<tr><th>#</th><th>PARAMETER</th><th>MAX. MARKS</th><th>EVIDENCE TO BE SUBMITTED</th></tr>
<tr><th colspan="2">TOTAL</th><th>100</th><th></th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>methodology (Objective of phases, deliverables at each phase, etc.)</td><td></td></tr>
<tr><td>2.</td><td>Methodology for performing business design</td><td>0.5</td></tr>
<tr><td>3.</td><td>Methodology for quality control and testing of configured system</td><td>0.5</td></tr>
<tr><td>4.</td><td>Methodology of internal acceptance and review mechanism for deliverables by the bidder</td><td>0.5</td></tr>
<tr><td>5.</td><td>Proposed Acceptance criteria for deliverables</td><td>0.5</td></tr>
<tr><td>6.</td><td>Methodology and approach along with proposed tools and processes which will be followed by the bidder during project implementation</td><td>0.5</td></tr>
<tr><td>7.</td><td>Change Management and Training Plan</td><td>0.5</td></tr>
<tr><td>8.</td><td>Risk and Quality management plan</td><td>0.5</td></tr>
<tr><td colspan="2"><b>Total</b></td><td><b>4</b></td></tr>
</table>
<ul><li>Solution Architecture – 4</li></ul>
</td><td></td><td></td></tr>
</table>

<table>
<tr><th>#</th><th>PARAMETER</th><th>MAX. MARKS</th><th>EVIDENCE TO BE SUBMITTED</th></tr>
<tr><td colspan="2"><b>TOTAL</b></td><td><b>100</b></td><td></td></tr>
<tr><td></td><td>Marks
<table>
<tr><th>#</th><th>Description</th><th>Max. Marks</th></tr>
<tr><td>1.</td><td>Technical/Data architecture view</td><td>1</td></tr>
<tr><td>2.</td><td>Application architecture view</td><td>1</td></tr>
<tr><td>3.</td><td>Network architecture view</td><td>0.5</td></tr>
<tr><td>4.</td><td>Data center architecture view</td><td>0.5</td></tr>
<tr><td>5.</td><td>Security architecture view</td><td>0.5</td></tr>
<tr><td>6.</td><td>End user computing view</td><td>0.5</td></tr>
<tr><td colspan="2"><b>Total</b></td><td><b>4</b></td></tr>
</table>
○ Solution Design meeting all the proposed functionalities – 7 Marks
<table>
<tr><th>#</th><th>Description</th><th>Max. Marks</th></tr>
<tr><td>1.</td><td>Proposed Solution, in detail (including various tools to be used)</td><td>1</td></tr>
<tr><td>2.</td><td>Proposed Technical architecture</td><td>1</td></tr>
<tr><td>3.</td><td>Capabilities of the proposed solution to address the functional</td><td>1</td></tr>
</table>
</td><td></td><td></td></tr>
</table>

<table>
<tr><th>#</th><th>PARAMETER</th><th>MAX. MARKS</th><th>EVIDENCE TO BE SUBMITTED</th></tr>
<tr><th colspan="2">TOTAL</th><th>100</th><th></th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>requirements</td><td></td></tr>
<tr><td>4.</td><td>Database design considerations</td><td>1</td></tr>
<tr><td>5.</td><td>Application Security Architecture</td><td>1</td></tr>
<tr><td>6.</td><td>Cloud DC DR Considerations</td><td>0.5</td></tr>
<tr><td>7.</td><td>Data Migration approach</td><td>0.5</td></tr>
<tr><td>8.</td><td>Testing approach</td><td>0.5</td></tr>
<tr><td>9.</td><td>Risk Management Plan</td><td>0.5</td></tr>
<tr><td colspan="2"><b>Total</b></td><td><b>7</b></td></tr>
</table>

○ Detailed Project Plan covering scope of work, activities & deliverables as per timelines, key personnel deployment, risk mitigation measures – 2 Marks

○ Approach towards integration with external systems – 1 Marks

○ Project Governance Methodology – 1 Marks

○ Change Management and Training – 1 Marks
</td><td></td><td></td></tr>
<tr><td><b>C.2</b></td><td>Technical Presentation
○ Understanding of the project objective
○ Approach & methodology of the proposed solution
○ Demo of the proposed system
○ Question and Answers</td><td><b>10</b></td><td>Presentation to Authorities of DGS (Inclusive of any site visit for designated DGS officials which could be done before or after the presentation). Evaluation of this shall be communicated accordingly to the committee for awarding of marks.
The bidders are expected to present their key resources which will be leading the implementation and</td></tr>
</table>

#	PARAMETER	MAX. MARKS	EVIDENCE TO BE SUBMITTED
TOTAL		100	
			whose profiles would be evaluated by the evaluation committee
C.3	Compliance to Functional Requirement specifications and Technical Requirement specifications as Listed in Annexure of the Tender	3	Signed Functional requirement compliance sheet with the Technical Bid MAF provided by OEM stating that product being proposed meets the requirement criteria as mentioned in the RFP including changes issued & Technical specification compliance sheet with the Technical Bid

Please note that:
All Resources proposed by the Bidder should be Full Time Employee with the Bidder organization for a minimum of 6 months

Bidders are required to use the format provided below and respond to each of the functional requirement, (excluding, sample forms and logic) with one of the below mentioned answer keys:

F = Fully provided "Out-of-the-Box” in proposed product /solution
C = Configuration / Customization required
N = New Development

Sr. No.	Process Type	System Requirement	Response (F/C/N)	Comments (if any)

The Bidders may also add explanatory details as necessary in the “comments” column.

Please note that:
Bidders must use only one response code per requirement.
In case of any unanswered response OR more than one response against any requirement it will be treated as “non-response”
While evaluating the key experts’ CVs, 20% weightage shall be given for their educational qualifications and remaining 80% for relevance of their work experience. The client reserves the right to assign zero marks to any key expert not meeting the minimum requirements stipulated in the Terms of Reference, and to seek replacement of the proposed key expert with a better qualified expert in case the Bidder is selected for award of contract.

Bidders must ensure that the documentary evidence submitted by them as part of their technical proposal must provide necessary information in adequate details to establish the facts without a scope for doubt. Any scanned documents being submitted must possess adequate resolution to ensure legibility without confusion. In case any information necessary for establishing Bidder’s qualifications is not clear from the documents submitted, the evaluation committee's interpretation in that regard shall be final. Incomplete or unclear documents may lead to disqualification of the Bidder.

The minimum qualifying technical score is 70 out of 100. Financial proposals of only those Bidders shall be opened who obtain at least 70 marks in the technical evaluation.

10. Commercial Bid Evaluation

i. The Financial Bids of technically qualified bidders (i.e., 70% marks) will be opened on the prescribed date in the presence of bidder representatives.

ii. Only fixed price financial bids indicating total prices for all the deliverables and services specified in this bid document will be considered.

iii. The bid price will include all taxes and levies and shall be in Indian Rupees and mentioned separately.

iv. Any conditional bid would be rejected.

v. Errors & Rectification: Arithmetical errors will be rectified on the following basis: "If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail and the total price shall be corrected. If there is a discrepancy between words and figures, the amount in words will prevail".

vi. Bidder should provide all prices as per the prescribed format provided in Annexure.

vii. Bidder should not leave any field blank. In case the field is not applicable, Bidder must indicate "0" (Zero) in all such fields.

viii. All the prices (even for taxes) are to be entered in Indian Rupees ONLY (%age values are not allowed)

ix. It is mandatory to provide breakup of all Taxes, Duties and Levies wherever applicable and/or payable. DGS shall consider all Taxes, Duties & Levies for the purpose of Evaluation

x. DGS reserves the right to ask the Bidder to submit proof of payment against any of the taxes, duties, levies indicated.

xi. The Bidder needs to account for all Out-of-Pocket expenses related to Boarding, Lodging and other related items in the commercial bids. Any additional charges have to be borne by the bidder. For evaluation of Commercial Bids, the DGS shall make appropriate assumptions to arrive at a common bid price for all the Bidders. This however shall have no co-relation with the Contract value or actual payment to be made to the Bidder

xii. The price quoted in the Commercial Proposal shall be the only payment, payable by DGS to the successful Bidder for completion of the contractual obligations by the successful Bidder under the contract, subject to the terms of payment specified as in the proposed commercial bid or the one agreed between DGS and the Bidder after negotiations.

xiii. It is mandatory to provide break up of all taxes, duties, and levies wherever applicable and/or payable. The taxes quoted in the offer should be as per the prevailing tax rates. Any subsequent increase in the tax rates or introduction of new tax will be paid by DGS. Similarly, any benefits arising due to downward revision in tax rates, or any exemptions availed by the Bidders organization should be passed on to DGS. The bid amount shall be inclusive of packing, forwarding, transportation, insurance till Go live, delivery charges and any other charges as applicable. Any other charges as applicable shall be borne by the bidder.

xiv. Percentage (%) of taxes etc. if any, to be claimed shall be indicated in the Price bid, otherwise it will be presumed that rates are inclusive of all taxes and no plea would be accepted in this regard after opening of the tenders and during the validity of the contract.

xv. The Bidders are advised not to indicate any separate discount. Discount, if any, should be merged with the quoted prices. Discount of any type, indicated separately, will not be considered for evaluation purpose. However, in the event of such an offer, without considering discount, is found to be the lowest, DGS shall avail such discount at the time of award of Contract. For future purposes, Unit prices of all individual components will be discounted accordingly (by the overall discount % in case overall discount % is given or by the individual component discount % in case item wise discount given) to arrive at component-wise unit prices.

11. Appointment of System Integrator

11.1. Award Criteria

i. Evaluation criteria proposed to be adopted will be Quality cum Cost Based System (QCBS) where Technical Bid Score will get a weightage of 70% and Commercial Bid Score a weightage of 30%.

ii. The bidder would be technically evaluated out of 100 marks. All the bidders who secure overall minimum of 70% (70 Marks out of 100 across all the components together) will be considered as technically qualified. Technical score of all bidders will be calculated based on the following formula:

iii. Technical Score of bidders (TS) = Technical Marks received by the bidder x 70%

iv. The Bid having the Lowest Commercial Quote shall be termed as the Lowest Evaluated Bid and will be awarded 100 marks. Commercial score of all the other bidders will be calculated based on the following formula:

$$\text{Commercial score of bidder (CS)} = \frac{\text{Commercial Quote of the lowest bidder x 100 x 30\%}}{\text{Commercial Quote of the bidder}}$$

v. Final Score of the bidder: Final Score of each bidding party will be computed by adding the technical score and Commercial Score on the basis of the following formula:

Total Score = TS + CS

vi. The bidder whose bid has secured the "Highest Total Score" out of 100 as per above evaluation will be considered as best evaluated Bid. In case of a tie where two or more bidders achieve the same highest overall score, the bidder with the higher technical score will be invited first for negotiations

vii. DGS is not bound to accept the best evaluated bid or any bid and reserves the right to accept any bid, wholly or in part.

Example demonstrating the calculation of Technical Score and Commercial Scores is provided below:

Bidder	Marks Received by bidder	Technical Score of bidders (TS)
Bidder 1	88	61.6
Bidder 2	90	63

Bidder	Marks Received by bidder	Technical Score of bidders (TS)
Bidder 3	80	56
Bidder 4	95	66.5

Commercial Score of a bidder (CS) = {lowest discounted quote / Bidder's discounted quote} X 100 (adjusted to 2 decimals)

Bidder	Commercial Quote Provided by Bidder	Calculation of commercial score	Commercial Score of Bidder (CS)
Bidder 1	110	(110/110) *100*30%	30.00
Bidder 2	140	(110/140) *100*30%	23.571
Bidder 3	160	(110/160) *100*30%	20.625
Bidder 4	130	(110/130) *100*30%	25.385

Total Score for each bidder

Bidder	Technical Score (TS)	Commercial Score (CS)	Total Score
Bidder 1	61.6	30.00	91.60
Bidder 2	63	23.571	86.571
Bidder 3	56	20.625	76.625
Bidder 4	66.5	25.385	91.885

The bidder with the highest final score shall be treated as the successful bidder. In the above example, Bidder 4 will be treated as successful bidder.

12. Rejection Criteria

Besides other conditions and terms highlighted in the RFP document, bids may be rejected under following circumstances:

12.1. General Rejection Criteria

i. Bids not qualifying under Pre-qualification criteria.

ii. Bids submitted without or improper EMD

iii. Bids received through Fax / E-Mail except wherever required

iv. Bids which do not confirm unconditional validity of the bid as prescribed in the Tender

v. If the information provided by the Bidder is found to be incorrect / misleading at any stage / time during the Tendering Process

vi. Any effort on the part of a Bidder to influence DGS' s bid evaluation, bid comparison or contract award decisions

vii. Bids received by the DGS after the last date for receipt of bids prescribed by the DGS

viii. Bids without signature of person (s) duly authorized on required pages of the bid

ix. Bids without power of authorization and any other document consisting of adequate proof of the ability of the signatory to bind the Bidder.

x. If it is found that multiple bidders have submitted separate tenders/ quotations under different names of firms/ establishments but with common address for such establishments/ firms, are managed or governed by the same person/ persons jointly or severally, such tenders shall be liable for penal and legal action including blacklisting.

xi. If it is found that firms have tendered separately under different names for the same contract, all such tender(s) shall stand rejected and tender deposit of each such firm/ establishment shall be forfeited. In addition, such firms/ establishments shall be liable at the discretion of the DGS for further penal action including blacklisting.

xii. The Bidders not confirming unconditional acceptance of full responsibility of providing services in accordance with the Scope of work, General Terms & Conditions and Service Level Agreements of this tender.

xiii. Bidders not complying with the General Terms and conditions as stated in the Tender Documents.

xiv. Failure to furnish all information required by the Tender Document or submission of a bid not substantially responsive to the Tender Document in every respect.

12.2. Technical Rejection Criteria

i. Technical Bid containing commercial details.

ii. Revelation of Prices in any form or by any reason before opening the Commercial Bid

iii. Failure to furnish all information required by the Tender Document or submission of a bid not substantially responsive to the Tender Document in every respect.

iv. Bidders not quoting for the complete scope of Work as indicated in the Tender documents, addendum (if any) and any subsequent information given to the Bidder.

v. Bidders not complying with the Technical and General Terms and conditions as stated in the Tender Documents.

vi. The Bidder not confirming unconditional acceptance of full responsibility of providing services in accordance with the Scope of work and Service Level Agreements of this tender.

vii. If the bid does not conform to the timelines indicated in the bid.

viii. Bidder not complying with the eligibility criteria.

12.3. Commercial Rejection Criteria

i Incomplete Price Bid

- If the bidder fails to fill in all required items in the price bid or leaves sections blank, the bid will be rejected.
- Example: Omitting cost for any major line item.

ii. Non-conformance to Price Bid Format

- If the submitted price bid does not follow the structure, template, or format prescribed in the tender documents, it will be rejected.
- Example: Submitting prices in a separate Excel file when the tender requires a filled BOQ format.

iii. Excluding Taxes and Levies

- If the bidder does not include **all applicable statutory taxes and levies** (e.g., GST, duties) in the quoted total price, the bid will be considered non-compliant.
- The total bid price should be **all-inclusive**.

iv. Arithmetic Discrepancy

- If there are calculation errors in the commercial bid (e.g., totals do not match line-item sums), the bidder must correct them when notified.
- If the bidder **does not accept** the corrections made by the evaluation committee, their bid **may be rejected**.

v. Abnormally Low Bids (≤ 30% below estimate)

- If a bid is **30% or more below** the official estimated cost, it is considered **abnormally low** and will be **rejected/disqualified**.
- This prevents unrealistic pricing that could lead to poor performance or cost escalations later.

vi. Abnormally High Bids (≥ 30% above estimate)

- If a bid is **30% or more above** the official estimated cost, it is considered **abnormally high** and will be **rejected/disqualified**.
- This ensures bids are within a reasonable range of the project estimate.

vii. Incomplete Scope Quoting

- If the bidder does not quote for **the entire scope of work** mentioned in the tender and addendums (if any), their bid will be rejected.
- Partial or selective quoting is not allowed.

viii. Premature Revelation of Prices

- If the bidder reveals prices (in technical bids, presentations, emails, or any form) **before the official commercial bid opening**, their bid will be rejected.
- This ensures confidentiality and fairness in the tendering process.

13. Constitution of Team

i. Key Personnel involved in the project shall be on the permanent payrolls and have a minimum tenure of six months with the company of the Lead Bidder or any of the consortium members.

ii. The bidder should have a defined hierarchy and reporting structure for various teams that would be part of the project.

iii. All the concerned staff should log an attendance on a daily basis at their respective reporting location.

iv. The bidder shall ensure that all the personnel identified for this project have high level of integrity. The bidder shall undertake necessary due diligence to ensure that the personnel have high standard of trustworthiness. The bidder should obtain an undertaking from each of the personnel assigned and the same should be submitted to the DGS or its nominated agencies/ partners as and when demanded by DGS or its nominated agencies/ partners. In addition, DGS could also get the background verification checks of the bidder personnel. Any information needed for this activity by DGS should be provided immediately by bidder.

v. The bidder is free to propose and deploy as many resources as possible apart from the below list for the successful and timely completion of the project. DGS or its nominated agencies / partners will provision space for Bidder personnel in its premises. For the key personnel working out of DGS' / its nominated agencies / partners office, DGS will provide them with basic office infrastructure like seating space, fan, etc. The bidder team is expected to bring their own laptops and data cards (as required).

vi. Bidder can provide additional manpower on the basis of their estimate of effort required to complete the scope of work given in of the tender.

vii. The bidder should provide sufficient Non-Key Personnel to complete the scope of work. Bidder need not submit the names of such Non-Key Personnel along with the tender.

viii. Bidder can offer more than one key personnel for a role to improve the quality of key personnel keeping in mind the scope of work as provided in the tender.

ix. For successful completion and execution of project the bidder shall have to deploy minimum resources as provided in the table below.

Sr. No.	Level	Min. No. of People	Minimum Onsite Deployment	
			During Phase I(Design & Development till Go Live)	Period (in months)
1.	Project Manager	1	100%	10.00
2.	Solution Architect	1	10%	1.00
3.	Database Administrator (DBA)	1	30%	3.00
4.	Cloud Infra Expert	1	20%	2.00
5.	Business Analyst	1	90%	9.00
6.	Domain Expert	1	80%	8.00
7.	Change Management Specialist / Trainer	1	10%	1.00

Sr. No.	Level	Min. No. of People	Minimum Onsite Deployment	
			During Phase II(O&M)	Period (in months)
1.	Project Manager	1	100% for first 6 months then 25% for the rest	13.5
2	Cloud Infra Expert	1	100% for first 6 months then 25% for the rest	13.5
3	Application Support	2	100% for first 6 months then 25% for the rest	13.5

Section 5 – Terms of Reference

14. Organizational Background of DGS

The Directorate General of Shipping (DGS), an attached office of the Ministry of Ports, Shipping and Waterways, Govt. of India, deals in matters relating to merchant shipping. The DGS deals with all matters concerning the Maritime Administration, Maritime Education and Training, development of Shipping Industry and other related subjects.

This Directorate deals with implementation of shipping policy and legislation so as to ensure the safety of life and ships at sea, prevention of marine pollution, promotion of maritime education and training in co-ordination with the International Maritime Organization, regulation of employment and welfare of seamen, development of coastal shipping, augmentation of shipping tonnage, `ination and certification of Merchant Navy Officers, Supervision and Control of the allied departments and officer under its administrative jurisdiction.

The details about DGS and its functions are available at website https://www.dgshipping.gov.in

15. Organizational Background of Casualty Branch

The Casualty Branch is a specialized division within the maritime regulatory body of a nation, tasked with the investigation and analysis of marine accidents and incidents. Its primary objective is to enhance maritime safety by identifying the causes of maritime casualties and recommending measures to prevent future occurrences. The branch operates independently from other maritime authorities to ensure impartiality and transparency in its investigations.

Duties and Responsibilities:

1. **Conducting Thorough Investigations:** The Casualty Branch is responsible for carrying out detailed investigations into marine accidents, focusing on identifying the root causes and contributing factors.
2. **Publishing Investigation Reports:** It publishes comprehensive reports that include findings, safety recommendations, and documentation of actions taken in response to each incident.
3. **Promoting Safety Awareness:** The branch plays a crucial role in increasing awareness of marine accident causes and prevention methods through educational outreach and training initiatives.
4. **International Cooperation:** It fosters international cooperation by working closely with global maritime organizations, such as the International Maritime Organization (IMO), investigation agencies of other maritime nations and participating in forums like the Marine Accident Investigators' International Forum (MAIIF).
5. **Data Analysis and Trend Monitoring**: The branch reviews and analyses statistical data on marine casualties to monitor trends and identify possible areas of concern.
6. **Regulatory Compliance:** It ensures that investigations and reporting practices comply with international conventions, such as UNCLOS, SOLAS, and the IMO Casualty Investigation Code.
7. **Annual Reporting:** The Casualty Branch publishes an annual report summarizing all preliminary investigations and inquiries undertaken during the year.

16. Purpose / Objectives

The purpose of this Request for Proposal (RFP) is to invite qualified System Integrators to develop and implement a platform to provide a unified source of maritime safety information, enabling the industry to learn from past incidents, apply best practices, and prevent future casualties, thereby promoting safer maritime operations on a global scale and also to enhance the safety of seafarers by promoting risk-free professional practices, ensuring a safer working environment at sea and in ports, and aligning with the objectives of the Global Maritime Safety Platform. The selected System Integrators will also be responsible for the operation and maintenance of the platform for a period of 3 Years, ensuring its continued efficiency and effectiveness.

The Objectives of as follows:

I. Develop a secure and transparent casualty reporting and management system that enables structured intake, anonymous reporting, evidence handling, legal documentation, timely investigations, and compliant data retention in alignment with DG Shipping regulations.

II. Implement dynamic, user-tailored dashboards for the Global Maritime Safety Platform, showcasing real-time safety metrics and trends through advanced analytics, with cross-device compatibility, comprehensive user training, and stringent data security.

III. Construct a comprehensive, multilingual repository for the Global Maritime Safety Platform to provide easy access to safety circulars and advisories, advisories on niche operational areas like pilot ladder usage, confined space entry, ballast operations, and berthing operations and IMO guidelines on maritime operations, ensuring up-to-date information dissemination and adherence to international maritime safety standards.

IV. Host a comprehensive series of 30-40maritime safety animation videos over a period of three years on streaming platform, with the development of the content to be addressed independently from the platform's scope of work which aims at reinforcing the adherence to safety and security protocols among seafarers and provide comprehensive safety training through a web-based learning management system and provide open free online courses for standardized safety and risk certification programs.

V. Develop a secure, integrated database for maritime incident management, incorporating AI and analytical tools such as Power BI, tableau etc. for standardized reporting, pattern recognition, and controlled access to bolster safety measures and support regulatory compliance.

VI. Commit to an overarching objective of zero incidents, injuries, and environmental harm across all maritime operations by fostering a safety-first culture, ensuring strict compliance with international maritime safety standards, providing comprehensive safety training, utilizing advanced technologies for real-time monitoring and data analysis, and developing effective incident response and management systems to maintain the highest levels of safety and operational efficiency.

VII. Create and maintain a centralized knowledge repository that aggregates a wide array of safety-related publications, including annual overviews of marine casualties and incidents, detailed safety analyses from data on navigation accidents, infographics from accident investigations, and a compilation of preventive measures. This repository will also feature in-depth explorations of the causes of accidents affecting personnel and ships, summaries of incidents, actions taken in response, and safety recommendations, all aimed at continuously enhancing maritime safety.

17. Scope of Work

The proposed scope of work encompasses the development of a platform which will serve as a centralized hub for maritime casualty analysis, safety learnings, and the dissemination of best practices, aiming to significantly enhance maritime safety and align with the Maritime Amrit Kal Vision, Suraksha Sarvapratham Initiatives and IMO regulations.

A. Since there is currently no existing maritime safety portal, it is challenging to provide an exact number of data users and system requests. The selected bidder will be responsible for conducting a comprehensive study to assess the overall capacity requirements, including user load, transaction volume, and system scalability. This assessment will help in designing an optimized infrastructure that ensures high availability, performance, and future scalability.

B. Bidders must conduct a feasibility study before submitting their bid at the RFP stage and include an 'Approach and Methodology' document as part of their technical bid.

The total estimated number of users for Indian Global Maritime Safety Platform on daily basis are given below:

Indian Global Maritime Safety Platform	2000 users per day

The implementation strategy for engaging a System integrator for design, development, operations and maintenance of Safety Platform would involve several key steps.

iii. Casualty Reporting and Management System:

- Casualty Reporting & Intake – Develop structured reporting mechanisms with web forms, guided wizards, guest access, authenticated submission, and secure API integrations, with configurable field validations.
- Anonymous Reporting – Enable secure anonymous reporting options with strict privacy safeguards, no PII storage, unique tracking references, and workflows for review, escalation, and trend analysis
- Assignment & Workflow Management – Implement automated and rule-based assignment of Investigation Officers, configurable workflows, SLA timers, and escalation mechanisms to ensure timely case handling.
- Evidence & Legal Documentation – Provide secure evidence management with chain-of-custody tracking, tokenized access, and version control, along with automated generation of notices, summons, and legal documents integrated with case systems.
- Timely Reporting & Compliance – Support standardized reporting templates aligned to DGS formats, enforce reporting timelines (Initial, Interim, Final, Recommendations), and enable automated reminders and escalations.
- Integration, Analytics & Retention – Integrate with AIS, weather, port, and international casualty databases, support AI-driven correlation of incidents, and

ensure compliant archival, retention, and secure deletion of records.

iv. Casualty Data Representation and Analysis Framework:

- Develop a robust incident reporting and analytics system modelled after global best practices such as EMCIP, enabling comprehensive data analysis to detect maritime safety trends and patterns.
- Design a high-performance dashboard offering 20-25 analytical insights across diverse maritime safety parameters.
- Ensure real-time data updates within the platform to provide stakeholders with the latest information and insights.
- Develop a responsive and device-agnostic interface, making the system accessible via desktops, tablets, and mobile devices.
- Provide user manuals, training resources, and technical support to ensure efficient utilization and navigation of the analytics platform.

v. Safety Circulars Repository:

- Create a centralized repository for safety circulars, advisories, compliance guidelines, and maritime safety updates, aligned with both Indian and international standards.
- Enable multilingual accessibility, allowing users to retrieve safety documentation in their preferred language.
- Integrate external links to global regulatory authorities and emergency response guidelines to enhance access to international safety standards.
- Implement secure role-based access control for authorized maritime agencies and stakeholders to update and maintain the repository.

III. Educational Video Library:

- Develop an extensive repository of animated educational videos covering key maritime safety protocols, inspired by leading global safety communication strategies.
- Organize video content into categorized learning modules for structured training and ease of reference.
- Establish a secure login facility for video content creators and stakeholders to upload new educational materials, maintaining a fresh and evolving collection of resources.

IV. Advanced Predictive Analytics and AI-Driven Safety Insights:

- Integrate AI-powered analytics to assess potential risks, incident probability, and safety trends proactively.
- Develop visually engaging and interactive dashboards with customizable analytics and safety metrics for enhanced stakeholder decision-making.
- Provide user-driven customization options for data visualization, allowing maritime professionals to tailor reports to their specific requirements.
- Implement industry-grade cybersecurity measures to protect sensitive maritime safety data from unauthorized access and breaches.

V. Achieve Safe, compliant and efficient response system:

- Ensure alignment with international maritime safety standards and best practices to enhance incident response efficiency.
- Establish a virtual platform for safety drills, crisis simulations, and capacity-building workshops to improve emergency preparedness.
- Enable a centralized command centre view for real-time monitoring and coordinated decision-making in case of maritime incidents.
- Achieve the Shell Goal Zero ambition by creating an efficient and informative platform that provides all necessary knowledge to maintain safety and security, improve risk handling situations and enhance the skills of seafarers and ship handling agencies.

VI. Publications and Knowledge Repository:

- Develop a comprehensive knowledge hub for safety reports, annual maritime incident analyses, and investigative case studies.
- Document lessons learned from major maritime incidents and provide actionable recommendations for future risk mitigation.
- Publish detailed risk assessment reports, compliance checklists, and innovative strategies for maritime safety improvement.
- Foster collaboration with global maritime safety organizations to share insights and enhance the repository with international best practices.

VII. Integration with DGcomm Portal, Crisis Management System and Third-Party System:

- Ensure seamless interoperability with the DG COMM platform for efficient data exchange and regulatory compliance tracking.
- Enable integration with third-party safety applications, ship monitoring tools, and global maritime safety networks.
- Design a flexible API architecture to facilitate future integrations with emerging maritime technologies and regulatory systems.

VIII. Capacity Building and Training Support:

- Develop training modules to enhance maritime safety awareness among seafarers, port authorities, and shipping operators.
- Establish a periodic training calendar for DGS employees to ensure continued professional development in maritime safety standards and best practices.
- The Solution Provider shall conduct end-user training and system administration training to the persons nominated by Casualty Branch.

  a) Training Requirements: Facilitation of practical training sessions to the new users and the plan for the numbers, locations, facility required in these training sessions.
  b) Training Plan: Preparation of a detailed Training plan to cover all the training needs mentioned Training programs. List of topics to be covered under various Training programs and get approval of the Casualty Branch on the Final Training topics and plan.
  c) Preparation of Training Materials: Preparation of a User Manual/Video Help for each function/module of the Software Application to be deployed. Soft copy of the same to be made available to all relevant participants.
  d) Delivery of Training: The class and the facility required in the training needs to be

planned.

e) Training Site Preparation: The selected Bidder/vendor is to provision for the training and the space at each location should be the responsibility of the Casualty Branch. It may hire an appropriate set up for the same.

IX. System Hosting, Security, and Data Retention:

- Deploy the platform on a MeitY-approved cloud infrastructure, ensuring high availability, security, and compliance with Indian data protection regulations.
- Implement a robust data retention and archival policy, allowing for secure historical data access and analysis.
- Conduct periodic security audits with CERT-IN empaneled agencies to ensure system integrity and compliance with cybersecurity standards.
- Propose the Client-side hardware requirements such as the size of processor, RAM, Storage, and network interface etc. for the smooth running of the software based on the nature of application, number of concurrent users, quantity of data etc.
- Propose the sizing of the server-side hosting infrastructure such as CPU, Memory, Storage etc. both at the Data Centre (DC) and Disaster Recovery (DR).

X. Testing:

- Design the testing strategy, including test cases, and conduct various testing phases, such as Unit Testing, System Integration Testing, Performance Testing, and User Acceptance Testing (UAT).

XI. Security Audit:

- Ensuring compliance with CERT-In Security Policy and Guidelines, the Solution Provider coordinates with a CERT-In empaneled auditor for STQC security audit conducted once for Go Live and three times during O&M period.

XII. Data Migration Requirements:

- The Solution Provider will offer Data Capture screens to ensure all relevant data is digitized. Data from the existing system should be migrated to the proposed system. If there is no digital data available, the solution provider should design a user-friendly data entry interface. By using these screens, the data entry operators to manually input the required information.
- Data integrity, validation, and rollback mechanisms must be ensured during migration.

XIII. User Acceptance Testing (UAT) & Go-Live:

- Host the beta version on a staging server, configuring user roles for testing team, and supporting UAT. The Solution Provider shall be responsible for preparing test strategy, test cases, and test results, hosting the beta version, demonstrating functionalities, and obtaining user acceptance sign-off

XIV. Software Installation & User Configuration:

- Upon acceptance and sign-off, the Solution Provider shall be responsible for deploying the software on a central server. This process includes setting up all master data as part of the installation. The Solution Provider shall also configure user roles and privileges, ensuring that authorized users have the necessary access.

XV. Operations & Maintenance:

- Provide 24/7 technical support and a helpdesk for user queries, issue resolution, and system troubleshooting.
- Establish a three-year maintenance framework, including periodic updates, security patches, and performance optimization. This will constitute support covering bug fixes, performance tuning, and security updates, followed by 36 months of AMC support for ongoing maintenance.
- Implement a feedback mechanism for continuous system improvements and enhancements based on stakeholder inputs.

18. Installation, Commissioning, Monitoring, and Maintaining Entire IT Infrastructure

I. The bidder shall be responsible for minimum impact to business operations continuity Maximum availability of services to users.

II. The bidder shall provision, configure, monitor, and maintain the entire cloud-based IT infrastructure required for the functioning of the solution. All infrastructure must be provisioned in the cloud, avoiding any hardware procurement.

III. IT infrastructure deployed should be dedicated for the project and bidder shall not be used for any other purpose.

IV. All IT infrastructure for the solution shall be provisioned in the cloud. No on-premises infrastructure should be required.

V. Bidder shall ensure warranties/ASCs/AMCs are procured for all the IT components for entire duration of the project. For all components the support from OEM to be obtained for prescribed components. There would be a mechanism to verify these details on annual basis or as required by DGS. Bidder shall warrant that the infrastructure procured for Project shall have no defects arising from design or workmanship or any act or omission..

VI. Bidder shall replace any parts/components of the IT Infrastructure supplied for project if the components are defective and during the O&M bidder shall apply all the latest upgrades/patches/releases for the software after appropriate testing

a) Bidders are to prepare and submit along with their technical proposal, the details of methodologies and computations for sizing and capacity of storage, compute, routers, switches, Internet facing IPS, backup, tape libraries, sizing of security appliances and their compute requirements. It must leverage autoscaling groups, load balancers to dynamically manage compute, storage, and bandwidth resources.

VII. The solution being deployed is expected to be hosted and running at following key physical infrastructure facilities. These are as given below:

a. Data Centre: This will be cloud based primary site for hosting the central system supporting the entire solution. This will include live production, testing and development environments.

b. Disaster Recovery Site: This will be a fully functional cloud-based disaster recovery center which will be used in case of disaster.

VIII. The responsibility shall include configuring and provisioning cloud-based infrastructure. Bidder shall also provide staff, technical and supervisory, in sufficient numbers to operate and manage the functioning of DC and DR at desired service levels.

IX. The bidder must perform an independent assessment of the infrastructure requirements for proposed system and provide a detailed BOM for the proposed infrastructure in line with the requirements of the project and performance on service level agreements. The quantities in detailed BOM after assessment may vary from the Indicative Bill of material in RFP. DGS reserves the right to add, delete, or modify the quantities in BOM basis the requirement during the assessment.

X. The architecture must ensure 99.9% uptime using load balancers, multi-AZ failover, and redundant resources. Compute and storage resources must be scalable on-demand to support concurrent users with zero performance degradation.

XI. Deployment shall include Web Servers, Application Servers, Virtual Machines (VMs), Managed Databases (SQL/NoSQL), Storage, Content Delivery Network (CDN), and Backup Services.

XII. Security infrastructure must include VPN gateways, IAM policies, WAF, endpoint protection, and VPC architecture.

18.1. Data Center and Disaster Recovery Center

A. Bidder shall host the entire application centrally at the data center. The core infrastructure shall provide:

i. Performance i.e., the system shall provide fast and steady response times (Quality of Service). The speed and efficiency of the system shall not be affected with growing volumes, especially during search operations, reporting, MIS, online processes and batch processes.

ii. Availability i.e., all components shall provide adequate redundancy with no single point of failure to ensure high availability.

iii. The systems shall be designed for 24x7 operations and meet all SLA requirements. Designing for availability assumes that the systems will fail, and therefore the systems must be configured to recover from component or server failures with minimum application outage.

iv. Version Control and Management i.e., the system shall have versioning features to track, document and process revisions made in the system

B. The cloud hosting shall include the following:

i. All compute infrastructure like web servers (VMs), application servers (VMs), database servers (VMs), etc.

ii. Software Licenses (Database, Application, VPN Clients, etc.)

iii. Cloud based data storage

iv. Backup Solution (including VMs and software)

v. Networking components like high availability switches, routers, firewalls, etc.

vi. Load Balancing components

vii. Any other components required for functioning of the solution

C. Bidder shall carry out DR drill minimum thrice every year.

D. The bidder will be responsible for all the technology, infrastructure at these sites over the period of the contract.

E. Replication technique

i. All data should be replicated between DC and DRC. There shall be no data inconsistencies issues with either data Centre sites. However, during the change from Primary DC to DR or vice-versa (regular planned changes), there should not be any data loss.

ii. Recovery Time and Point Objectives (RTO/RPO) Alignment

The CSP shall ensure that the Recovery Point Objective (RPO) is maintained at 15 minutes or less and the Recovery Time Objective (RTO) does not exceed 4 hours. If the proposed solution achieves an RTO of 2 hours, as mentioned earlier, it should be explicitly validated against business requirements.

iii. PDC and DRC shall be multi-cloud enabled and should be designed to operate in active-active or active-passive mode across different cloud providers to ensure high availability and failover flexibility.

iv. The connectivity between both sites should ensure the replication works seamless with no minimal data loss.

v. No Data Loss During Planned Switchovers - The CSP shall ensure that during regular planned changes (switching from Primary Data Center (DC) to Disaster Recovery (DR) and vice versa), there shall be no data loss. The replication mechanism should be designed to guarantee zero data loss during controlled failovers

vi. Replication should ensure that there are no data inconsistencies on both application as well as storage level. There shall be asynchronous replication of data between Primary DC and DR and the CSP will be responsible for sizing and providing the DC-DR replication link so as to meet the RTO and the RPO requirements.

vii. In event of disaster, DRC should be brought up as primary site within the defined timelines

viii. Optimized Compute Utilization at DR Site

During normal operations, the DR site shall remain fully functional. Upon failover, the compute environment must dynamically scale up to match the primary DC's capacity, ensuring seamless transition and minimal downtime while optimizing costs.

ix. Defined Pre-Requisites for Routing Requests to DR Site - The CSP must define and share a comprehensive list of pre-requisites and technical configurations necessary for routing requests to the DR site. This includes network routing dependencies, security requirements, load balancer configurations, and necessary automation steps to ensure a smooth transition in case of failover.

x. The applications infrastructure provisioned in DRC shall be capable to handle minimum 100% load at any point in time.

xi. Ensure that data replication, backup, and storage solutions are fully cloud-native and not tied to traditional physical storage architecture.

xii. The infrastructure by the bidder must be designed to avoid a “single point of failure” with redundant components to eliminate system outage.

xiii. The proposed infrastructure should have high availability i.e., there should be no disruption in services on account of routine maintenance procedures, troubleshooting, loading hardware and software revisions, patches, etc.

xiv. Services shall be available with at least 99.5% availability on the infrastructure. The bandwidth at the DR shall be scaled up to the level of Data Centre when DR is activated. In the event of a site failover or switchover, DR site will take over the active role, and all requests should be routed through DR site. The pre-requisite to route request to DR should be articulated properly and shared by service provider.

xv. The Indian Global Maritime Safety Platform (IGMSP) shall be hosted on enterprise-grade, cloud-based compute and storage infrastructure. The deployed application instance and associated database must be fully operational and adhere to the same Service Level Agreements (SLAs) as defined for the primary Data Centre (DC)Network Infrastructure and security infrastructure should be complaint with technology and security principles as mentioned later in this tender

xvi. Bidder shall carry out a detailed assessment of the LAN, WAN and Internet leased line networking requirements considering sufficient redundancy of the proposed system with respect to the scope of work.

xvii. Officials, as authorized by DGS, shall be allowed to access the systems or its components including databases, subject to such rights & privileges as DGS may decide from time to time for the purpose of testing, audit, certification, review, inspection etc.

18.2. Overall Cloud Requirements:

i. CSP should be empaneled under MeitY's "Provisional Empanelment of Cloud Service Offerings of Cloud Service providers (CSPs)" and successfully complete STQC Audit

ii. Meet any security requirements published (or to be published) by MeitY or any standards body setup / recognized by Government of India from time to time and notified to the CSP by MeitY as a mandatory standard

iii. Meet the ever-evolving security requirements as specified by CERT-In (http://www.cert-in.org.in/)

iv. The CSP data center facilities considered for cloud services should be located within India

v. The cloud infrastructure must adhere to security and compliance standards such as SOC 2, ISO 27017, and NIST, instead of traditional data center tiering models (e.g., Tier III, TIA 942). The provider should ensure a multi-cloud strategy to avoid vendor lock-in.

vi. The primary DC and the disaster recovery site should be in different seismic zones within India

vii. The Data Center should be certified for the latest version of ISO 27001:2018 and provide service assurance and effectiveness of Management compliant with SSAE 16 / ISAE 3402 standards

18.3. Cloud Service Requirements:

i. The cloud services should provide scalable, redundant, dynamic compute and storage across multiple cloud providers to avoid vendor lock-in

ii. Service shall provide users with the ability to procure and use compute and storage capabilities remotely over the SSL with multi factor authentication.

iii. Perform an Image backup of Customer VM Image information or support the ability to take an existing running instance or a copy of an instance and import / export the instance into a MeitY-approved image format.

iv. Configuration and Management of the Virtual Machine shall be enabled via a web browser over the SSL VPN clients only as against the public internet

v. The bidder must ensure that all security, patch management, vulnerability assessment, and backup tools are cloud-agnostic and not dependent on a specific CSP's tools. Third-party security solutions must be compatible with multiple cloud environments."

vi. Monitor VM up/down status and resource utilization such as RAM, CPU, Disk, IOPS and network

vii. The purchaser retains ownership of all virtual machines, templates, clones, and scripts/applications created for the organization's application

viii. The purchaser retains the right to request full copies of these virtual machines at any time.

ix. The purchaser retains ownership of loaded business solutions / bespoke software installed on the VMs

x. Support a secure administration interface - such as SSL/TLS or SSH - for the purchasing organization's designated personnel to remotely administer their virtual instance

xi. Provide the capability to dynamically allocate virtual machines based on load, with no service interruption

xii. Provide the capability to copy or clone virtual machines for archiving, troubleshooting, and testing

xiii. The CSP should provide tools and mechanism to the purchaser or its appointed agency for defining their backup requirements & policy.

xiv. The bidder must ensure that backup solutions are cloud-native, capable of functioning across multiple cloud providers and integrating with third-party disaster recovery solutions and restore activities (when required) of all the data including but not limited to files, folders, images, system state, databases and enterprise applications in an encrypted manner as per the defined policy.

xv. The Indian Global Maritime Safety Platform (IGMSP)and its supporting infrastructure must be deployable and fully operational across multiple cloud environments without dependence on proprietary features of a single CSP

xvi. Transfer data back in-house either on demand or in case of contract or order termination for any reason

xvii. CSP shall not delete any data at the end of the agreement (for a maximum of 45 days beyond the expiry of the Agreement) without the express approval of the purchaser.

xviii. Provide capability to perform live migrations (ability to move running VM's) from one host to another.

xix. Provide support to all Application Programming Interfaces (APIs) including REST API that CSP develops/provides.

xx. CSP should offer fine-grained access controls including role-based access control, use of SSL certificates, or authentication with a multi-factor authentication.

xxi. Cloud service should support auditing with features such as what request was made, the source IP address from which the request was made, who made the request, when it was made, and so on.

xxii. Purchasing organization should be permitted to bring and upload additional properly licensed non-operating system software for operation in cloud as required for the Purchasing organization solution for use within the Services by installing it directly on a VM.

xxiii. The solution must provide auto-scaling compute and storage resources to handle workload spikes dynamically. Cloud-native serverless or containerized workloads should be preferred where applicable, ensuring optimal cost and performance efficiency.

xxiv. Provide facility to configure virtual machine of required vCPU, RAM and Disk.

xxv. CSP to design the solution for different types of disks like SAS, SSD, etc. based on the application performance / SLA requirements considering the volume growth.

xxvi. CSP is responsible for Disaster Recovery Services to ensure continuity of operations in the event of failure of primary data center of the purchasing organization and meet the RPO and RTO requirements. The CSP should offer dashboard to monitor RPO and RTO of cloud infrastructure and systems.

xxvii. The Bidder (in consultation with CSP) shall clearly define the procedure for announcing DR based on the proposed DR solution. The Bidder / CSP shall also clearly specify the situations in which disaster shall be announced along with the implications of disaster and the time frame required for migrating to DR. The Bidder / CSP shall plan all the activities to be carried out during the Disaster Recovery Drill and issue a notice to the purchaser at least two weeks before such drill.

xxviii. The Bidder / CSP should offer Switchover and switchback of individual applications instead of entire system.

xxix. Any lag and/or loss in data replication should be reflected in terms of the business requirements in terms of the defined RTO and RPO impact.

xxx. Support replication of data between primary and DR cloud environment

xxxi. When the purchaser or Bidder /CSP (with prior approval of the purchaser) scales down the infrastructure services, Bidder / CSP is responsible for deleting or otherwise securing purchaser's content/data prior to VM deletion and in case deleted, shall ensure that the data cannot be forensically recovered.

xxxii. All security solutions, including firewall, IPS, DDoS mitigation, antivirus/EDR, WAF, DLP, SIEM, and IAM, must be fully cloud-agnostic and operable across multiple CSPs. No CSP-proprietary security tools should be mandated.

18.4. Cloud Operational Requirements:

i. Manage the network, storage, server and virtualization layers, to include performance of internal technology refresh cycles applicable to meet the SLAs

ii. Provide a secure, dual factor method of remote access which allows the purchaser's designated personnel (privileged users) the ability to perform duties on the hosted infrastructure

iii. Infrastructure upgrades and maintenance should be managed through cloud lifecycle management practices, ensuring seamless updates without financial impact. All the data within it shall be retained as per Data Archival Policy as defined by DGS.

iv. Bidder / CSP to perform patch management appropriate to the scope of their control including:

- Alerts on the upcoming patches via email and management portal, and ability to defer or reject patches before they are applied in the next patch cycle
- Patch approved VMs on the next available patch management change window
- Application of automated OS security patches, unless deferred or rejected by purchaser or designated agency
- Send regular approval reminders to purchaser or authorized agency designated email address five (5) days prior to patch cut-off dates
- Bidder / CSP should undertake OS level vulnerability management – all OS images created within the cloud platform are regularly patched with the latest security updates

v. Provide the artifacts, security policies and procedures demonstrating its compliance with the Security Assessment and Authorization requirements as described in Security Requirements in this RFP.

vi. Monitor availability of the servers, CSP -supplied operating system & system software, and CSP's network

vii. The Bidder / CSP is fully responsible for tech refreshes, patch management and other operations of infrastructure with regards to the cloud environment (DC and DR).

viii. Investigate outages, perform appropriate corrective action to restore the hardware, operating system, and related tools

ix. CSP should manage CSP provisioned infrastructure including VMs as per the ITIL or equivalent industry standards.

x. Comply with technology refresh requirements as mandated by CERT-IN and MeitY

xi. Software within the CSP's scope will never be more than one version behind unless deferred or rejected by MeitY / Purchaser / Purchaser's authorized agency.

18.5. Cloud Management Reporting Requirements:

i. Provide service level management reports (as per the service levels agreed in the Service Level Agreement between the purchaser and the CSP)

ii. description of major outages (including description of root-cause and fix) resulting in greater than 1-hour of unscheduled downtime within a month

iii. Helpdesk tickets reports submitted

iv. Monthly and quarterly utilization reports (peak and average volumetric details)

v. CSP should provide a portal for the purchaser (administration role) which should provide data related to:

- Utilization reports (with threshold limits defined by the user) and SLA reports
- Cloud service usage
- Helpdesk and tickets
- User profile management

vi. The Bidder should set the baseline threshold limits for cloud infra utilization.

vii. In the event of cloud infra utilization breaching the baseline threshold limits, the CSP is required to notify the purchaser and Bidder with adequate justifications for increasing baseline capacity.

viii. Installation and commissioning of Servers as per solution requirement.

ix. Installation and provisioning of Storage and backup as per solution requirement.

x. Installation and commissioning of Software (OS/VM/backup software) along with relevant and requisite patches but not limited to.

- Installation and commissioning of requisite Clusters for High Availability.
- Installation and commissioning of Network and Security equipment for providing secured network environment.
- Liaison with Network Bandwidth Service Provider for Link provisioning and commissioning.

Scope of work for infrastructure provisioning at on-cloud disaster recovery center includes the followings:

i. The entire DR setup must be cloud-hosted with virtualized security perimeters, identity-based access controls, and zero-trust architecture. The solution should allow for seamless failover and automated recovery without reliance on physical locations.

ii. Bidder to ensure scalability of the DR cloud environment considering the future growth for next 5 -7 years.

iii. All the VM, OS, DB, Middleware, application, etc version should be identical at DC and DR.

19. Methodologies to ensure Data Security & Confidentiality

19.1. Data Classification and Handling

- The bidder shall define and implement a comprehensive Data Classification Policy aligned with the sensitivity of information, categorizing it as Public, Confidential, Restricted, and Highly Confidential, in accordance with applicable government and industry standards.
- The bidder shall conduct a sensitization and classification exercise for all existing data maintained by DG Shipping, including legacy data, to bring it under the new classification framework.
- Consent mechanisms should be embedded for user data usage where applicable.
- All maritime incident reports, seafarer records, safety analytics, and regulatory documents shall be systematically tagged based on the defined classification levels and protected through appropriate access control measures.
- The bidder must enforce strict access control protocols to ensure secure handling of Personally Identifiable Information (PII), incident-related data, and any classified government communications, preventing unauthorized access, modification, or disclosure.
- Role-Based Access Control (RBAC) shall be implemented across all environments to ensure that only authorized personnel can access, process, or store sensitive datasets, with access privileges granted based on job responsibilities and reviewed periodically.

19.2. Encryption Standards

- The bidder shall ensure that all data, both at rest and in transit, is encrypted using robust cryptographic standards, with AES-256 or higher as the baseline encryption algorithm.
- All communication across the platform must use secure transmission protocols, including but not limited to HTTPS, SFTP, TLS 1.2/1.3, and SSL, to protect data integrity and confidentiality during transit.
- The bidder shall implement the use of internal trusted Root CA (Certifying Authority) certificates wherever applicable, ensuring end-to-end secure authentication within the application ecosystem.
- Encryption keys must be securely generated, stored, and managed using a Hardware Security Module (HSM) compliant with FIPS 140-2 standards or an equivalent certified vault system. Key rotation policies must align with ISO/IEC 27001 and NIST SP 800-57 guidelines.
- The bidder shall implement a Database Access Management (DAM) solution to monitor all privileged database administrative activities. The tool must provide audit trails and real-time alerts.
- Passwords, API secrets, and authentication tokens must never be stored in plaintext. They shall be securely stored using salted-hash mechanisms and industry-grade hashing algorithms such as bcrypt, PBKDF2, or equivalent.

19.3. Access Control and Identity Management

- The bidder shall implement a centralized Identity and Access Management (IAM) system that enforces Multi-Factor Authentication (MFA) for all users, especially those accessing privileged or administrative functions.
- The IAM system must ensure complete segregation of access across development, staging, and production environments, with detailed logs maintained for all administrative and user activities. These logs must be tamper-proof and auditable.
- IAM should support integration with government authentication mechanisms for Indian seafarer credentials.

19.4. Secure Software Development Life Cycle (SSDLC)

- The bidder shall adopt a Secure Software Development Life Cycle (SSDLC) across all phases of the project, incorporating threat modelling, secure coding standards, peer code reviews, and mandatory security testing at each stage of development.
- Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) tools must be integrated into the CI/CD pipeline, ensuring automated detection and remediation of vulnerabilities prior to deployment.
- The bidder shall ensure that all open-source software components are scanned for known vulnerabilities and license compliance using Software Bill of Materials (SBOM)-based analysis tools.
- Source code must be stored in a secure, access-controlled code repository with version control. Access to the repository must be restricted and must be shared with designated DG Shipping officials for oversight and transparency.

- Source code repositories and CI/CD environments must be protected with access control and integrity validation mechanisms.

- Code deployments to the production environment shall be made only after approvals through the Central Advisory Board (CAB), including DG Shipping officials. For each deployment, the hash value of the code must be recorded and maintained to ensure traceability, integrity, and accountability.

19.5. Data Hosting and Localization

- The bidder shall host the platform and all associated components exclusively on Government of India–approved cloud infrastructure, specifically MeitY-empanelled Cloud Service Providers (CSPs), ensuring complete data residency within Indian territory.
- The selected hosting partner(s) must be compliant with international and national information security standards, including ISO/IEC 27001 (Information Security Management), ISO/IEC 27017 (Cloud Security), ISO/IEC 27018 (PII Protection on Cloud), and ISMS-DC (Information Security Management System – Data Centre) guidelines.
- Under no circumstances shall any data be transferred, mirrored, or stored outside India. If exceptional cases arise, prior written approval must be obtained from DG Shipping, along with a documented justification and risk mitigation plan.

19.6. Incident Response and Reporting

- The bidder shall develop, implement, and maintain a detailed Incident Response Plan (IRP), clearly defining the roles, responsibilities, communication protocols, and response timelines for various types of security incidents.
- An Incident Response Management (IRM) form must be designed and maintained by the bidder for each incident, capturing the root cause analysis (RCA), preventive actions taken, and lessons learned.
- The bidder must notify DG Shipping within 30 minutes of detecting any breach or suspicious activity, including but not limited to application-level, server-level, operational, physical, or environmental security incidents.
- All incidents must be logged and escalated based on severity levels and must comply with CERT-In and NCIIPC guidelines regarding classification, reporting, and handling of security events.
- Post-incident analysis reports must be submitted to DG Shipping for each incident, along with documentation of corrective actions and preventive measures implemented.
- The bidder shall maintain a centralized repository of all incident records and lessons learned, along with the corresponding IRM forms. This repository must be shared with DG Shipping on a quarterly basis for review and knowledge sharing.
- An internal escalation matrix covering all key stakeholders, contact points, and escalation timelines shall be prepared and shared with DG Shipping at the start of the project, and updated promptly in case of any changes.

19.7. Logging, Monitoring, and Auditing

- The bidder shall ensure that all system, application, and user activity logs are securely stored for a minimum of three years online and seven years offline, with accessibility to DG Shipping upon request for compliance, forensic, or investigative purposes.
- Logs must be tamper-proof and accessible only to authorized system administrators. The bidder shall ensure that audit logs are reviewed internally every two weeks, and a summary report of significant events is prepared and submitted to DG Shipping monthly basis.
- The system must support real-time logging and alerting for all security events, including system logs, application logs, and user access logs, through an integrated Security Information and Event Management (SIEM) tool.
- The bidder shall provision and manage SIEM monitoring through their Security Operations Center (SOC), and bi-weekly SOC monitoring reports must be submitted to DG Shipping, covering key observations, alerts, and response actions.
- The bidder must ensure that half yearly security audits are conducted, including Server Vulnerability Assessment and Penetration Testing (VAPT) and Web Application Penetration Testing (WAPT), by an external, CERT-In empaneled agency (or equivalent approved by DG Shipping). All audit reports must be submitted half yearly to DG Shipping, with supporting evidence of issue remediation and validation.

19.8. Compliance with Cybersecurity Policies (DGS Data Std, Doc.)

- The bidder shall ensure that the platform complies with all applicable cybersecurity regulations and standards, including but not limited to: National Cyber Security Policy, Information Technology Act 2000 (and amendments),NCIIPC guidelines, DG Shipping’s internal cybersecurity guidelines, and CERT-In/MeitY advisories.
- The platform must undergo Standardization Testing and Quality Certification (STQC) and be developed in full compliance with GIGW 3.0 guidelines to ensure accessibility, usability, and security of government applications.
- The bidder shall conduct cybersecurity and information security training sessions in alignment with DG Shipping’s information security standards and submit a formal assessment report to DG Shipping post-training, summarizing training outcomes, participant attendance, and evaluation results.
- Upon the platform going live, the bidder must submit an annual training plan, outlining the schedule and content for cybersecurity awareness, secure coding, privacy, BCP/DR, and compliance topics. Records of training, including attendance sheets, training materials, and issued certificates, must be submitted to DG Shipping for audit and governance purposes.
- The selected bidder shall execute Non-Disclosure Agreements (NDAs) with all team members involved in the project, covering development, testing, operations, and support phases.
- A Roles and Responsibilities (R&R) matrix defining the complete resource

deployment plan must be submitted to DG Shipping. Authorized personnel shall be nominated to oversee adherence to the bidder's information security policies and DG Shipping's cybersecurity procedures throughout the development, operational, and maintenance phases.

- The bidder shall ensure full compliance with the Digital Personal Data Protection (DPDP) Act, 2023, including lawful processing of personal data, implementation of consent and grievance redressal mechanisms, safeguarding data through technical and organizational controls, adherence to data retention and cross-border transfer restrictions, and timely breach notification to DG Shipping as per applicable provisions.

19.9. Business Continuity and Data Recovery

- The bidder shall implement and maintain a robust Business Continuity Plan (BCP) and Disaster Recovery (DR) strategy to ensure uninterrupted platform operations and data integrity in the event of disruptions, outages, or disasters.
- The DR setup must operate in an active-active configuration, and the bidder must ensure a minimum uptime of 99.99% between the Data Centre (DC) and Disaster Recovery (DR) environments.
- The data backup schedule must include daily incremental backups, weekly full backups, and monthly encrypted offsite archival, with all backups stored within Indian jurisdiction in compliance with data localization requirements.

The DR site must be geographically separate from the primary DC, and the infrastructure and failover mechanism must meet MeitY guidelines, ensuring a maximum Recovery Time Objective (RTO) of 4 hours and clearly defined Recovery Point Objective (RPO) targets.

20. Implementation and Adherence to policies as per DGS

The bidder must apply, obtain and maintain the STQC certification for the project. The cost incurred for obtaining and maintaining the certification shall be borne by the bidder. The bidder shall get the certificate as per timelines defined failing which the subsequent payments will be deferred till the certification is obtained.

Adherence to Standards

The selected SI should ensure that the system complies with defined industry and open standards.

A. Compliance with Open Standards

The proposed system would be designed based on open standards and in line with overall system requirements, to provide for good interoperability with multiple platforms and avoid any technology or technology provider lock-in. The system should adhere to all open standards guidelines and other guidelines relevant to the project as issued by GoI

B. Compliance with Standards for State Portal, SSDG and Forms Framework

The SI while developing the Application shall take cognizance of the technicalities of the State Portal, SSDG and e-forms framework and any other guidelines issued in this regard by the Government. The SI also has to ensure that all content of the Department's Portal is as per the State Portal Framework guidelines. The web portal must comply with all the Guidelines for Indian Government Websites as defined at the following websites:

https://guidelines.india.gov.in/ and https://egovstandards.gov.in/guidelines . It is a mandatory requirement that the developed application be Web1 compliant i.e. it should look good on all resolutions and platforms and be simple as well as user friendly. Also, the functionalities developed the application should be easily accessible to all intended users.

C. Compliance with Industry Standards

In addition to above, the proposed solution has to be based on and be compliant with industry standards (their latest versions as on date) wherever applicable. This will apply to all the aspects of solution including but not limited to its design, development, security, installation, and testing. The suggested architecture must be scalable and flexible for modular expansion. It should ensure ease of integration with software / applications developed using common industry standards since the solution may be linked and connected to other sources (websites, contents, portals, systems of other Tax administrations etc.) as well as there may be loose/tight integration with backend system of other departments depending on individual service processes. The solution architecture should thus have provision to cater to the evolving requirements of the Department.

The bidder shall ensure to adherence to DGS data and security standards and ensure that the system complies with defined industry and open standards. The security standards mentioned in the below listed documents need to have adhered by the bidder.

i. Agreement for Model RFP Templates for Implementation Agencies.

ii. Interoperability Framework for e Governance (IFEG) in India by MeitY

iii. MeitY Guidelines for Procurement of Cloud Services - V 2.0

iv. DPDP Act 2023

v. UX Design Guidelines and & Design System for Government application to enhance user experience

vi. GIGW Guidelines 3.0

ii. W3C's Web Content and Accessibility Guidelines (WCAG 2.1) Rights of Persons with Disabilities Act, 2016

21. Operation and Maintenance of the platform

i. Overall monitoring and management of the systems implemented for the Project at locations, which includes administration of Infrastructure at DC (Web /Application servers, database servers, storage, etc.), Networks, and all other services ancillary to these facilities to ensure performance and availability requirements of the Project.

ii. The SI must implement 24x7 automated monitoring using a Security Information and Event Management (SIEM) system.

iii. Ensuring compliance to the uptime and performance requirements for Solution performance as defined in the tender.

iv. Implement Helpdesk solution and provide issue resolution support for addressing the issues reported by the internal users of Information systems deployed in the project.

v. 24x7 monitoring & management of availability & security of the infrastructure & assets (including data, network, servers, systems etc.) through the Safety

Platform solution implemented for Project.

vi. SLA-based support must be provided for all infrastructure issues with guaranteed resolution timelines (L1, L2, L3).

vii. Quarterly SLA compliance and incident resolution reports must be submitted.

viii. Implementation of a comprehensive security policy in respect of the digital systems and assets, to comply with the requirements of this RFP and conforming to relevant standards.

ix. Ensuring uptime, performance and other key performance requirements of DGS Project including data backup & business continuity.

x. Perform patch management, testing and installation of software upgrades issued by the OEM/vendors from time to time. These patches/upgrades, before being applied on the live infrastructure of the Data Repository at DC, shall be adequately tested. Any downtime caused due to upgrade & patches shall be to the account of the Implementation Agency and it shall not be considered as 'Agreed Service Downtime'.

xi. Ensure overall security of the solution including installation and management of Antivirus solution for protection of all the servers and systems implemented for the project, application of updates/patches etc. The antivirus patches must be updated and applied from time to time, after appropriate testing of the patches in the staging area.

xii. Develop the Standard Operating Procedures (SOPs), in accordance with the ISO 27001& ISO 20000/ITIL standards, for Project management. These SOPs cover all the aspects including monitoring, management, data backup & restoration, security policy, business continuity & disaster recovery, operational procedures etc. Bidder shall obtain signoffs on the SOPs from the DGS and shall make necessary changes, on a half yearly basis, to the fullest satisfaction of DGS.

xiii. Proactive and Reactive maintenance are intended to troubleshoot the system with sufficient teams

xiv. Performance tuning of system as may be needed to comply with SLA on continuous basis

xv. Continuous monitoring & management of network during the working hours & restoration of breakdown within prescribed time limits.

xvi. Monitoring security and intrusions into the system, which include taking necessary preventive and corrective actions.

xvii. Monitor and record, server & network performance and take corrective actions to ensure performance optimization on a daily basis.

xviii. Escalation and co-ordination with other vendors for problem resolution wherever required.

xix. System administration tasks such as managing the access control system, creating and managing users, taking backups etc.

xx. Ensure that daily back-up copies of the data are created and maintained safely.

xxi. Produce and maintain system audit logs on the system for a period agreed to with the DGS. On expiry of the said period the audit logs should be archived and stored off-site.

xxii. Regularly review the audit logs for relevant security lapses.

xxiii. Review security advisories (such as bulletins generally available in the industry) on a regular basis to determine vulnerabilities relevant to the information assets and take necessary preventive steps.

xxiv. Supply consumables required for day-to-day operations of the Data Repository at DC. During the operations/management period, bidder shall not charge any additional cost to the DGS for replacement of these consumables.

xxv. Ensure that persons from DGS support team are duly trained and prepared in a progressive manner to operate the system on their own, with a view to eventually takeover operations at the end of contractual term

xxvi. Ensure that all necessary know-how is transferred to DGS support team in an effective manner to facilitate a smooth transition. Performance metrics for the transition will need to be agreed between the Bidder and DGS

xxvii. Produce and maintain system audit logs on the system for a period agreed to with the DGS. On expiry of the said period, the audit logs should be archived and stored off-site. Location for off-site storing of logs will be the responsibility of the bidder at no additional cost.

xxviii. Regularly review the audit logs for relevant security lapses and share the same with DGS.

xxix. Review security advisories (such as bulletins generally available in the industry) on a regular basis to determine vulnerabilities relevant to the information assets and take necessary preventive steps.

xxx. Supply consumables required for day-to-day operations of the Data Repository at DGS where this project has been deployed. These consumables include, but not limited to, storage medias, CD/DVDs, data cables etc. During the /operations/ management period, bidder shall not charge any additional cost to DGS for replacement of these consumables. **Supply of Printer cartridges and paper will be the responsibility of DGS.**

xxxi. SI to upgrade the system if any latest version of software is available either nationally or internationally within 45 days of launch in India or 12 months from launch internationally or as agreed with DGS. All updates and patches will be provided at no extra cost to DGS

xxxii. SI to Complete data sanitization and secure handover of credentials, logs, and documentation must be certified.

xxxiii. Bidder will ensure that the entire setup is certified and complies with the applicable standards. The Industry Standards which bidder is required to comply with are given below:

#	Component / Application / System	Prescribed Standard
1	Workflow Design	WFMC / BPM Standard
2	Portal Development	W3C Specification
3	Information Access/Transfer Protocols	SOAP, HTTP/HTTPS
4	Interoperability	Web Services, Open Standard

#	Component / Application / System	Prescribed Standard
5	Scanned Documents	TIFF / PDF (Resolution of 600 X 600 dpi)
6	Digital Signature	RSA standards
7	Document Encryption	PKCS specification
8	Information Security	ISO 27001 certified system
9	Operational Integrity & Security Management	ISO 27002 certified system
10	Operation	ISO 9001 certification
11	IT Infrastructure Management	ITIL/ EITM specification
12	Service Management	CMMI / ISO / IEC 20000
13	Project Documentation	IEEE/ISO specifications for documentation

Quality Audits:

a. The bidder is expected to align all phases of the project and sustenance as per best industry standards e.g. CMMI, ITIL, ISO 20000, ISO 27001, etc. It is expected that an independent Quality Team of bidder shall independently and regularly audit this system against these standards and processes laid down by bidder. The frequency of such audits must be at least once per half-year for every process. The result of the audit shall be directly shared with DGS with an effective action plan for mitigations of observations/non-compliances, if any.

b. DGS, at its discretion, may also engage independent auditors to audit any/some/all standards/processes. The bidder shall support all such audits as per calendar agreed in advance. The result of the audit shall be shared with the bidder who must provide an effective action plan for mitigations of observations/non- compliances, if any.

22. Resource Requirements

I. The BIDDER shall be responsible for sourcing of the personnel and the management of all matters relating to such personnel, to carry out the responsibilities assigned to the BIDDER under the agreement with the BIDDER. In particular, these include:

a. Recruitment of the personnel possessing the qualifications prescribed in the RFP.

b. Training of the personnel.

c. Payment of salaries and benefits to the personnel on time

d. Meeting all statutory obligations / payments arising out of engaging the personnel.

e. Meeting all the liabilities arising out of the acts of the personnel

II. Below table gives the indicative number of resources which need to be deployed across locations for this project.

#	Key Resources	No. of Resources	Essential Qualification
1	Project Manager	1	BE / BTech / MCA / MTech and MBA with at least 15 years of total work experience in project management and implementing large-scale digital platforms or mission-critical IT systems.
2	Solution Architect	1	BE / BTech / MCA / MTech / MBA with 10 years' work experience in designing and implementing large-scale digital platforms or mission-critical IT solutions.
3	Database Administrator (DBA)	1	BE / BTech / MCA / MTech / MBA with at least 6 years of Total work experience in database administration.
4	Cloud Infrastructure specialist	1	Engineer with experience in Cloud Computing technologies (IAAS/ PAAS / SAAS) with at least 8 years of total work experience.
5	Business Analyst	1	BE / BTech / MCA / MTech and MBA with at least 5 years of Total work experience
6	Domain Expert	1	BE / BTech / MCA / MTech and MBA with at least 8 years of total work experience.
7	Change Management Specialist / Trainer	1	Any graduation degree from recognized university / institute with at least 8 years of experience and at least 2 years of total work experience in all the following: • Conducting large scale awareness, training, promotional programs. • Expertise in development of course material for training on technical area

#	Non-Key Resources	No. of Resources	Essential Qualification
1	To be proposed by bidder		

III. During the course of the contract, if it becomes necessary to replace any of the Key Personnel, the BIDDER shall forthwith with due approval from DGS, provide as a replacement, a person of equivalent or better qualifications and experience than the resource being replaced / or proposed in the bid.

IV. The team proposed in the proposal should be on the rolls of the bidder(s) at the time of submission of the proposal. For any change of the resource or any resource being proposed for operations, the bidder should have to submit the CV of the resource, at least 2 weeks in advance for DGS to decide on the replacement.

Support Provided by Client

a. The client shall provide office space to the Bidder’s team. Laptops and peripherals are to be provided to its team by the Bidder.

b. The client shall provide access to relevant documentation, reports, budget documents, etc. to enable Bidder’s team to prepare a comprehensive vision document.

c. The client shall grant necessary access permissions to the Bidder’s team to visit DGS office and other parts of the premises for carrying out field visits.

d. The client shall make available its conference hall facility which is equipped with Cisco WebEx hardware to carry out offline and online consultations with stakeholders.

23. Project Plan and Payment Schedule

23.1. Timeline of Services

This section outlines the development schedules for the Indian global maritime safety platform (IGMSP) to be developed. These timelines presented in the below Gantt charts. The system integrator is expected to adhere to these timelines with precision to ensure the timely delivery of high-quality software solutions that align with the project’s objectives and milestones. This section serves as a crucial reference point for understanding the temporal aspects of the project and will aid in effectively managing and tracking progress throughout the engagement.

#	Particulars	Month 1	Month 2	Month 3	Month 4	Month 5	Month 6	Month 7	Month 8	Month 9	Month 10	Year 1	Year 2	Year 3
1.	Design & Development	**M1**	**M2**	**M3**	**M4**	**M5**	**M6**	**M7**						
2.	UAT								**M8**					
3.	Pilot Testing									**M9**				
4.	STQC & CERT-In Audit									**M9**	**M10**			
5.	Go-Live										**M10**			
6.	O & M											**Y 1**	**Y 2**	**Y 3**

23.2. Deliverables

i. The bidder has to deliver the following deliverables to DGS as part of an assurance to fulfil the obligations under the Payment schedule & meet the applicable SLA. The table given below may not be exhaustive and Bidder is responsible to provide all those deliverables which may be specified in this RFP but not listed here and those agreed by the Bidder in response to any request from DGS. The timelines for producing each of these deliverables will be in line and closely linked with the overall project timeline as indicated in the table above.

ii. Any conflict with respect to project and/or deliverable timelines will have to be resolved by bidder in consultation with DGS and approved by DGS. Thereafter the approved timelines will have to be adhered to by bidder, unless specified otherwise. It is to be noted that upon completion of Go-live, bidder is required to submit all the updated system design documents, specifications, source code, application deployment files, user manuals, administration manuals and all other applicable deliverables listed below.

iii. Following is a brief description of the deliverables & expected submission timelines

Deliverables	Deliverable Description	Expected Timelines (in Months)
D1	Kick-off presentation and/or duly signed agreement	T = 0
D2	Project charter should cover the following: • Setting up of PMIS • Study of scope of work & functional coverage • Detailed project plan • Governance Structure for Project Implementation • Project implementation approach • Detailed Project Plan with work breakdown structure • Delivery schedule • Key milestones • Resource deployment • Change & communication management plan • Change control procedure • Exit management plan • Draft SRS template • Backup Plan for resources	T+1
D3	Data migration report should cover the following: • Data migration assessment • Migration & transitioning approach • Detailed data migration plan • Scripts required for importing data that has been migrated Data back-up and archival process document	T+1 months
D4	Cloud Data centers establishment report should cover the following: • Specifications & Design of Cloud DC & DRC Installation & Commissioning of Cloud DC & DRC detailed plan	T+3 months
D5	Software Requirements Specifications (SRS) should cover the following not limited to: • Detailed requirement captures and analysis • Software requirement • Functional requirement • Flow chart, process workflows and interconnections of each module Interface specifications • Software Design document including Software	T+4 months

Deliverables	Deliverable Description	Expected Timelines (in Months)
	Architecture design, Logical and Physical Database Design, Programming Logic, Workflows & Finalization of KPIs / KRAs for Dashboard etc. • Application security requirements • Mapping of FRS & SRS Document. • Requirements sign-off from DGS • List of implemented open-source components, along with compliance sheet as per e-Gov standards • Identify third party interfaces required along with the type / specifications • Finalization of data analysis tools and techniques for output MIS / reports / parameters • Dashboard design with list of MIS / reports with source of data availability • Detail integration requirements with MIS / Reports / dashboards of inter & intra Ministries (API details, data fields to be shared, data fields required from other ministry systems, process flows, flow charts, design diagrams, etc.)	
D6	System Design & Configuration report should cover the following: • Business Blueprint Document • System Configuration and module wise configuration needs as per the design envisaged • Legacy and Third-party System Integration / interface Report and integration of same with the envisaged solutions • Customization Development Plan and Design / development plan of components of functionalities • Wireframe design of dashboard • IGSMP Dashboard and analytics with user manual and video help • List of MIS / Reports with recommended visualizations • List of external data point integrations with detailed integration process flows and documentation • Data Analysis tools, techniques, and usability documentation	T+7 months
D7	Data migration completion report should cover the following: • Details of actual data that has been migrated • Detailed methodology used for data migration with flow charts, size of data migrated, data validation reports.	T+ 7 months

Deliverables	Deliverable Description	Expected Timelines (in Months)
	Certificate from DGS officials confirming successful completion of data migration	
D8	Completion of DC and DR setup	T+ 7 months
D9	Software Deployment report should cover the following: • Complete Source Code with documentation • Test Plans and Test cases (including Unit Test Plan, System / Integration Test Plan, User Acceptance Test Plan, Security Test Plan, Load Test Plan) • Software Testing Documentation (including details of defects / bugs / errors and their resolution) • User Acceptance Test Cases, Test Data and Test Results, User Acceptance Test Scripts, Unit Test Cases, Integration Test Results / Cases • System Integration Test (SIT) Report including Performance Test (PT) Report • Security Test Report • Dashboard and analytical tool deployment with data validation report • Requirement Traceability Matrix (RTM)	T+8 months
D10	STQC report and Certificate (Relevant to Mgmt. System, Product Certification (IT & E-Gov)) including GIGW (Guidelines for Indian Government Website) Certificate. Security Audit Certificate from CERT-IN / CERT-IN empaneled agencies	T+10 months
D11	Go-live report should cover the following: • UAT sign-off • Complete updated Source Code and updated Deployment script with documentation • Deployment sign-off from DGS • User Manuals and System Manuals • Sign-off from DGS on Dashboard and Data Analytics requirements • DGS approved Security Testing, Load Testing, Unit Testing and System Acceptance report • DB entity relationship diagram • Pending Issues in the system, dependencies • Updated System Design documents, specifications for every change request • Updated user Manuals, administration manuals, training manuals Go-Live Certificate from DGS indicating readiness for roll-out with trainings	T+10 months
D12	Change Management & Training report should cover the following:	T+11 months

Deliverables	Deliverable Description	Expected Timelines (in Months)
	• Detailed training & Transition plan • Communication plan • Training Materials and Curriculums	
D13	Change Management & Training completion should cover the following: • Training session-wise completion reports • Certification from DGS officials confirming successful completion of Change Management & Trainings	T+12 months
D14	System stabilization report should cover the following: • Report indicating results, observations and action items • Latest source code, application deployment files, configuration files for entire solution • Detailed change description • Sign off from DGS for pending issues in the system	T+12 months
D15	Certification of successful completion of system stabilization from DGS Certification of SLA monitoring system Third party agency should certify SLA monitoring system	T+12 months
D16	3 years O & M SLA Compliance Reports (Monthly) should cover the following: • Performance Monitoring reports for system • SLA Compliance Reports Count of SMS sent • Training session-wise completion reports • Patches / Upgrades of all components • Incremental updates to solution • Change Requests Managed • Issue / Problem / Bugs / Defect Tracker • On-Going Project Updates • Audit / Standard Compliance Reports	(T+12) +36 months

23.3. Payment schedule

Payment would be done on the basis of components given in the following tables:

The bidder alone shall invoice all payments only after receiving due approval / acceptance of Deliverables / Services / Goods from DGS or any nominated agency.

SN	Milestone	Timelines (in Months)	Deliverables	Payment Milestone (% of contract value)
1	Kick-off presentation and/or duly signed agreement	T=0	D1	NA
2	• Submission and Acceptance of 'Project charter' – D2 • Submission and Acceptance of 'Data migration report' D3	T+1	D2, D3	5% of project cost
3	Specifications for required Cloud Data Centre and Disaster Recovery Centre – D4	T+3	D4	5% of the project cost
4	Business and system requirements study including interfaces – D5	T+4	D5	5% of the project cost
5	• Solution design including configuration requirements, interface design, etc. – D6 • Completion of data migration – D7 • Completion of DC and DR setup-D8	T+7	D6, D7, D8	10% of the project cost
6	Deployment of complete application software with all modules & required functionalities for user acceptance testing – D9	T+8	D9	5% of the project cost
7	Initiation of STQC Certification and completion of security audit – D10	T+9	D10	4% of the project cost
8	Full scale deployment of the system at location – D11	T+10	D11	4% of the project cost
9	Submission of change management plan covering training and transitioning requirements – D12	T+11	D12	4% of project
10	Completion of change management activities including training	T+12	D13	4% of Project cost
11	• Stable operations (SLA compliance) of the system for the 2 months post full-scale deployment – D14 • Certification of successful completion of system stabilization from DGS. Certification of SLA monitoring system – D15	T+12	D14, D15	4% of the project cost

SN	Milestone	Timelines (in Months)	Deliverables	Payment Milestone (% of contract value)
12	Payment every 3 months for next 3 years (O & M Phase)- D16	(T+12) + 36	D16	50% of the cost. (Equal payout in quarters each year at the end of the quarter)

All the deliverables should be as per the mentioned timeline for successful payment.

23.4. Terms of payment

i. In consideration of the obligations undertaken by the bidder under this Agreement and subject to the provisions of this Agreement, DGS shall pay the bidder for successful delivery of Services / Deliverables / Goods and System in pursuance of this Agreement, in accordance with the Terms of Payment Schedule set out in this clause.

ii. DGS shall not be required to make any payments in respect of the Services, Deliverables, obligations and scope of work mentioned in the RFP and Agreement other than those covered in the table as per Payment Schedule. For the avoidance of doubt, it is expressly clarified that the payments shall be deemed to include all ancillary and incidental costs and charges arising in the course of performance of obligations under the RFP and Agreement including consultancy charges, infrastructure costs, project costs, implementation and management charges and all other related costs including taxes which are addressed in this Clause.

23.5. Invoicing and settlement

i. The bidder shall submit its invoices in accordance with the following principles:

   a. Generally, and unless otherwise agreed in writing between the Parties, the bidder shall raise an invoice as per scheduled payment milestones; and

   b. Any invoice presented in accordance with this Clause shall be in a form agreed with DGS.

ii. The bidder alone shall invoice all payments only after receiving due approval / acceptance of Deliverables / Services / Goods from DGS or any nominated agency. Such invoices shall be correct and accurate and shall be raised in a timely manner.

iii. Subject to accomplishment to obligations of bidder and delivery of Deliverables / Services / Goods to the satisfaction of DGS, payment shall be made by DGS within 45 working days of the receipt of invoice along with supporting documents.

iv. Not with standing anything contained in clause (III) above, DGS shall be entitled to delay or withhold payment of any invoice or part of it where DGS disputes such invoice or part of it provided that such dispute is bona fide. The withheld amount shall be limited to that which is in dispute. A notice of such withholding shall be provided within 10 days of receipt of the applicable invoice.

v. The bidder shall be solely responsible to make payment to its personnel, sub-contractors, OEMs, third parties.

23.6. Taxes

i. DGS shall be responsible for withholding taxes from the amounts due and payable to the bidder wherever applicable under extant law. The bidder shall pay for all taxes in connection with this Agreement, SLAs, scope of work and any other engagement required to be undertaken as a part of this Agreement, including, but not limited to, property, sales, use, excise, value-added, goods and services, consumption and other similar taxes or duties

ii. DGS shall provide the bidder with the original tax receipt of any withholding taxes paid by DGS or its nominated agencies on payments under this Agreement within reasonable time after payment. The bidder agrees to reimburse and hold DGS or its nominated agencies harmless from and against any claims, losses, expenses (including attorney fees, court fees) etc. arising out of deficiency (including penalties and interest) in payment of taxes that is the responsibility of the bidder.

iii. If, after the date of this Agreement, there is any unforeseen change in the levies or rate of levy under the applicable laws of India with respect to indirect taxes and duties, which are directly payable by the bidder for providing the Deliverables/Services i.e. service tax or any such other applicable tax from time to time, which increase or decreases the cost incurred by the bidder in performing the Services, then the remuneration and reimbursable expense otherwise payable by the DGS under this Agreement shall be increased or decreased accordingly by correspondence between the Parties hereto, and corresponding adjustments shall be made. However, in case of any new or fresh tax or levy imposed after submission of the proposal the bidder shall be entitled to reimbursement on submission of proof of payment of such tax or levy.

23.7. Adherence to Deliverables

i. The bidder has to deliver the deliverables mentioned in Deliverables Schedule to DGS as part of an assurance to fulfil the obligations under the SLA. The table given in Project Timeline & Deliverables Schedule may not be exhaustive and bidder is responsible to provide all those deliverables which may be specified in this RFP but not listed here and those agreed by bidder in response to any request from DGS. The timelines for producing each of these deliverables will be in line and closely linked with the overall project timelines.

ii. Any conflict with respect to project and/or deliverable timelines will have to be resolved by bidder in consultation with DGS and / or its designated agencies and approved by DGS. Thereafter the approved timelines will have to be adhered to by bidder, unless specified otherwise. It is to be noted that upon completion of Go-live, bidder is required to submit all the updated system design documents, specifications, source code, application deployment files, user manuals, administration manuals and all other applicable deliverables listed in Deliverables Schedule.

24. Annexure II – Bidding Forms

24.1. Tech Form 1: Letter of Proposal

The Consultant must prepare the Letter of Proposal on its letterhead clearly showing the Consultant's complete name and address.

Note: All italicized text is for use in preparing these forms and shall be deleted from the final products.

Date:

Proposal Ref. No.:

To,
Directorate General of Shipping,
9th Floor Beta Building,
i-Think Techno Campus,
Kanjurmarg (East),
Mumbai - 400 042 (India)
Tel. No.: 91-22-25752040/41/42/43/45
Fax. No. :91-22-25752029/35.
Email: dgship-dgs[at]nic[dot]in

1. We have examined and have no reservations to the Request for Proposals, including Addenda issued in accordance with Instructions to Bidders;
2. We meet the eligibility requirements in accordance with ITB 4 and have no Conflict of Interest in accordance with GFR 175;
3. We offer to provide, in conformity with the Request for Proposals, the following Consultancy Services: Selection of System Integrator to develop the Indian Global Maritime Safety Platform (IGMSP) for Directorate General of Shipping, Govt. of India.
4. Our final price offer is as submitted in our financial Proposal.
5. Our Proposal shall remain valid for 180 days from the last date of submission of the Proposal and it shall remain binding upon us and may be accepted at any time before the expiration of that period;
6. We are not participating, as a Bidder or as a sub-Bidder, in more than one proposal in this bidding process;
7. We, along with any of our sub-Bidders, key experts or joint venture partners for any part of the contract, are not debarred by any Client under the State Government, the Central Government or any State Government or any Public Undertaking, Autonomous body, Authority by whatever name called under them;
8. We hereby certify that we have taken steps to ensure that no person acting for us or on our behalf will engage in any activities which is in contravention of the Code of Integrity proscribed in GFR 175;
9. We hereby certify that we neither are associated nor have been associated directly or indirectly with the Bidder or any other individual or entity that has prepared the design, specifications and other documents for the subject matter of procurement or is being proposed as Project Manager for the contract from the DGS;

10. We hereby certify that we have fulfilled our obligations to pay all such taxes as payable to the Central Government or the State Government or any local authority;
11. We hereby certify that we are not insolvent, in receivership, bankrupt or being wound up, not have its affairs administered by a court or a judicial officer, not have its business activities suspended and must not be the subject of legal proceedings for any of the foregoing reasons;
12. We hereby certify that our directors and officers have not been convicted of any criminal offence related to their professional conduct or the making of false statements or misrepresentations as to their qualifications to enter into a procurement contract within a period of three years preceding the commencement of the procurement process, or not have been otherwise disqualified pursuant to debarment proceedings;
13. We understand that this Proposal, together with your written acceptance thereof included in your notification of award, shall constitute a binding contract between us, until a formal contract is prepared and executed; and
14. We understand that DGS is not bound to accept the highest evaluated Proposal or any other Proposal that DGS may receive and that the decision of the DGS shall be final & binding.

Name of the Bidder:
Name of Bidder’s Authorized Signatory:
Designation of the person signing the Proposal:

Signature of the person named above
Date signed

24.2. Tech Form 2: Checklist of documents comprising Proposal

Document	Form	Included (Y/N)	Page No.
Covering Letter – Technical Bid	Please refer Tech 3		NA
Prequalification compliance sheet	Please refer Tech 19		
Particulars of the Bidder	Please refer Tech 2		
Financial Capabilities	Please refer Tech 5		
Profile of Resource	Please refer Tech 6		
Certificate from HR demonstrating its Organization Strength	Please refer Tech 7		
Technical Solution	Please refer Tech 6		
Unpriced Bill of Material	Please refer Tech 18		NA
Approach and Methodology	Please refer Tech 9		
Project Plan and development	Please refer Tech 10		
Deployment of Personnel	Please refer Tech 9		
Details of Experience of Bidder in Various Projects	Please refer Tech 12		
List of Sub-Contractors and OEMs and their details	Please refer Tech 13		
Black-listing Certificate	Please refer Tech 14		
Format of Consortium Agreement	Please refer Tech 15		
Bank Guarantee for Earnest Money Deposit	Please refer Tech 16		
Certificate of Conformity / No Deviation	Please refer Tech 17		
Declaration for No Conflict of Interest	Please refer Tech 18		
Bid Security Declaration	Form of Bid security declaration		
Compliance sheet for Functional Requirements	Please refer Annexure Consolidated		
Compliance sheet for Technical Requirements	Please refer annexure Consolidated		

24.3. Tech Form 3: Technical Bid - Covering Letter

<<On Bidder / Lead Bidder Letterhead>>
Date:

To:
Directorate General of Shipping
9th Floor, Beta Building,
i-Think Techno campus
Kanjurmarg (East), Mumbai – 400042

Subject: Selection of System Integrator for development of Platform for the Indian Global Maritime Safety Platform (IGMSP) for Directorate General of Shipping.

Dear Sir,
We hereby request to be qualified with the Directorate General of Shipping as a Tenderer **for "Selection of System Integrator for development of Platform for the Indian Global Maritime Safety Platform (IGMSP) for Directorate General of Shipping.** I / We declare that all the services shall be performed strictly in accordance with the RFP documents, and we agree to all the terms and conditions in the RFP. I / We confirm that I / we am / are withdrawing all the deviations, counter clauses, proposed modifications in the Scope of work, Terms and Conditions, Functional Requirement Specifications and Technical Specifications which may have been mentioned in our proposal.

We authorize Directorate General of Shipping or its authorized representatives to conduct any investigations to verify the statements, documents and information submitted and to clarify the financial and technical aspects of this application. For this purpose, we hereby authorize (any public official, engineer, bank, depository, manufacturer, distributor, etc.) or any other person or firm to furnish pertinent information deemed necessary and requested by Directorate General of Shipping to verify statements and information provided in this application or regarding our competence and standing.
The names and positions of persons who may be contacted for further information, if required, are as follows:
Name: ______________________________
Designation: ______________________________
Telephone: ______________________________
E-mail id: ______________________________

We declare that the statements made, and the information provided in the duly completed application are complete, true and correct in every detail. On verification at any time in the future if it is found that information furnished with this application and statements made therein are not true, incomplete or incorrect, we hereby authorize Directorate General of Shipping to reject our application.

We confirm having submitted the information as required by you in Qualification Criteria. In case you require any other further information / documentary proof in this regard before evaluation of our bid, we agree to furnish the same in time to your satisfaction.

We undertake, if our proposal is accepted, to provide all the services related to **Selection of System Integrator for development of Platform for the Indian Global Maritime Safety Platform (IGMSP) for Directorate General of Shipping,** Put forward in the bid document or such features as may subsequently be mutually agreed between us and DGS or its appointed representatives.

I. We agree for unconditional acceptance of all the terms and conditions set out in the bid document and also agree to abide by this bid response for a period of 180 days from the date fixed for bid opening and it shall remain binding upon us with full force and virtue. Till a formal contract is prepared and executed, this bid response, together with your written acceptance thereof in your notification of award, shall constitute a binding contract between us and Directorate General of

Shipping(DGS),the Ministry of Ports,Shipping and Waterways(MOPSW),Govt. of India..

II. We hereby declare that in case the contract is awarded to us, we will submit Performance Bank Guarantee equivalent to 3 % of total contract value as quoted in the commercial bid in the form prescribed in the RFP.

III. I/We understand that Directorate General of Shipping (DGS)reserves the right to reject any application without assigning any reason thereof.

IV. I/We hereby undertake that I/We have not made any payment or illegal gratification to any person/authority connected with the bid process so as to influence the bid process and have not committed any offence under the PC Act in connection with the bid.

V. All the prices mentioned in our Tender are in accordance with the terms as specified in the RFP documents.

VI. We hereby confirm that our prices include all taxes. However, all the taxes are quoted separately under relevant sections.

VII. We understand that the actual payment would be made as per the existing tax rates during the time of payment.

VIII. We have indicated in the relevant forms enclosed, the unit rates for the purpose of on account of payment as well as for price adjustment in case of any increase to / decrease from the scope of work under the contract.

IX. We further confirm that the prices stated in our bid are in accordance with your Instruction to Bidders included in Tender documents.

X. In case you require any other further information/documentary proof before/during evaluation of our Tender, we agree to furnish the same in time to your satisfaction.

XI. We declare that our Bid Price is for the entire scope of the work as specified in the tender document. These prices are indicated in Commercial Bid submitted as part of the requirements of Tender.

XII. Our commercial proposal shall be binding upon us subject to the modifications resulting from Contract negotiations, up to expiration of the validity period of the Proposal.

XIII. We understand you are not bound to accept any Proposal you receive.

XIV. We hereby declare that our Tender is made in good faith, without collusion or fraud and the information contained in the Tender is true and correct to the best of our knowledge and belief.

XV. I/We shall disclose any payments made or proposed to be made to any intermediaries (agents, etc.) in connection with the bid.

XVI. It is hereby confirmed that I/We are entitled to act on behalf of our corporation/ company/firm/organization and empowered to sign this document as well as such other documents, which may be required in this connection.

XVII. We declare that we have read through the Tender document, all related clarifications and corrigendum.

Thanking you,
Yours faithfully

(Signature of the Authorized signatory of the Bidding Organization)
Name :
Designation :
Date :
Company Seal :
Business Address :

24.4. Tech Form 4: Particulars of the Bidder (please fill separate sheet for each consortium members)

SI No.	Information Sought	Details to be Furnished
A	Name and address of the bidding Company	
B	In case of consortium, please indicate name of Lead Bidder	
C	Incorporation status of the firm (public limited / private limited, etc.)	
D	Year of Establishment	
E	Date of registration	
F	ROC Reference No.	
G	Details of registration with appropriate authorities for service tax	
H	Name, Address, email, Phone nos. and Mobile Number of Contact Person	

(Signature of the Authorized signatory of the Bidding Organization)
Name :
Designation :
Date :
Company Seal :
Business Address :

24.5. Tech Form 5: Financial Capability

<<To be completed by the Bidder / In case of consortium, by each partner as appropriate to demonstrate that they meet the requirements>>
<<On the letterhead of the Chartered Accountant >>
<<To be submitted along with Audited Financial Statements>>

Date
To:
Directorate General of Shipping

9th Floor, Beta Building,

i-Think Techno campus

Kanjurmarg (East), Mumbai - 400042

We have examined the books of accounts and other relevant records of <<Bidder / consortium Partner Name along with registered address>>. On the basis of such examination and according to the information and explanation given to us, and to the best of our knowledge & belief, we hereby certify that the annual turnover, Profit before Tax and Profit after tax for the three years i.e., from 2021-22, 2022-23 and 2023-24 was as per details given below:

Information from Balance Sheets (in Indian Rupees)			
	2021-22	2022-23	2023-24
Annual Turnover			
Profit before Tax			
Profit After Tax			

(Signature of the Chartered Accountant)
Name :
Designation :
Membership Number :
Date :
Company Seal :
Business Address :

24.6. Tech Form 6: Profile of Resource

<table>
<tr><td></td><td>Name of the employee</td><td></td></tr>
<tr><td></td><td>Name of the employer</td><td>&lt;&lt;Name of the Bidder / Consortium Member &gt;&gt;</td></tr>
<tr><td></td><td>Proposed position</td><td></td></tr>
<tr><td></td><td>Date of Birth</td><td></td></tr>
<tr><td></td><td>Nationality</td><td></td></tr>
<tr><td></td><td>Total years of relevant experience</td><td></td></tr>
<tr><td></td><td>Certifications</td><td>Note: Please attach copies of relevant certificates</td></tr>
<tr><td></td><td>Education</td><td>
<table>
<tr><th>Qualification</th><th>Name of School / College / University</th><th>Degree Obtained</th><th>Date Attended</th></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="4">Note: Please attach copies of relevant certificates</td></tr>
</table>
</td></tr>
<tr><td></td><td>Language</td><td>
<table>
<tr><th>Language</th><th>Read</th><th>Write</th><th>Speak</th></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td></td><td>Employment Record</td><td>
<table>
<tr><th>Employer</th><th>Position</th><th>From (MM / YYYY)</th><th>To (MM / YYYY)</th><th>Exp. in Months</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table>
<i>(Starting with present position list in reverse order)</i>
</td></tr>
<tr><td></td><td>Relevant Experience</td><td>
<i>(Give an outline on the experience most pertinent to tasks mentioned in the project. Describe degree of responsibility held on these relevant assignments). (Details shall be provided as per the number of project experience in the evaluation criteria specified in section 6.5 of the RFP. Bidders are expected to clearly state the total number of projects for the respective criterion as applicable.)</i>
<i>Maximum 8 Projects:</i>
<table>
<tr><th><b>Name of Assignment/Project</b></th><th></th></tr>
<tr><td>Year</td><td></td></tr>
<tr><td>Location</td><td></td></tr>
<tr><td>Client</td><td></td></tr>
<tr><td>Main project features</td><td></td></tr>
<tr><td>Positions held</td><td></td></tr>
<tr><td>Activities performed</td><td></td></tr>
</table>
</td></tr>
<tr><td></td><td>Certification</td><td>I, the undersigned, certify that to the best of my knowledge and belief, this bio-data correctly describes myself, my qualifications, and my experience.

Date:
Place Signature of the employee / Authorized Signatory</td></tr>
</table>

24.7. Tech Form 7: Certificate from HR demonstrating its Organization Strength

<<On the letterhead of the Bidding Organization>>
<<In case of consortium, separate certificates to be submitted from respective HR authorized representatives>>

Date:
To:
Directorate General of Shipping

9th Floor, Beta Building,

i-Think Techno campus

Kanjurmarg (East), Mumbai - 400042

This is to certify that the number of full-time employees having experience in implementing all the major modules/solution components of the proposed solution in <<Organization Name>> is greater than <<Number>> as on DD/MM/YYYY

For <Organization Name>

HR Signature (with Organization Stamp)
HR Name

24.8. Tech Form 8: Technical Solution

The Bidder is required to describe the proposed Technical Solution in this section. The Technical Solution would be evaluated on the following broad parameters. The DGSreserves the rights to add, delete, or modify these parameters at any time during the Tender process, without assigning any reasons whatsoever and without being required to intimate the Bidders of any such change.

Clear articulation and description of the design and technical solution and various components
Extent of compliance to functional and technical requirements specified in the scope of work and in accordance with leading practices.
Technical Design and clear articulation of benefits to DGS of various components of the solution vis-à-vis other options available.

The Bidder should provide **detailed design** for the following listing all assumptions that have been considered:

i. Proposed Solution, in detail (including various tools to be used)
ii. Proposed Technical architecture
iii. Capabilities of the proposed solution to address the functional requirements
iv. Database design considerations
v. Application Security Architecture
vi. Cloud DC DR Considerations
vii. Data Migration approach
viii. Testing approach
ix. Risk Management Plan

24.9. Tech Form 9: Approach & Methodology

i. The Bidder should cover details of the methodology proposed to be adopted for planning and implementation of solutions relating to establishment of the DGS solution.

ii. The Bidder may give suggestions on improvement of the scope of work given and may mention the details of any add on services related to this project over and above what is laid down in the tender document. List of deliverables should also be identified and explained.

iii. The Bidder shall describe the knowledgebase, best practices and tools that will be used by the project team for the execution of scope of work activities.

iv. The Bidder should cover details of the methodology proposed to be adopted for operations and maintenance of the DGS solution.

v. The bidder shall cover the details for best practices from imparting similar kind of training for users in an organization similar to the DGS based on bidder's prior implementation experience in the same

vi. Detailed Methodology and approach provided for training of the different stakeholders within DGS

vii. Best practices from undertaking Change Management for users in an organization similar to DGS based on bidder's prior implementation experience in the same.

viii. Detailed Training Plan indicating the number of training sessions, batch sizes and number of batches with respect to all the stakeholders, and all different kinds of training vis-à-vis the requirements in the tender.

ix. Project Methodology should contain, but not limited to the following

- Overall implementation methodology (Objective of phases, deliverables at each phase, etc.)
- Methodology for performing business design
- Methodology for quality control and testing of configured system
- Methodology of internal acceptance and review mechanism for deliverables by the bidder.
- Proposed Acceptance criteria for deliverables
- Methodology and approach along with proposed tools and processes which will be followed by the bidder during project implementation
- Change Management and Training Plan
- Risk and Quality management plan

24.10. Tech Form 10: Project Plan & Deployment of Personnel

S. No	Item of Activity	Month-Wise Program					
		M1	M2	M3	M4	M5	…..
1	Activity 1	■	■				
1.1	Sub-Activity 1	░					
1.2	Sub-Activity 2		░				
2	Activity 2						
	..						
3	Activity 3					■	
3.1	Sub-Activity 1					░	
3.2	Sub- Activity 2					░	

Indicate all main activities of the assignment, including delivery of reports (e.g.: inception, interim, and final reports), and other benchmarks such as Bidder approvals. For phased assignments indicate activities, delivery of reports, and benchmarks separately for each phase.

Duration of activities shall be indicated in the form of a bar chart.

Note: The above activity chart is just for the purpose of illustration. Bidders are requested to provide detailed activity & phase wise timelines for executing the project with details of deliverables & milestones as per their proposal.

24.11. Tech Form 11: Format of Deployment of Personnel

The Bidder should provide a detailed resource deployment plan in place to ensure that technically qualified staff is available to deliver the project.

The Bidder should provide the summary table of details of the manpower that will be deployed on this project along with detailed CVs of each key personnel

No.	Name of Staff	Education Qualification and Designation	Area of Expertise	Deployment Period (In Months)						Total Man-Months Proposed	Full Time/ Part Time
				M1	M2	M3	M4	M5	n		
1											
2											
3											

24.12. Tech Form 12: Details of Experience of Bidder in Various projects

The bidder should provide information for each project on similar assignments required for pre-qualification and technical evaluation criteria as per the format mentioned below

Sr. No.	Credential for < Prequalification Criteria No. / Technical Criteria No>		
	Name of the Organization - <<Name of the Bidder / Consortium Member that have executed / executing the project>>		
	Parameter	Details	
General Information			
	Customer Name		
	Name of the contact person and contact details for the client of the assignment		
	Whether client visit can be organized	(YES / NO)	
Project Details			
	Project Title		
	Start Date and End Date		
	Date of Go-Live		
	Total Cost of the project		
	Current Status (Live / completed / on-going / terminated / suspended)		
	No of staff provided by your company		
	Please indicate the current or the latest AMC period with the client *(From Month –Year to Month-Year)*		
	Please indicate whether the client is currently using the implemented solution		
Size of the project			
	Number of total users and concurrent users of the solution at the client location(s):	Total users	
		Concurrent users	
	Training responsibilities of Bidder		
	Any other information to be shared with DGS		
Narrative Description of the Project:			
Detailed Description of actual services provided by Bidder:			
Documentary Proof:			

24.13. Tech Form 13: List of Sub-Contractors and OEMs and their details

List of Sub-Contractors

Sr. No.	Role	Name of Sub-Contractor / OEM	Responsibility	Products/Services Offered

List of OEMs

Sr. No.	Role	Name of OEM	Responsibility	Products/Services Offered

(Signature of the Authorized signatory of the Bidding Organization)
Name :
Designation :
Date :
Company Seal :
Business Address :

24.14. Tech Form 14: Details of ineligibility for corrupt or fraudulent practices / blacklisted with any of the Government or Public Sector Units

<<On the letterhead of the Bidding Organization>>
<<In case of consortium, separate certificates to be submitted from respective authorized representatives>>

Date:
To:
Directorate General of Shipping
9th Floor, Beta Building,
i-Think Techno campus
Kanjurmarg (East), Mumbai - 400042

Subject: Declaration for not being under an ineligibility for corrupt or fraudulent practices or blacklisted with any of the Government or Public Sector Units in India

Dear Sir,

We, the undersigned, hereby declare that
We are not under a declaration of ineligibility / banned / blacklisted by any State or Central Government / any other Government institutions in India for any reason as on last date of submission of the Bid or convicted of economic offence in India for any reason as on last date of submission of the Bid

Thanking you,
Yours faithfully

(Signature of the Authorized signatory of the Bidding Organization)
Name :
Designation :
Date :
Company Seal :
Business Address :

24.15. Tech Form 15: Format for Consortium Agreement

<<On the letterhead of the Bidding Organization>>

<<In case of consortium, separate certificates to be submitted from respective authorized representatives>>

[Date]

To
Directorate General of Shipping
9th Floor, Beta Building,
i-Think Techno campus
Kanjurmarg (East), Mumbai - 400042

Sir,
Sub: Declaration on Consortium
I / We as Lead Partner of the Consortium, hereby declare the Roles and Responsibilities of the Consortium members:

Sr. No.	Member	Role	Responsibilities

I / We understand that as Lead Partner, I / we are be responsible for executing at least one component of the scope of work from the following components:

1. Application Development and Maintenance
2. Transitioning and Change Management

I / We understand that if this information / declaration is found to be false or incorrect, Directorate General of Shipping reserves the right to reject the Bid or terminate the Contract with us immediately without any compensation to us.

Yours faithfully,
Authorized Signatory of the Lead Partner
Designation
Date
Time
Seal
Business Address

Pre-qualification Bid Forms

24.16. Tech Form 16: Bank Guarantee for Earnest Money Deposit

WHEREAS _______________________________________ (Name of Tenderer) (hereinafter called 'the tenderer') has submitted its tender dated ________ (date) for the execution of ____ (Name of work) (hereinafter called 'the tender')

KNOW ALL MEN by these presents that we __________________________ (Name of Bank) having our registered office at ________________________________ (hereinafter called 'the Bank') are bound unto the Directorate General of Shipping, Mumbai appointed by Government of India under Merchant Shipping Act 1958 (hereinafter called 'the Employer') in the sum of Rs. _________/- (Rs. __________________) for which payment well and truly to be made to the said Employer the Bank binds itself, its successors and assigns by these presents.
The CONDITIONS of this obligation are
If the Tenderer withdraws its Tender during the period of Tender validity specified in the Tender; or
If the Tenderer having been notified of the acceptance of his Tender by the Employer during the period of Tender Validity;
fails or refuses to execute the Agreement, if required; or
fails or refuses to furnish the Performance Security, in accordance with the General Conditions of Contract.
We undertake to pay the Employer up to the above amount upon receipt of his first written demand, without the Employer having to substantiate his demand, provided that in his demand the Employer will note that the amount claimed by him is due to him owing to the occurrence of one or both of two conditions, specifying the occurred condition or conditions.
This guarantee will remain in force up to and including the date upto ________ (it shall be valid upto one eighty (180) days after the date of expiry of the period of tender validity), and any demand in respect thereof should reach our ________ branch situated in Mumbai limits for encashment not later than the date of expiry of this guarantee.

Dated _____________ day of ___________ 2020
Name of the Bank
Signature & Name & Designation
Seal of the Bank

24.17. Tech Form 17: CERTIFICATE OF CONFORMITY/ NO DEVIATION

<<To be submitted on the Company Letter head of the Lead Bidder>>

Date:
To:
Directorate General of Shipping
9th Floor, Beta Building,
i-Think Techno campus
Kanjurmarg (East), Mumbai – 400042

This is to certify that, the specifications of Software/ hardware which I/ We have mentioned in the technical bid, and which I/ We shall supply if I/ We am/ are awarded with the work, are in conformity with the minimum specifications of the bidding document and that there are no deviations of any kind from the requirement specifications.

Also, I/ we have thoroughly read the RFP and by signing this certificate, we hereby submit our token of unconditional acceptance to all the terms & conditions of the bidding document without any deviations.

I/ We also certify that the price I/ we have quoted is inclusive of all the cost factors involved in the end-to-end implementation and execution of the project, to meet the desired Standards set out in the bidding Document.

Thanking you,
Yours faithfully

(Signature of the Authorized signatory of the Bidding Organization)
Name :
Designation :
Date :
Company Seal :
Business Address :

24.18. Tech Form 18: Format – Declaration for No Conflict of Interest

<<To be submitted on the Company Letter head of the Lead Bidder>>

Date:

To
Directorate General of Shipping,
9th Floor, Beta Building,
i-Think Techno campus
Kanjurmarg (East), Mumbai – 400042

Sir,

Sub: Undertaking on No Conflict of Interest

I / We as System Integrator (SI) do hereby undertake that there is absence of, actual or potential conflict of interest on our part, on part of our Consortium partner (in case of a Consortium) due to prior, current, or proposed contracts engagements, or affiliations with Directorate General of Shipping, Government of India.

I / We also confirm that there are no potential elements (time frame for service delivery, resource, financial or other) that would adversely impact our ability to complete the requirements of this RFP.

We undertake and agree to indemnify and hold Directorate General of Shipping, Government of India harmless against all claims, losses, damages, costs, expenses, proceeding fees of legal advisors (on a reimbursement basis) and fees of other professionals incurred (in the case of legal fees & fees of professionals, reasonably) Directorate General of Shipping, Government of India and / or its representatives, if any such conflict arises later.

Yours faithfully,

Authorized Signatory
Designation
Date
Time
Seal
Business Address

24.19. Tech Form 19: Compliance Sheet for Pre-Qualification Proposal

The Bidder is required to fill relevant information in the format given below. The pre-qualification bid must contain documentary evidences and supporting information to enable DGS to evaluate the eligibility of the Bidder without ambiguity.

Sr. No	Qualification Criteria	Documents / Information to be provided in the submitted proposal	Compliance (Yes / No)	Reference & Page Number
1.	**PQ 1**			
2.	**PQ 2**			
3.	**PQ3**			
4.	**PQ4**			
5.	**PQ5**			
6.	**PQ6**			
7.	**PQ7**			
8.	**PQ8**			

24.20. Tech Form 20: Bid Security Declaration

{*Use Company Letterhead*}

I/We, M/s (Name of bidder) am/are aware that I/We have been exempted from submission of Bid Security/Earnest Money Deposit in lieu of this Bid Security Declaration. I/We understand and accept that if I/We withdraw my/our bid within bid validity period or if awarded the tender and on being called upon to submit the performance Guarantee/Performance Security fail to submit the same within the stipulated time period mentioned in tender documents or on being called upon to sign the contract agreement fail to sign the same within stipulated period mentioned in tender documents, I/We i.e., the bidder shall be banned from submission of bids in any Works/Service Tender issued by DGSfor a period of 24 months from the date of such banning order.

Authorized Signatory
Sign and
Stamp

25. Annexure – III Functional Requirements Specification

25.1. Casualty Reporting and Management

25.1.1. Reporting & Intake

- The System should provide a structured web form and guided wizard to capture casualty details, including structured fields, free text inputs, attachments, vessel information, voyage data, crew lists, and geolocation.
- The System should allow submission of casualty reports via authenticated accounts, guest submission, and secure API ingestion from authorized external systems such as other DGS modules, AIS feeds, and DG Communication Center.
- The System should enable configurable field validations, including mandatory fields as defined by the administrator.

25.1.2. Anonymous Reporting

- The System should allow submission of reports without capturing Personally Identifiable Information (PII) by offering an explicit “Anonymous Reporting” option in the UI.
- The System should ensure no PII or identifiable metadata (e.g., IP address, browser fingerprint) is stored unless anonymized or hashed, with temporary retention only for abuse prevention.
- The System should store anonymous reports separately with restricted access for authorized reviewers only.
- The System should generate a unique tracking reference for each submission, whether anonymous or identified.
- The system shall provide an option for users to submit incident reports anonymously, without requiring login or personal identification.
- The system shall ensure that no personally identifiable information (PII) is collected, stored, or logged for anonymous submissions.
- The incident reporting interface shall clearly indicate the option to report anonymously and explain its implications (e.g., limited follow-up).
- Anonymous reports shall be flagged and stored distinctly from identified reports for audit and workflow purposes.
- The system shall ensure that metadata (e.g., IP address, browser fingerprint) is not stored or is anonymized for such submissions.

- Access to anonymous reports shall be restricted to authorized personnel with appropriate privileges.
- Anonymous incident reports shall be processed, analyzed, and visualized alongside identified reports within dashboards and analytics modules.
- The system shall support configurable workflows for handling anonymous reports, including review, categorization, and escalation.
- The system shall allow administrators to configure which incident types can be reported anonymously.
- The system shall maintain audit logs for anonymous submissions, recording submission time and processing steps, without capturing user identity.
- The system shall comply with relevant data privacy and protection regulations regarding the handling of anonymous data.
- The reporting interface shall provide clear instructions and disclaimers about the anonymous reporting process, including the inability to follow up with the reporter.
- The system shall display confirmation messages upon successful anonymous submission, with a unique reference number for tracking
- The system shall include filters and indicators in dashboards and reports to distinguish between anonymous and identified incident submissions.
- The system shall allow analysis of trends and patterns in anonymous reporting to support safety culture and risk management initiatives.

25.1.3. Assignment & Workflow Engine

- The System should automatically assign Investigation Officers (IOs) based on jurisdiction, vessel flag, port of occurrence, or other configurable rule-based criteria.
- The System should allow authorized users to manually override automated assignments.
- The System should support configurable workflow states for case handling, such as: Reported → Assigned → Evidence Collection → Hearing/Inspection → Report Drafting → Interim → Final → Recommendations → Closed.
- The System should allow SLA timers and escalation paths to be set for each workflow stage, based on case type.

25.1.4. Evidence Management

- The System should enable secure uploading, tagging, categorization, and version control of documents, photos, videos, audio, and VDR extracts related to a case.
- The System should maintain chain-of-custody metadata and an audit trail for each evidence artifact.
- The System should support secure tokenized access and streaming for multimedia files.
- The System should allow forensic handling, including the ability to quarantine extracted files or media.

25.1.5. Notices, Summons & Legal Actions

- The System should auto-generate official documents such as notices, summons, and letters using configurable templates.
- The System should support electronic signatures and export to PDF or print formats.
- The System should track service attempts, legal case numbers, and court dates associated with the casualty.
- The System should integrate with relevant case management systems for matters referred to police or courts.

25.1.6. Reporting & Timelines

- The System should support pre-defined report templates aligned to DGS formats for Initial, Interim, Final Investigation, and Recommendations reports.
- The system shall allow configurable timelines for each stage of casualty reporting, including:

    - Initial Report: within 3 days
    - Interim Report: within 30 days
    - Final PI/Investigation Report: within 90 days
    - Recommendations Report: within 90 days

- The System should allow authorized users to modify and manage these templates.
- The System should automatically trigger reminders and escalate delays in report submission, while capturing reasons for missed deadlines.

25.1.7. Integration & Correlation (AI assisted)

- The System should integrate with relevant internal and external maritime data sources, not limited to :
  - AIS / LRIT / Vessel movement feeds
  - Weather feeds
  - Port systems, PSC inspection data, international casualty DBs (EMCIP, MAIB when permitted)
  - SMS / Email gateways and Crisis Management module
- The System should support automated correlation of incoming reports with existing vessel and incident data for case linkage.

25.1.8. Archival & Retention

- The System should support configurable retention policies for casualty case data in line with DG Shipping regulations.
- The System should maintain active case data for a minimum of 3 years online and archived data for a minimum of 7 years.
- The System should allow secure deletion or anonymization of records upon expiry of retention period.

25.2. Casualty Data Representation, Integration and Analysis Framework

25.2.1. Incident Reporting Integration and Data Exchange:

- The System should allow users to create personalized dashboards with various widget types for incident reporting and analysis.
- The system shall link compliance monitoring data with other IGMSP modules such as Incident Reporting (25.1.1) and Predictive Risk Scoring (25.5.1).
- The system shall use this integration to generate risk-adjusted compliance views, highlighting which non-compliances are most likely to lead to future incidents.
- The System should offer visualization widgets, such as charts, graphs, maps, and tables, that users can configure with casualty data.
- The System should enable customization of dashboard elements, including colours, fonts, and themes, to align with IMO guidelines and organizational branding.

- The system shall allow AI-driven correlation of incident reports with external datasets such as weather conditions and vessel movement data to derive root cause insights and predictive patterns.
- The System should provide the ability to set up role-specific dashboards displaying relevant information tailored to each user's responsibilities.
- The System should support real-time data feeds integration into dashboards for up-to-the-minute casualty data visualization.
- The System should allow users to interact with dashboard elements for in-depth analysis, including filtering data and drilling down for more detailed information.
- The System should permit users to save and manage multiple dashboard configurations for quick access to different data views.
- The System should facilitate the sharing of dashboards among users or groups with appropriate access controls.
- The System should ensure dashboards are responsive and render effectively across various devices.
- The System should provide options for exporting dashboard data into different formats for reporting or presentation purposes.
- The System should include the ability to schedule automated refreshes of dashboard data at user-defined intervals.
- The System should incorporate dashboard usage analytics to track user engagement and identify frequently accessed dashboards or widgets.
- The System should maintain dashboard performance, even when handling large volumes of data or complex visualizations.
- The System should offer a library of pre-designed dashboard templates for common maritime safety monitoring scenarios.
- The system should be integrated with AI to identify patterns and anomalies in casualty reports, flagging inconsistencies or potential risks in real-time.
- The System should use AI to recommend optimal chart types, graphs, and widgets based on data trends, improving user experience.
- The system should use AI to track user behaviour and suggest dashboard modifications or widgets that align with individual user preferences and responsibilities.
- The System should use AI to correlate different data sources (e.g., weather, vessel movement, historical incidents) for comprehensive casualty analysis.

25.3. Integrated Dashboard

25.3.1. Dashboard Design and Features:

- The system shall display risk scores and indicators on intuitive dashboards including vessel-specific and port-specific risk levels, geographic heatmaps, and predictive incident forecasts.
- The system shall include decision support tools that suggest preventive actions, issuance of safety circulars, or targeted training based on emerging risk patterns.
- The System should allow users to create personalized dashboards by selecting, positioning, and resizing various widget types.
- The system shall provide responsive, web-based and mobile-compatible dashboards to visualize real-time alerts, safety indicators, and operational statuses.
- The system shall support drill-down features and visual cues (e.g., blinking markers, color-coded warnings) for faster interpretation of live alerts.
- The System should offer a wide range of visualization widgets, such as charts, graphs, maps, and tables, that users can configure with different data sets.
- The System should enable users to customize the appearance of dashboard elements, including colours, fonts, and themes, to align with user preferences or organizational branding.
- The System should provide the ability to set up different dashboards for various user roles, displaying relevant information tailored to the responsibilities of each role.
- The System should support the integration of real-time data feeds into dashboards, allowing for up-to-the-minute data visualization.
- The System should allow users to interact with dashboard elements, such as filtering data, drilling down for more detailed information, or linking to external reports.
- The System should permit users to save and manage multiple dashboard configurations, enabling quick switching between different views.
- The System should facilitate the sharing of dashboards among users or groups, with appropriate access controls to manage viewing and editing permissions.
- The System should ensure that dashboards are responsive and render effectively across various devices, including desktops, tablets, and smartphones.

- The System should provide options for exporting dashboard data or visualizations into different formats for reporting or presentation purposes.
- The System should include the ability to schedule automated refreshes of dashboard data at user-defined intervals.
- The System should incorporate a dashboard usage analytics feature to track user engagement and identify the most frequently accessed dashboards or widgets.
- The System should maintain performance and loading speed of dashboards, even when handling large volumes of data or complex visualizations.
- The System should offer a library of pre-designed dashboard templates that serve as starting points for common scenarios.
- The System should be developed using well-established technologies, preferably open source, without financial implications.
- The System should comply with W3C Guidelines and GIGW and undergo security audits by selected agencies.
- The System should provide multiple design options/templates for the dashboard, ensuring a user-friendly information architecture and speed optimization.
- The System should allow customization of the UI in terms of colour, font size, and language.
- The System should integrate social media and accessibility features as per GIGW Guidelines.
- The system should use AI to enhance data organization by automatically tagging and classifying datasets for more effective searchability and filtering.
- The system should use AI to monitor dashboard usage patterns to recommend layout optimizations, ensuring efficiency and improved user engagement.
- The system should have AI-powered virtual assistants to guide users through dashboard functionalities, helping them set up widgets or troubleshoot issues.

25.3.2. Dashboard Maintenance:

- The System should create new web pages within the existing Dashboard as required.
- The System should allow for Dashboard design changes as needed.
- The System should upgrade Dashboard technical functionality as required.
- The System should monitor and maintain Dashboard speed, sign-up process, navigation links, etc.

- The System should design and upload banners, jQuery, graph artwork, infographics, and audio–video files on the Dashboard.
- The System should convert documents to required formats such as HTML/HTML5.
- The System should keep the Dashboard secured from all possible cyber-attacks and hackers at all times.
- The System should conduct security audits as required.
- The System should provide content upload and Dashboard support on a 24x7 basis.
- The System should keep an activity log for all web updates.
- The System should create and maintain the archive section on the Dashboard.
- The System should troubleshoot issues as they arise.
- The system should use AI to proactively detect and suggest resolutions for common dashboard errors, reducing downtime and manual intervention.

25.4. Safety Circulars & Documentation Repository:

25.4.1. Document Management System:

- The System shall have a document management module for storing, archiving, and retrieving documents efficiently.
- The system shall store documents like lessons to be learned for presentation to seafarers, the analysis of casualty reports, potential safety issues, and draft safety recommendations.
- The System must be scalable to accommodate growing data and user needs and adhere to e-Government standards as formulated by MeitY, GoI.
- The System shall offer out-of-the-box integration with leading application servers.
- The System shall provide a web interface with drag-and-drop functionality, supporting popular browsers like Microsoft Explorer, Firefox, Netscape, and Google Chrome.
- The System shall allow for document/image capturing and provide the ability to send these to a centralized repository.
- The System shall offer a standard file hierarchy structure with folders and sub-folders for document organization and state any limitations on the number of folders or subfolder levels.
- The System shall enable document creation, editing, and management, with automatic version updating when the original document is updated.

- The web interface shall provide multiple views of content and allow user access based on rights and permissions, with the ability to restrict access based on pre-defined user rights and privileges.
- The System must provide a web-based administration tool for managing repositories, servers, users, and groups from a single access point.
- The System shall allow users to add attributes/metadata to documents and classify them based on their type.
- The System shall have both simple and advanced search facilities.
- The System shall provide a policy engine to execute storage placement and migration policies.
- The System shall maintain audit trails and migration logs for traceability of operations on content.
- Documents received from external agencies shall be stored and managed within the DMS.
- The System shall store and support various document formats and be capable of supporting additional content types like audio and video in the future.
- The System shall not require additional licenses for data exchange between client/host machines and the server.
- The System shall support the application of metadata taxonomy based on keywords within the document.
- The System shall enable cross-referencing of documents for easy navigation and association.
- The System shall support full-text searching, metadata searching, or a combination of both.
- The System shall enable users to search and find documents based on associated metadata such as document type, author, title, location, active/inactive status, date created, etc.
- The System shall provide the capability to refine searches to narrow down results.
- The System shall provide an interface for managing the entire lifecycle of a document, from creation to disposition.

25.4.2. Knowledge Repository Integration:

- The System should integrate with existing knowledge repositories, including IMO's Global Maritime Information Sharing Symposium (GMISS) and other maritime safety forums.
- The System should provide advanced search capabilities to quickly locate IMO documents, resolutions, and other maritime safety information.
- The System should offer a user-friendly interface for accessing a wide range of safety knowledge assets, including research papers, case studies, and best practice guidelines.

25.4.3. Multilingual Support and Distribution:

- The System should provide a multilingual interface and document translation for global accessibility.
- The System should enable automated distribution of safety circulars to targeted user groups.
- The System should incorporate a user feedback mechanism for continuous improvement of repository content.
- The System should integrate AI-driven translation services to provide multilingual support for global accessibility.

25.4.4. Search Engine:

- The System shall enable full-text search capabilities, allowing users to search within the content of safety circulars and documentation for specific terms or phrases.
- The System shall support advanced search options, including the use of Boolean operators, wildcards, and exact phrase matching to refine search results.
- The System shall allow users to search by metadata attributes associated with safety circulars, such as document type, author, publication date, topic, and relevance to specific safety standards or regulations.
- The System shall provide a faceted search feature that enables users to filter results by multiple criteria simultaneously, such as category, date range, or status.
- The System shall offer the capability to save frequently used search queries or filters for quick access in future searches.

- The System shall maintain search history for individual users, allowing them to revisit previous searches and results.
- The System shall index safety circulars and documentation in real-time to ensure that newly added or updated materials are immediately searchable.
- The System shall provide search suggestions and auto-complete features to assist users in formulating their search queries.
- The System shall enable the ranking and sorting of search results based on relevance, date, frequency of access, or other customizable criteria.
- The System shall support the search within attachments or linked documents related to safety circulars, ensuring comprehensive coverage of all related materials.
- The System shall allow for the configuration of access permissions within the search engine to ensure that users only see search results for documents they are authorized to view.
- The System shall provide a preview feature that allows users to view snippets or summaries of documents within the search results before opening the full document.
- The System shall offer the capability to export search results into various formats for reporting or analysis purposes.
- The System shall ensure that the search engine's performance is optimized for speed and efficiency, even when handling large volumes of documents and complex queries.
- The System shall include the ability to cross-reference search results with related safety circulars or documentation, facilitating a more comprehensive understanding of safety topics.
- The System should use AI to rank search results based on document importance, user engagement, and contextual relevance.
- The system should use AI-powered virtual assistants or bot should guide users for finding safety circulars & documentations.
- The system should use AI-driven voice recognition to enable hands-free document search, enhancing accessibility.
- The system should use AI to continuously index documents as they are added or updated, ensuring instant availability in search results.

25.5. Educational and Training Content Module

25.5.1. Safety Video Library:

- The System should expand the video library to include training content on IMO conventions, codes, and emerging maritime safety topics.
- The System should enable easy access to safety videos for seafarers and maritime professionals, with bookmarking and offline viewing features.
- The System should provide analytics on video usage to identify popular topics and areas for additional training resources
- The System should allow authorized users to upload videos in common formats such as MP4, AVI, MKV.
- The System should allow embedding external videos using secure iFrame links (e.g., YouTube, Vimeo, internal cloud servers).
- The System must sanitize all iFrame inputs to prevent XSS or malicious attacks.
- The System must support metadata tagging for all videos including Title, Description, Duration, Language, Safety Category, Vessel Type, Regulation Reference (e.g., SOLAS, STCW).
- The System should auto-generate thumbnails and video previews.
- The System must support version control and archival of outdated content while retaining historical metadata and analytics.
- The System must allow content reviewers to approve, reject, or send back uploads for revision with comments.
- The System must maintain an audit trail of all uploads, edits, and publishing activities.
- The System should prevent unauthorized downloads using tokenized URLs or watermarking.
- The System should allow administrators to organize individual videos into structured learning modules with hierarchical topics.
- The System should allow defining module-level metadata such as Title, Objective, Completion Time, and Target Audience.
- The System should enable setting sequential viewing or free-flow access modes.
- The System must track individual user progress at module and video level.
- The System should allow users to resume playback from the last watched timestamp.
- The System must support linking videos to specific incidents, safety circulars, or regulatory advisories.

- The System must enforce HTTPS across all endpoints and transactions.
- The System must restrict unauthorized video access via tokenized sessions or domain-locked streaming.
- The System must log all activities (upload, view, download, delete) with timestamp and user ID.
- The System must comply with MeitY guidelines, Indian IT Act, and NIC data hosting standards.
- The System should support regular vulnerability scans, WAF, SIEM logging, and backup policies.

25.5.2. Multilingual & Accessibility Compliance:

- The System must support multilingual metadata (at minimum: English and Hindi).
- The System should allow uploading subtitles in SRT or VTT format and associate them with videos.
- The System must comply with WCAG 2.1 accessibility standards.
- The System should support screen reader compatibility, keyboard navigation, and proper color contrast.

25.5.3. Analytics and Reporting Engine:

- The System must track and display metrics such as:
  - Total Views
  - Average Watch Time
  - Completion Rates
  - User-wise/module-wise activity

- The System should support heatmaps to identify most/least engaged video segments.
- The System should allow filtered analytics by time period, category, language, and user type.
- The System should allow exporting reports in CSV or Excel format.

25.6. Advanced Analytical and Proactive Safety Tools (AAPST):

25.6.1. Predictive Analytics and Risk Assessment:

- The system shall establish a unified maritime data warehouse that integrates inputs from maritime incident reports, inspection records, vessel history, weather logs, port calls, and global safety databases (e.g., MAIB, EMCIP).
- The system shall apply data quality rules and anomaly detection mechanisms to ensure consistency, accuracy, and reliability of datasets used for modeling.
- The System should utilize predictive analytics to identify vessels, companies, or regions with higher risk profiles based on historical data and compliance records.
- The System should integrate risk assessment tools that align with IMO risk management frameworks, such as Formal Safety Assessment (FSA) guidelines.
- The System should support the proactive identification of safety trends and the development of preventive measures in line with IMO's proactive safety approach.
- The System should utilize predictive analytics models (ML/AI-based or statistical) to identify vessels, companies, ports, or regions with a high likelihood of safety incidents.
- The System must allow ingestion and analysis of data from:
  - Historical casualty/incident databases
  - PSC detentions and inspections
  - Safety violation logs
  - Environmental and navigational factors
- The System should provide risk profiling dashboards with color-coded severity indicators (e.g., High / Medium / Low Risk).
- The System must align with IMO’s Formal Safety Assessment (FSA) framework for risk quantification and control options.
- The System should enable the generation of recommendations and preventive safety circulars based on identified trends.
- The System should allow authorized users to configure risk parameters, weights, and threshold criteria dynamically.
- The system shall support the use of AI/ML models such as logistic regression, decision trees, and random forest algorithms for incident likelihood modeling.

- The system shall enable time-series forecasting using ARIMA and LSTM models for identifying high-risk operational periods.
- The system shall use clustering algorithms (e.g., K-Means) to detect patterns across vessels, operators, or trade routes associated with elevated risks.
- The system shall offer a configurable risk scoring engine that calculates composite risk scores based on parameters such as vessel type and age, incident frequency, compliance history, and environmental factors.
- The system shall categorize maritime entities (e.g., ships, ports) into high, medium, or low-risk tiers based on defined thresholds.
- The system shall enable real-time ingestion of data to trigger risk alerts and update dashboards dynamically.
- The system shall support scheduled batch processes (e.g., nightly or weekly) to refresh predictive models and update risk indices.
- The system shall implement feedback loops to refine AI models using new incident reports, enforcement actions, or safety interventions.
- The system shall support retraining of ML models based on performance metrics, user feedback, and SME inputs.
- The system shall provide confidence scores and explainable AI outputs with each prediction, enabling transparency and trust.
- The system shall maintain version control for risk models and allow oversight by a designated safety governance committee.

25.6.2. Real Time Monitoring and Alerting:

- The system shall integrate with live data sources such as AIS (Automatic Identification System), weather feeds, inspection logs, and incident reporting systems using event-streaming platforms like Apache Kafka or equivalent.
- The system shall support continuous ingestion and processing of safety-related data streams for real-time operational intelligence.
- The System should enable real-time monitoring of maritime operations.
- The system shall support streaming data ingestion from AIS, LRIT, weather feeds, and port systems.
- The system shall include an event-detection engine capable of generating alerts based on predefined rule sets and machine learning models.
- The system shall allow configurable rules for detecting high-risk vessel entries, overdue inspections, repeated non-compliance, etc.

- The system shall detect anomalies and trigger alerts for unsafe behavior or potential incidents.
- The system shall allow configuration of alert rules and escalation paths.
- The system shall log all alerts and provide a dashboard of active/inactive alert status.
- The system shall provide configurable alert workflows that route messages via email, SMS, or in-app notifications based on severity, risk level, and user roles.
- The system shall enable escalation logic that ensures alerts are acknowledged or acted upon within predefined SLAs.
- The system shall correlate related events across modules (e.g., equipment malfunction, inspection failures, and resulting incidents) to enable contextual understanding.
- The system shall visualize such incident linkages for enhanced situational awareness.
- The system shall allow dynamic configuration of thresholds for safety KPIs such as incident frequency spikes, late inspections, equipment malfunctions, or compliance violations.
- The system shall support adaptive alerting where thresholds may be tightened or relaxed based on evolving risk scores.

25.7. Cybersecurity and Data Protection (CDP):

25.7.1. Compliance and Regulatory

- The bidder shall comply with the Information Technology Act, 2000, its amendments, CERT-In guidelines, and MeitY directives.
- All data protection measures must align with India's forthcoming Digital Personal Data Protection Act (DPDP), 2023, and any future amendments thereof.
- International standards such as ISO/IEC 27001, NIST Cybersecurity Framework, and OWASP Top 10 shall guide the platform’s security architecture.

25.7.2. System and Network Security

- All systems must be protected using firewalls, intrusion detection and prevention systems (IDPS), anti-malware, and endpoint protection tools.
- Internal and external penetration testing shall be conducted quarterly by CERT-In empanelled auditors, and reports must be shared with DG Shipping.
- The platform must include protection against DDoS attacks and support IP whitelisting, port lockdowns, and runtime application self-protection (RASP).

25.7.3. Data Protection Measures

- All data at rest must be encrypted using AES-256 or higher standards; data in transit must be encrypted using TLS 1.2 or higher.
- Access to PII, maritime incident logs, and regulatory content must be governed through Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA).
- Data minimization, purpose limitation, and retention control principles must be enforced programmatically.

25.7.4. Incident Management and Breach Notification

- A documented Incident Response Plan (IRP) shall be maintained.
- In case of any data breach or cybersecurity incident, operational application or server level incident and incident related to physical & environmental security the bidder must notify DG Shipping and CERT-In within 30 minutes and submit a Root Cause Analysis (RCA) report within 72 hours.
- The platform must log all user and system activities, with logs retained securely for a minimum period of three years online and seven years offline and to be made available to DG Shipping upon request.
- The system shall log all alert-related activities, including creation, updates, acknowledgments, escalations, and user responses, with full timestamping for audit compliance.
- The system shall generate audit-ready reports for regulatory submissions and internal reviews.

25.7.5. Cloud and Infrastructure Security

- All services shall be hosted on MeitY-empanelled cloud service providers with in-country data residency.
- Cloud environments must be configured using zero-trust architecture, and sensitive workloads must be isolated from public-facing components using VPC, subnets, and access gateways.
- Cloud-native security tools such as Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platforms (CWPP) must be deployed.

25.7.6. Personnel and Vendor Security

- All project staff shall sign Non-Disclosure Agreements (NDAs) and undergo background verification.
- Security awareness training must be conducted bi-annually for all personnel involved in the development, deployment, and support of IGMSP.
- Third-party tools or services used must undergo a security evaluation and be documented in a Third-Party Risk Register approved by DG Shipping.

25.7.7. Privacy and Data Governance for Integrated Data:

- The system should establish robust data governance policies aligned with international data protection regulations, including GDPR.
- The system should ensure privacy compliance for user data, with clear policies on data collection, processing, and sharing.
- The system should implement data access management and monitoring mechanisms to regulate and audit access to sensitive maritime safety information.
- The system should define and enforce a structured data retention and deletion policy in line with the GDPR's "storage limitation" principle (Article 5) and the "right to be forgotten" (Article 17). This policy should specify retention periods (in days/months), review mechanisms, and procedures for data deletion or anonymization once data is no longer required. This will be complying as per the policy or circular of Directorate General of Shipping to be implemented.
- The system should align with DG Shipping’s forthcoming Data Privacy Framework, ensuring compliance with the DPDP Act and Rules.
- The system shall enforce governance frameworks for all AI models and maintain detailed documentation of model logic, training datasets, and accuracy metrics.
- The system shall ensure that AI-generated risk assessments are privacy-compliant and do not expose sensitive or personally identifiable information.

25.8. Compliance and Regulatory Framework:

25.8.1. Compliance Monitoring and Reporting:

- The System should monitor vessel and company compliance with IMO conventions, including MARPOL, SOLAS, and the Ballast Water Management Convention.
- The System should automate the generation of compliance reports for submission to the IMO and flag states.
- The System should provide a compliance dashboard that displays real-time compliance status and highlights areas requiring attention.
- The system shall provide digital, role-based checklists for vessel inspections, audits, port state controls, and incident investigations.
- The system shall allow administrators to configure checklist templates according to formats issued by IMO, DG Shipping, or classification societies.
- The system shall log all compliance-related activities (e.g., inspections, violations, corrective actions, audit findings) in immutable, timestamped records for legal and regulatory purposes.
- All audit logs shall be retained securely and made available to DG Shipping or authorized personnel on demand.
- The system shall trigger real-time alerts for non-compliance incidents such as overdue corrective actions, repeated regulatory breaches, or failure to conduct mandated inspections.
- Alerts shall be routed via SMS, email, and in-platform notifications based on severity level and user role.
- The system shall offer graphical dashboards displaying real-time compliance status for vessels, operators, and ports.
- Dashboards shall include filters by regulation type, compliance history, and time range, along with trend visualization of past violations and rectifications.
- The system shall auto-generate periodic compliance reports in templates aligned with statutory formats from IMO, DG Shipping, and Flag States.
- The system shall allow custom reporting by filtering data based on regulation type, organization, or violation category.

25.8.2. Regulatory Information System:

- The System should provide robust authentication mechanisms, including multi-factor authentication, to ensure secure access to the platform.

- The System should manage user roles and permissions in accordance with IMO's access control guidelines, ensuring that users have appropriate access to the system's features and data.

25.8.3. Communication and Outreach Platform:

- The System should serve as a communication platform for disseminating safety communications, updates, and alerts in line with IMO's outreach initiatives.
- The System should integrate with social media and other digital platforms to engage with the maritime community and promote safety awareness.
- The System should include analytics to measure the reach and impact of safety communications, supporting continuous improvement of outreach strategies

25.9. User Access Management:

25.9.1. User Authentication and Authorization

- The System should provide secure authentication mechanisms, including multi-factor authentication, for user access to the platform.
- The System should manage user roles and permissions, ensuring that users have appropriate access to the system's features and data.
- The system shall offer a password recovery mechanism, using email verification or pre-configured security questions to help users reset their passwords securely.
- The system shall implement access control measures, including Role-Based Access Control (RBAC), to restrict access to specific content, modules, and administrative functions based on user roles.
- The system shall securely hash and salt user passwords, using strong hashing algorithms such as bcrypt or SHA-256 to prevent unauthorized access.
- The system shall support email verification, sending a confirmation email to the registered email address to verify user identity before activating the account, if required.
- The system shall enforce strict access control using RBAC (Role-Based Access Control) to ensure that users (e.g., inspectors, administrators, operators) can only access relevant compliance data.
- Each user role shall have visibility and editing permissions aligned with their regulatory responsibilities.

25.9.2. User Account Management:

- The System should allow administrators to create, modify, and deactivate user accounts in a secure and auditable manner.
- The System should provide self-service options for users to manage their account settings, preferences, and password resets, enhancing user autonomy and reducing administrative overhead.
- The system shall provide user registration functionality, enabling all types of users to create accounts with necessary credentials as per defined roles and permissions.
- The system shall validate and verify user input data during registration to ensure accuracy and prevent fraudulent or spam registrations.
- The system shall create a user profile for each registered user and securely store their details in a centralized user database.
- The system shall allow users to edit their profile information, including name, email address, password, and other editable fields.
- The system shall provide an option to delete or deactivate user profiles, including a confirmation process to avoid accidental deletions or deactivations.
- The system shall send automated email notifications to users, including account registration confirmations, password recovery emails, profile updates, and alerts as per system configurations.

25.9.3. Access Control Policies:

- The System should enable the definition and enforcement of comprehensive access control policies that govern how users interact with the platform.
- The System should support the creation of policies based on user attributes, data classification, and contextual factors such as location or time of access.
- The system shall support the creation of multiple user roles, such as Administrator, Maker, Checker, Reviewer, and Viewer, each with unique permissions and access levels.
- The system shall allow administrators to assign users to specific roles, with the ability to manage, update, or revoke role assignments.
- The system shall allow editing of role permissions, enabling administrators to customize access levels and features available to each role.
- The system shall implement access control measures, including Role-Based Access Control (RBAC), to enforce defined access control policies across the platform.

25.9.4. User Training and Awareness:

- The System should offer training modules to educate users on security best practices, platform features, and responsible use of the system.
- The System should provide awareness programs to ensure users understand the importance of security measures such as multi-factor authentication and password management.
- The system shall provide onboarding resources, such as tooltips, walkthroughs, and training videos, to educate users on platform usage, best practices, and security awareness.

25.9.5. User Support & Helpdesk:

- The System should include a helpdesk or support system to assist users with access issues, account recovery, and other related inquiries.
- The System should provide a knowledge base or FAQ section to help users resolve common issues independently.
- The system shall incorporate user feedback mechanisms, including options such as feedback forms, discussion forums, surveys, and support ticket submissions.
- The system shall display in-app notifications to users, including alerts, reminders, updates, and warnings, tailored to their role and activity on the platform.
- The system shall provide robust error handling and user feedback, displaying meaningful messages and guidance when actions fail or return no results.

26. Annexure- V – Technical Requirements Specification

26.1. Manufacturer Authorization Form (MAF)

#	Components	Submitted				Document Reference				
1	Cloud Network security Services									
2	Cloud Application and Platform Services									
3	Next Generation Firewall Services									
4	DDOS Services Cloud DC & DR									
5	Antivirus + EDR Services for Cloud DC & DR									
6	Web Application Firewall Services									
7	DLP Service									

26.2. Cloud Network Security Services

Sr. No.	Description of Requirement	Compliance (Yes/No)	Details of Reference Document for Verifying Compliance	Reference Page No
Cloud Data Center Security				
1	Cloud service provider should offer redundant availability zones (AZs) and regions for resilience in case of failures.			
2	Continuous monitoring of access using IAM policies, audit logs, and cloud security monitoring tools (e.g., AWS Guard Duty, Azure Security Center, Google Security Command Center).			
3	Multi-factor authentication (MFA) must be enforced for access to cloud consoles, APIs, and management tools.			
4	Cloud-native fire protection mechanisms, including automated fire risk assessments and backup procedures (e.g., geo-redundant data storage).			
5	Data centers should adhere to cloud-specific physical security certifications (ISO 27001, SOC 2 Type II, FedRAMP).			
6	Geo-redundant backup and disaster recovery planning across multiple cloud regions to ensure high availability and compliance.			
Cloud Server Security				
7	Cloud servers should have network-based security controls (e.g., security groups, cloud-native firewalls, host-based IDS/IPS like AWS Inspector, Azure Defender). Use cloud-agnostic IDS/IPS solutions.			
8	Use hardened cloud VM images with minimal services enabled (e.g., CIS-hardened AMIs for AWS, Azure Security Baselines).			
9	Enforce secure guest OS configurations through automated tools (e.g., AWS Systems Manager, Azure Policy, Google OS Config).			

26.3. Cloud Application and Platform Services

#	Description of Requirement	Compliance (Yes/No)	Details of Reference Document for Verifying Compliance	Reference Page No
1	Ensure secure, isolated applications on a cloud-based PaaS using containerization (e.g., Kubernetes, AWS Fargate, Azure Kubernetes Service) and microservices			

#	Description of Requirement	Compliance (Yes/No)	Details of Reference Document for Verifying Compliance	Reference Page No
	architecture.			
2	Follow secure cloud application development guidelines, including secure coding standards (e.g., OWASP, NIST), API security best practices, and encryption enforcement.			
3	Implement automated security testing for vulnerabilities in applications before deployment using cloud-native tools (e.g., AWS Code Guru, Azure DevOps Security, Google Cloud Security Scanner).			
4	Automate patch management and change control using cloud-native services (e.g., AWS Systems Manager Patch Manager, Azure Update Management, Google Cloud OS Patch Management).			
5	Ensure patches are tested in staging environments before production deployment using automated CI/CD pipelines (e.g., GitHub Actions, AWS Code Pipeline, Azure DevOps).			

26.4. Next Generation Firewall Services

Sr. No.	Description of Requirement	Compliance (Yes/No)	Details of Reference Document for Verifying Compliance	Reference Page No
1	The solution/offering should be a cloud-based service.			
2	The proposed solution should have certifications relevant to cloud security, such as SOC 2, ISO 27001, FedRAMP, or equivalent.			
3	The cloud firewall should provide firewall, IPS, and VPN (both IPSec and SSL) functionality in a single solution.			
4	Ensure the firewall is fully virtualized and supports cloud-native horizontal scaling rather than relying on hardware-bound architecture. threats.			
5	Firewall should support concurrent VPN peers (IPSec/SSL) as required.			
6	Firewall should support minimum VLANs as required in the project.			
7	Firewall should support virtual firewalls from day one and allow license-based scalability when needed.			
8	Firewall should provide application inspection for DNS, FTP, HTTP, SMTP,			

Sr. No.	Description of Requirement	Compliance (Yes/No)	Details of Reference Document for Verifying Compliance	Reference Page No
	LDAP, VLAN, VXLAN, MGCP, RTSP, SIP, SQLNET, SNMP, etc.			
9	Use a distributed cloud firewall that dynamically scales across regions and availability zones instead of hardware-based clustering.			
10	Ensure the NGFW solution supports cloud-native HA using multiple availability zones without requiring dedicated hardware.			
11	Firewall should support routed & transparent modes, with the ability to set modes independently in multi-context environments.			
12	In transparent mode, the firewall should support ARP inspection to prevent Layer-2 spoofing.			
13	Should support non-stop forwarding (NSF) in HA mode to ensure minimal downtime during failover.			
14	Firewall should support NAT (static, dynamic, PAT, destination-based NAT, NAT66, NAT64, NAT46).			
15	Should support Remotely Triggered Black Hole (RTBH) for BGP security.			
16	Firewall should support RESTful API for integration with third-party solutions, including Software-Defined Networking (SDN).			
17	Firewall should support stateful failover of sessions in Active/Standby or Active/Active mode.			
18	Firewall should replicate NAT translations, TCP/UDP connection states, ARP table, ISAKMP & IPSec SA's, SIP signaling sessions during failover.			
19	Firewall should support client-based and clientless SSL VPN connections from day one. Use cloud-native traffic analysis services rather than dedicated hardware-based monitoring solutions.			
20	Firewall should comply with VPNC/ICSA for interoperability.			
21	Should support pre-shared keys & digital certificates for VPN peer authentication.			
22	Should support Perfect Forward Secrecy (PFS) & Dead Peer Detection (DPD) for VPN connections.			
23	Should support NAT-T for IPSec VPN.			
24	Routing Features: Should support IPv4 & IPv6 static routing, RIP, OSPF v2 & v3,			

Sr. No.	Description of Requirement	Compliance (Yes/No)	Details of Reference Document for Verifying Compliance	Reference Page No
	BGP, PBR, VLAN, VXLAN for PBR, and BGPv6.			
25	Firewall should support PIM multicast routing.			
26	Firewall should support SLA monitoring for static routes.			
27	Firewall should allow management of firewall policies via CLI, SSH, and inbuilt GUI.			
28	Firewall should support automatic software updates to check for and download the latest versions.			

26.5. Intrusion Prevention System (IPS) Services

Sr. No.	Description of Requirement	Compliance (Yes/No)	Details of Reference Document for Verifying Compliance	Reference Page No
1	Solution/offering should be a cloud-based IPS service.			
2	The IPS should be capable of detecting and blocking all known, high-risk exploits along with their underlying vulnerabilities.			
3	The IPS should be capable of detecting and blocking zero-day attacks without requiring an update.			
4	The IPS should employ full seven-layer protocol analysis for detecting threats across various internet protocols and data file formats.			
5	The IPS should be able to detect and block malicious web traffic on any port.			
6	The IPS should detect attacks inside IPv6 encapsulated packets.			
7	The IPS should be capable of active blocking of traffic based on pre-defined rules to prevent attacks before damage occurs.			
8	The IPS should detect intrusion attempts such as unauthorized access, pre-attack probes, DoS/DDoS attacks, brute force, and zero-day attacks.			
9	The IPS should allow traffic filtering based on IP address/network range, protocol, and service to enforce organizational security policies.			
10	The IPS should support Active/Passive and Active/Active modes for High Availability to prevent session drops.			

Sr. No.	Description of Requirement	Compliance (Yes/No)	Details of Reference Document for Verifying Compliance	Reference Page No
11	The IPS should allow policy assignment based on device, port, VLAN tag, and IP address/range.			
12	The IPS should offer built-in responses including console alerts, database logging, email notifications, SNMP traps, and packet captures.			
13	The IPS should operate in asymmetric traffic environments and provide vulnerability/exploit filters for protection.			
14	The IPS should use machine learning to prevent attacks from obfuscated script-based content and detect domain generation algorithms used for malware downloads.			

26.6. Distributed Denial-of-Services (DDOS)

Sr. No.	Description of Requirement	Compliance (Yes/No)	Details of Reference Document for Verifying Compliance	Reference Page No
1	The solution should be a cloud-based DDoS mitigation service.			
2	The solution should be capable of detecting and mitigating multiple attack vectors simultaneously, covering OS, Network, Application, and Server-side attacks.			
3	The solution should be able to detect, inspect, and mitigate both IPv4 & IPv6 attacks.			
4	The solution should provide real-time DDoS detection using statistical anomaly-based detection mechanisms.			
5	The system should provide near-real-time traffic graphs and tables for anomaly detection and alerts.			
6	The system should have zero-day DDoS flood attack detection and prevention capabilities.			
7	The system should allow rule-based notification alerts based on anomaly severity and traffic thresholds.			
8	The system should have portal-based user access, with different roles and permission levels for administrators and operators.			
9	The system should provide real-time dashboards for alert activity and mitigation status.			

Sr. No.	Description of Requirement	Compliance (Yes/No)	Details of Reference Document for Verifying Compliance	Reference Page No
10	The system should allow configuration rollback to previous versions for recovery.			
11	The system should support automated anomaly classification (e.g., Possible Attack, False Positive).			
12	The system should allow traffic diversion for selective mitigation without impacting legitimate traffic.			
13	The system should allow automatic fingerprint downloads from a central server to recognize ongoing threats.			
14	The system should provide alert-based notifications via SYSLOG, SNMP, or SMTP for mitigation events and service degradation.			

26.7. Anti-Virus + EDR Services for Cloud DC & DR

Sr. No.	Description of Requirement	Compliance (Yes/No)	Details of Reference Document for Verifying Compliance	Reference Page No
1	Cloud-based Anti-virus and EDR solution should be deployed on all servers/VMs in the Cloud DC & DR.			
2	The anti-virus definitions and security updates should be automatically downloaded and applied from a centralized cloud-based management system.			
3	The solution should provide real-time, scheduled, and on-demand scanning capabilities to detect and mitigate threats.			
4	The EDR solution should provide behavioral analysis, heuristic scanning, and threat intelligence integration for advanced threat detection.			
5	The solution should include firewall, intrusion prevention, and exploit prevention features for endpoint security.			
6	The anti-virus and EDR solution should detect and prevent zero-day malware, ransomware, and advanced persistent threats (APT).			
7	The solution should support automated incident response with forensic analysis and rollback capabilities.			

Sr. No.	Description of Requirement	Compliance (Yes/No)	Details of Reference Document for Verifying Compliance	Reference Page No
8	The cloud-based platform should provide centralized policy enforcement, reporting, and visibility across all endpoints.			
9	The solution should have data leak prevention (DLP) and application control to prevent unauthorized data exfiltration and application misuse.			
10	The cloud-native EDR solution should block blacklisted applications and prevent malicious code injection in trusted processes.			

26.8. Web Application Firewall (WAF) Services

Sr. No.	Description of Requirement	Compliance (Yes/No)	Details of Reference Document for Verifying Compliance	Reference Page No
1	The WAF solution should be cloud-native and fully managed, providing protection for web applications hosted in the Cloud DC & DR.			
2	The solution should address OWASP Top Ten security vulnerabilities, including SQL Injection, Cross-Site Scripting (XSS), Broken Authentication, and others.			
3	The WAF should prevent Brute Force, DDoS, unauthorized access, and reconnaissance attacks.			
4	Should support positive and negative security models for threat protection.			
5	Should have built-in caching, compression, and SSL acceleration for optimized performance.			
6	Should have integrated SSL Offloading and TLS termination for encrypted traffic inspection.			
7	Should have basic load balancing capabilities for high availability.			
8	The WAF should inspect application output, log actions, and enforce security policies dynamically.			
9	Should inspect HTML, DHTML, CSS, HTTP, HTTPS (TLS), and other web protocols.			
10	WAF should support dynamic source IP blocking to mitigate malicious attacks.			
11	Should inspect XML traffic along with HTTP/HTTPS requests.			
12	Should support WebSocket traffic inspection for application security.			
13	Should support inline bridge and proxy mode deployment.			
14	Should have an option for Reverse Proxy mode configuration.			
15	The WAF should have actions to block/drop malicious requests and IPs.			
16	Transactions matching attack signatures should be blocked using heuristics-based detection.			
17	Should include a pre-configured attack signature database with real-time updates.			
18	Admins should be able to modify or add custom attack signatures.			

Sr. No.	Description of Requirement	Compliance (Yes/No)	Details of Reference Document for Verifying Compliance	Reference Page No
19	WAF should support automatic signature updates for up-to-date threat intelligence.			
20	Should support various normalization methods (URL-decoding, Null byte handling, Unicode encoding, etc.).			
21	Should support different policies for different application sections.			
22	Should automatically learn web application structure and adapt to changes.			
23	Should perform behavioral learning for anomaly detection and policy recommendations.			
24	WAF should maintain low latency and high throughput for performance optimization.			
25	Should support uploading SSL certificates and key pairs for secure applications.			
26	The WAF should have anti-automation protection against bot attacks.			
27	Should provide out-of-band management capabilities.			
28	The WAF should support web-based centralized management and reporting.			
29	WAF should be deployable with minimal impact on existing applications and network.			
30	Should generate custom or pre-defined graphical reports on demand.			
31	Should provide a dashboard for system status and web activity monitoring.			
32	Should generate detailed event reports with filtering options (date, IP, incident types, geo-location).			
33	Should support multiple report formats (PDF, XML, HTML, etc.).			
34	Each HTTP transaction should have a unique transaction ID for logging.			
35	WAF should support log uploads to external logging servers (via FTP, SFTP, SCP).			
36	Should provide real-time notifications (Email, Syslog, SNMP Trap, HTTP push).			
37	Should log full session data for suspicious transactions.			
38	Should allow automatic policy			

Sr. No.	Description of Requirement	Compliance (Yes/No)	Details of Reference Document for Verifying Compliance	Reference Page No
	relaxation for fine-tuning.			
39	The solution should allow manual acceptance of false positives.			
40	Should be able to recognize and trust specific hosts.			
41	In passive mode, WAF should simulate impact of rule changes.			
42	Should support clustering and shared policy deployment across multiple WAFs.			
43	The WAF should support virtual environments and cloud-based deployments.			
44	Should provide load balancing in active-active environments.			
45	Should integrate with LDAP and RADIUS authentication.			
46	Should support troubleshooting commands (PING, traceroute).			
47	Should allow NTP server configuration for time synchronization.			
48	Should support both IPv4 and IPv6 networks.			

26.9. Data Leak Prevention (DLP) Services

Sr. No.	Description of Requirement	Compliance (Yes/No)	Details of Reference Document for Verifying Compliance	Reference Page No
1	The solution should be a cloud-native and fully managed DLP service.			
2	Should provide centralized web-based management for system administration.			
3	Ensure compatibility with industry-standard SAML, OAuth, and OpenID for multi-cloud support.			
4	The solution should maintain detailed audit logs tracking all admin activities, including:			
4a	Creation, deletion, and updating of DLP user groups.			
4b	Creation, deletion, and updating of DLP user roles.			
4c	Modifications to DLP network policies and configurations.			
4d	All logins to the web console for monitoring and administration.			

Sr. No.	Description of Requirement	Compliance (Yes/No)	Details of Reference Document for Verifying Compliance	Reference Page No
4e	Creation, deletion, and modification of DLP policies.			
5	Should support agent-based scanning with incremental scans to optimize performance.			
6	Should provide granular role-based access control (RBAC) for administrators and security teams.			
7	Ability to define system administration roles separately from policy and incident management roles.			
8	Ability to create roles for policy authors without permission to deploy policies live.			
9	Ability to define roles that can only view security incidents but not modify them.			
10	Should support rules based on cloud directory attributes (e.g., business unit, department).			
11	Should provide predefined compliance policies for regulations like GDPR, HIPAA, PCI DSS.			
12	Ability to define policies for individual users or groups, with exception management.			
13	Policies should be applicable across data in transit, at rest, and in use in the cloud.			
14	Should enforce different policies based on network connectivity (on-prem vs. remote/cloud).			
15	Should provide consistent detection capabilities across cloud and endpoint devices.			
16	Should support policy segregation for content discovery and action rules.			
17	Should offer a unified web-based console for policy management across all cloud workloads.			
18	Should monitor and protect data in motion across cloud-based communication channels:			
18a	Cloud email (Microsoft 365, Google Workspace).			
18b	Cloud file-sharing services (OneDrive, Google Drive, Dropbox).			
18c	Cloud messaging platforms (Slack, Microsoft Teams, WhatsApp, etc.).			
19	Use cloud-native traffic analysis			

Sr. No.	Description of Requirement	Compliance (Yes/No)	Details of Reference Document for Verifying Compliance	Reference Page No
	services rather than dedicated hardware-based monitoring solutions.			
20	Ability to scan cloud storage (S3, Azure Blob, Google Cloud Storage, SharePoint Online, etc.).			
21	Support for definable scan schedules for cloud environments.			
22	Ability to measure scanning efficiency and balance workload dynamically.			
23	Should support full and partial fingerprinting for structured and unstructured data.			
24	Role-based access should allow summary reports without exposing detailed incidents.			
25	Should include pre-built content classification templates and contextual detection:			
25a	Keyword-based and machine-learning-based detection.			
25b	Detection of encrypted or password-protected files.			
25c	Fingerprinting and proximity-based detection.			
26	Should detect content based on actual file content, not just file extensions.			
27	Should provide out-of-the-box predefined policies for cloud data protection.			
28	Custom policies should allow classification based on metadata, sender, recipient, file type, risk level, and severity.			
29	Ability to assign severity ratings (High/Medium/Low) to incidents.			
30	Should define and enforce data security throughout the customer data lifecycle.			
31	Should support secure data isolation mechanisms for multi-tenant cloud environments.			
32	Should perform regular cloud backups, with customer access to audit logs.			
33	Should provide data erasure capabilities to ensure complete data deletion upon request.			

26.10. Additional Security Requirements

Sr. No.	Security Component	Description of Requirement	Compliance Standards/Best Practices
1	Cloud Security Posture Management (CSPM)	Solution must detect and remediate cloud misconfigurations, provide continuous monitoring, and align with industry compliance frameworks.	NIST SP 800-53, CIS Benchmarks, ISO/IEC 27001:2022
2	Cloud Workload Protection Platform (CWPP)	Must provide runtime protection for VMs, containers, and Kubernetes, including IDS/IPS, malware detection, and vulnerability management.	CIS Benchmarks, NIST 800-190, PCI DSS Requirement 5
3	Cloud Identity & Entitlement Management (CIEM)	Must enforce least-privilege access, monitor excessive permissions, and support MFA, RBAC, and Just-In-Time (JIT) access controls.	ISO 27002:2022, NIST 800-63, CIS IAM Best Practices
4	Secure Web Gateway (SWG)	Solution must protect against web-based threats, enforce browsing policies, inspect SSL/TLS traffic, and integrate DLP policies.	GDPR (Article 32), ISO 27001 Annex A.13, PCI DSS Requirement 4
5	Threat Intelligence & Dark Web Monitoring	Must continuously monitor cyber threats, detect leaked credentials, and integrate with SIEM for proactive threat detection.	NIST Cybersecurity Framework, MITRE ATT&CK, GDPR (Article 33)
6	Serverless & API Security	Must provide protection for APIs and serverless applications against OWASP API Top 10 threats, enforce authentication, and detect anomalies.	OWASP API Security, NIST SP 800-204, ISO 27001: A.14
7	Zero Trust Network Access (ZTNA)	Solution must enforce identity-based access, replace traditional VPNs with granular controls, and prevent lateral movement.	NIST 800-207, CISA Zero Trust Model, ISO 27001 Annex A.9
8	Cloud-Native SIEM & SOAR	Must provide centralized logging, automated incident response, correlation with threat intelligence, and compliance with security monitoring regulations.	ISO 27035, NIST 800-92, PCI DSS Requirement 10
9	Data Security Posture Management (DSPM)	Must classify and secure sensitive data across multi-cloud environments, ensuring encryption and access controls.	GDPR (Article 5), HIPAA Security Rule, ISO 27018
10	Cloud Forensics & Incident Response (CFIR)	Solution must capture and analyze cloud activity logs, automate incident response, and store forensic evidence securely.	NIST 800-86, ISO 27037, PCI DSS Requirement 12.10
11	Cloud-Based Deception Technology	Must deploy decoys and honeypots to detect insider threats and lateral movement, providing high-fidelity alerts.	MITRE Engage, NIST Cybersecurity Framework, CIS Control 7

Undertaking from Vendor:

1 Vendors must detail how their solutions meet each requirement.

2 Proposals should include references to compliance frameworks and certifications.

3 Solutions must be cloud-agnostic, fully managed, and independent of any single cloud service provider (AWS, Azure, GCP, etc.).

4 Vendors should specify integration capabilities with existing security tools (e.g., SIEM, IAM, threat intelligence platforms).

5 Any additional security features beyond the listed requirements should be highlighted.

Section 6 – Service Level Agreement

1. Structure

This SLA shall operate as a legally binding services agreement specifying terms which apply to the Parties in relation to the provision of the Services by the Bidder to DGS and its nominated agencies under the Agreement and the MSA

1.1. Objectives of SLA

The objective of SLA is to clearly define the expected level of the services being offered by the Bidder (Successful Bidder) to the Purchaser (DGS) for the period of the contract or until the SLA has been amended. SLA defines the responsibility of the successful bidder in ensuring adequate delivery of the deliverables and the services coupled with correctness of the same based on the performance indicators detailed out in this document.

The Bidder shall be required to ensure that the Service Levels which shall ensure the following:

i. Improving the efficiency of operations for the departments.

ii. Leveraging the benefits in new system in order to:

   a. Reduce of manual records and replace with computerized standardized documents.

   b. Infuse transparency in operations by enabling the stakeholders to have easy access to the records and provision of login ids and biometrics to infuse accountability in operations

   c. Enable faster request processing in delivery of services with better turnaround time.

   d. Facilitate automated data transfer with state-wide connectivity to prevent unnecessary duplication & simplify preparation of registers and reports.

   e. Generate meaningful MIS from the system.

   f. Provide inbuilt mechanism of security and quality control for crucial dealer data.

To meet the aforementioned objectives the Bidder will provide the Service Levels in accordance with the performance metrics as set out in detail in this. Bidder shall provide services as defined in the scope of work in accordance with the conditions mentioned in Section to ensure adherence to project timelines and error free availability of the services.

1.2. Details of SLA Penalty Mechanism and Calculations

The MSP will get 100% of Quarterly Payout for the concerned quarter if the performance metrics are complied with for all the parameters and the total SLA score in a quarter is 50 or above. The Bidder will get lesser payment in case of a lower performance exhibited by a SLA score of less than 50. The maximum penalty to be levied is 10% of Quarterly Payout.

The payment will be made by DGS to the bidder on quarterly basis. The quarterly invoice will be submitted by the Bidder to the DGS, who will in turn release the 80% of the payment if there is no dispute and after verification/audit of the invoices and necessary documents, release balance 20% payment.

The Bidder will be eligible for an SLA holiday period wherein the SLAs shall not be applicable. This SLA holiday period will not be more than a quarter from the date of GO-Live of the project, until and unless decided or agreed with DGS. The SLA holiday period is for streamlining the SLA measurement and monitoring process of the project.

The payment and SLA penalty applicability will be against the specific SERVICE LEVEL PARAMETERS depending on the impact. The values will be calculated separately, and payment will be made against invoices raised for the port.

DGS reserves the right to modify the SLAs in terms of addition, alteration or deletion of certain parameters, based on mutual consent of all the parties i.e. DGS and BIDDER.

The Penalties will be calculated based on the following table:

S. No.	SLA Score Range	Deductions (Penalties)
Deductions		
1	=50	No Penalty
2	<50 & >=45	0.25% penalty for every point < 50
3	<45 & >=40	0.5% penalty for every point < 50
4	<40	0.75% for every point < 50
Note: The percentage penalty would be calculated on the bill raised by the Bidder for the concerned quarter.		
Example: • SLA Score of 48 will lead to a Penalty of 0.5% (i.e. 2 x 0.25 = 0.5%) • SLA Score of 43 will lead to a Penalty of 3.5% (i.e. 7 x 0.5 = 3.5%) • SLA Score of 38 will lead to a Penalty of 9% (i.e. 12 x 0.75 = 9%)		

Note

1 Annual review SLA shall be done by DGS and appropriate modifications/amendments to the SLAs may be carried out.

2 Cascading effect (effect on multiple SLA criterions) of failure or non-performance of a particular project component on SLAs shall be avoided.

3 Web-based Incident and SLA monitoring tool providing reports against the parameters mentioned below will be used for measurement. DGS may request for supporting documents in certain cases if required. Such tool needs to be deployed after certification from a Third-Party CERT-IN agency such as STQC before Go-live of the project.

4 Implementation of a Web-based Project Management Information System (PMIS) for Project progress and ITIL based SLA monitoring and Incident Management (EMS) has to be carried out by before Go-live in order to receive any payment for the project

1.3. SLA Measurement and Monitoring

1.3.1. SLA applicable during Implementation Phase

Implementation of a Web-based Project Management Information System (PMIS) for Project progress and SLA monitoring has to be carried out by before Go-live in order to receive any payment for the project.

#	Services	Parameter	Validation	Penalty
1	Adherence to project timelines	Up to 4 calendar weeks delay from the timelines as mentioned in the project timelines Volume	**Measurement Tool:** Project Management Information System (PMIS) Periodic Project Progress Reports	No Penalty
		Delay beyond 4 weeks		Rs. 1,00,000 per week of delay If the delay exceeds more than 12 weeks, DGS may decide to invoke breach clause
2	Substitution of resources from those CVs provided during the technical evaluation	Substitution of resources will be allowed with prior approval from DGS, provided that the substitute resource has a similar or better profile in terms of qualifications and experience. The substitution request must be submitted along with the project plan or thereafter, with a justification for the substitution	Request submitted for substitution along with the project plan or thereafter. The substitute resource's profile must be reviewed and approved by DGS.	No penalty will be imposed if the substitution is approved by DGS and the substitute resource meets the required qualifications and experience. A penalty of 50% of the amount quoted for that resource in the financial bid will be imposed if the substitution is made without prior approval or if the substitute resource does not meet the required qualifications and experience. This will be detailed in the contract document

1.3.2. SLA parameters during Operations and Maintenance Period

The key Service Level Agreement required for the Platform for IGMSP(Indian Global Maritime Safety Portal) software’s availability, which need to be ensured by the Bidder during the operations and maintenance support period. All complaints shall be lodged with the service desk managed by the BIDDER, which will allot ticket number for each complaint indicating location, function, time of registration and severity of the complaint. Centrally managed web-based ticketing tool for lodging the complaints will be provided by Bidder, as a part of the facilities.

SLA shall become the part of contract between DGS and the Bidder. The Bidder has to comply with Service Levels requirements to ensure adherence to quality and availability of services, throughout the period of this contract - for a period of 2 (Two) years. The performance of the support shall be tracked monthly as per the SLA service levels detailed in this section.

Please note that the Bidder shall be responsible for overall monitoring and management. The Bidder shall monitor the uptime of all associated infrastructure components for Platform solutions.

In case of any breach on above stated associated infrastructure uptime, Bidder has to submit an auto generated report from automated measurement tool of all the SLA requirements wherever applicable in this section.

SLA Parameters during Operations and Maintenance Period							
Parameter	**Baseline**		**Lower Performance**		**Breach**		**Measurement**
	Metric	**Score**	**Metric**	**Score**	**Metric**	**Score**	
Application							
Availability for application functionality							
Availability (uptime) of applications for doing business activities, except during scheduled down time as agreed with the department	>=99%	5	<99% to >= 95%	2.5	<95%	-3	Automated measurement tool to be developed as part of SLA monitoring tool to provide metric values against this parameter. End-to-end loop back mechanism must be established for checking the availability of services.
Uptime = {1 - [(Application downtime – maintenance Downtime) / (Total Time – Maintenance Downtime)]}							
Time for on-line submission of the electronic forms.	<=5 seconds	2	>5 seconds and <=7 seconds	1	>7 seconds	-1	Automated measurement tool to be developed as part of SLA monitoring tool to provide metric values against this parameter.
Average must be achieved with maximum time till success for 90% or more of the total submissions within the stipulated time							
Web-to-web response time							
Time for uploading data file including xml, txt, etc. (other than images and pdf) on various portals.	<=20 seconds	2	> 20 seconds and <=30 seconds	1	> 30 seconds	-1	Automated measurement tool to be developed as part of SLA monitoring tool to provide metric values against this
Average must be achieved with maximum time till							

SLA Parameters during Operations and Maintenance Period							
Parameter	Baseline		Lower Performance		Breach		Measurement
	Metric	Score	Metric	Score	Metric	Score	
success for 90% or more of the total uploads within the stipulated time							parameter.
Web-to-web response time							
API service availability							
Availability of API services for mobile, portal and other third-party applications	>=99%	2	<99% and >=95%	1	<95%	-1	Automated measurement tool to be developed as part of SLA monitoring tool to provide metric values against this parameter. End-to-end loop back mechanism must be established for checking the availability of services.
Response time for API Service requests							
Time for providing response to the request received	<=5 seconds	2	> 5 seconds and < =7 seconds	1	> 7 seconds	-1	Automated measurement tool to be developed as part of SLA monitoring tool to provide metric values against this parameter. End-to-end loop back mechanism must be established for checking the availability of services.
Application Maintenance							

SLA Parameters during Operations and Maintenance Period							
Parameter	Baseline		Lower Performance		Breach		Measurement
	Metric	Score	Metric	Score	Metric	Score	
Time to deliver the application changes as per desired functionality.	Within Agreed timeline	2	NA	NA	Beyond Agreed timeline	-1	Reports regarding the same to be captured through PMIS tool. All requests will be entered in PMIS by the bidder team as per records and provide status against the same
Documentation Management							
Maintaining document versioning (SRS, User Training Manual etc.), application version control	at the end of every quarter	1	Up to one week beyond the quarter end date	0.5	more than a week beyond the quarter end date	-1	Reports to be displayed through PMIS tool (and if requested by DGS) and emails to provide these details
Integration and interfacing							
Time to post information to External system in form of messages after the transaction carried out within Web Platform/application	<=10 seconds	2	>10 seconds and < =15 seconds	1	> 15 seconds	-1	Automated measurement tool to be developed as part of SLA monitoring tool to provide metric values against this parameter.
Time to receive and update information in Web Platform/application system after receipt of same from External system	<=5 seconds	2	>5 seconds and < =7 seconds	1	> 7 seconds	-1	Automated measurement tool to be developed as part of SLA monitoring tool to provide metric values against this parameter.
Data exchange with external systems							

SLA Parameters during Operations and Maintenance Period							
Parameter	Baseline		Lower Performance		Breach		Measurement
	Metric	Score	Metric	Score	Metric	Score	
Time to post information to external system after the transaction carried out within Web Platform/application	as agreed at the time of design	2	NA	NA	Beyond agreed timelines	-1	Automated measurement tool to be developed as part of SLA monitoring tool to provide metric values against this parameter.
Time to receive and update information in external system after receipt of same from eGov system	as agreed at the time of design	2	NA	NA	Beyond agreed timelines	-1	Automated measurement tool to be developed as part of SLA monitoring tool to provide metric values against this parameter.
Compute and Storage Infrastructure							
Data Centre Availability							
Uptime of all components at DC, (Network infrastructure related) & DR including but not limited to: · Servers · Storage · Tape Library · SAN · SwITBhes · Routers Any downtime for maintenance shall be with prior written intimation and approval of DGS . Uptime = {1 - [(Component downtime – maintenance Downtime) / (Total Time – Maintenance Downtime)]}	>=99.5%	3	<99.5% and >=99%	1	<99%	-1	Automated measurement tool to be developed as part of SLA monitoring tool to provide metric values against this parameter. End-to-end loop back mechanism must be established for checking the availability of services.

SLA Parameters during Operations and Maintenance Period							
Parameter	Baseline		Lower Performance		Breach		Measurement
	Metric	Score	Metric	Score	Metric	Score	
Security Components Availability							
Uptime of all security components for DC and BCP/DR site including but not limited to: · Perimeter Security · Firewall, Network swITBhes etc. Any downtime for maintenance shall be with prior written intimation and approval of DGS. Uptime = {1 - [(Component downtime – maintenance Downtime) / (Total Time – Maintenance Downtime)]}	>99%	3	< 99% to >= 98%	1	<98%	-1	Automated measurement tool to be developed as part of SLA monitoring tool to provide metric values against this parameter. End-to-end loop back mechanism must be established for checking the availability of services.
Monitoring and management							
IT Infrastructure monitoring solution availability							
Availability of IT Infrastructure Monitoring Tools at the active site.	>99%	2	< 99% to >= 95%	1	<95%	-1	Automated measurement tool to be developed as part of SLA monitoring tool to provide metric values against this parameter. End-to-end loop back mechanism must be established for checking the availability of services.
CPU and RAM Utilization							

SLA Parameters during Operations and Maintenance Period							
Parameter	**Baseline**		**Lower Performance**		**Breach**		**Measurement**
	Metric	**Score**	**Metric**	**Score**	**Metric**	**Score**	
Peak CPU and RAM utilization for Application & Database Servers at DC site. The number of such occurrences where in the CPU utilization is more than 80% for a sustained period of more than 4 hours except for scheduled batch processing tasks.	No Breach	2	NA	NA	CPU utilization is more than 80% for a sustained period of more than 4 hours	equal to in Where in is number of such instances in the reporting period	Automated measurement tool to be developed as part of SLA monitoring tool to provide metric values against this parameter. End-to-end loop back mechanism must be established for checking the availability of services.
Applications Operations Infrastructure							
Tickets / Incident Response time*							
Time taken for sending email response & ticket assignment from the time of registering of request. Must be achieved within agreed timeline for resolution for at least 95% of the cases in a month.	<=1 hrs	2	>1 hrs and <=4 hrs	1	> 4 hrs	-1	Automated measurement tool (reports from ticket management system) to be developed as part of SLA monitoring tool to provide metric values against this parameter.
Resolution for Critical incident	<=2 hours	2	> 2 hours to <= 4 hrs	1	> 4 Hours	-1	Automated measurement tool (reports from ticket management system) to be developed as part of SLA monitoring tool to provide metric values against this parameter.
Resolution for	<=4	2		1		-1	Automated

SLA Parameters during Operations and Maintenance Period							
Parameter	Baseline		Lower Performance		Breach		Measurement
	Metric	Score	Metric	Score	Metric	Score	
medium level incident	hours		> 4 hours to < = 8 hrs		> 8 Hours		measurement tool (reports from ticket management system) to be developed as part of SLA monitoring tool to provide metric values against this parameter.
Resolution for Low level incident	<= 1 day	2	>1 day to < = 3 days	1	> 3 Days	-1	Automated measurement tool (reports from ticket management system) to be developed as part of SLA monitoring tool to provide metric values against this parameter.
Training and capacity building							
Training Rating							
The training and capacity building satisfaction will be measured by feedback rating given by the trainees during online and face to face training. Average rating must be achieved above the specified rating score for more than 80% of the feedback ratings received	Rating >= 80%	2	Rating <80% and Rating >= 70%	1	Rating < 70%	-1	Feedback rating given by the trainees during online and face to face training and uploaded on PMIS
Training material							
Update of training materials on all portals within 1 week from date of	Within 1 Week	2	up to 2 weeks	1	more than 2 weeks	-1	Automated measurement tool (reports from PMIS) to

SLA Parameters during Operations and Maintenance Period							
Parameter	Baseline		Lower Performance		Breach		Measurement
	Metric	Score	Metric	Score	Metric	Score	
release of modification to software into production environment							be developed as part of SLA monitoring tool to provide metric values against this parameter.
Human Resource availability							
Human Resource availability measures the availability of the required skill sets as proposed by the Bidder in its proposal. This parameter shall also take into account the quality of resources in terms of skill set, experience and ability to perform in similar environment besides deployment on the project. In case of replacements, the new resource should be of similar or higher skill set. The skill sets to be taken into account for measuring this parameter includes the following at a minimum:	No Deviation	2	NA	NA	In case of deviations	-1	All deviations would be recorded, and MIS report shall be made available to the DGS and ports via PMIS
• Resource requirements as per Volume I of RFP • Team members for various skills required for carrying out the activities of the project							Occurrences such as national / public holidays, force majeure, labor laws, etc. shall not be considered as an occurrence for deduction

SLA Parameters during Operations and Maintenance Period							
Parameter	**Baseline**		**Lower Performance**		**Breach**		**Measurement**
	Metric	**Score**	**Metric**	**Score**	**Metric**	**Score**	
Monthly Project Progress Report							
Submission of monthly progress report including the following:	Within 2 days from month end	2	NA	NA	Greater than 2 days	-1	Automated measurement tool (reports from PMIS) to be developed as part of SLA monitoring tool to provide metric values against this parameter.
- Progress against project plan							
- Key dependencies							
- Details of non-compliances if any							
- Issues list							
- Activities completed within the reporting period							
- Activities to be completed in the next reporting period							

1.3.3. Severity definition chart

Severity definition chart is tabulated below for reference

Severity level	Severity Particulars	Service window
Critical	Outage that impacts >=1 Services & Higher Management call	24*7
Medium	Outage that does not impact Services but affects department services	24*7
Low	Upgrade, shifting and preventive maintenance	7am to 7pm (Monday to Friday)

1.4. SLA Categories

The SLA has been classified into two broad categories as given under.

i. Category I: These are system delivery level targets which shall be adhered to during the implementation of the system, these services may be considered as pre-requisites to the service level targets mentioned in the post implementation phase.

ii. Category II: These are business critical level targets which shall be adhered to post implementation/commissioning of the system. Default on any of the service levels mentioned under this will incur penalties as defined in this section.

The Service level agreement would be valid for the complete period of contract. This SLA may be reviewed and revised according to the procedure detailed in SLA Change Control Mechanism.

1.4.1. Uptime calculation for the month

i. DGS would provide a maximum of 04 hours of planned downtime for the preventive maintenance (as part of scheduled downtime) per month per service.
ii. The downtime for scheduled maintenance (patch application, upgrades – OS, Database, etc.) would need to be mutually agreed between DGS and the Bidder. To reduce this time, various maintenance activities can be clubbed together with proper planning.

1.4.2. Cumulative Downtime

i. The recording of downtime shall commence at the time of registering the call with bidder for any downtime situation for the equipment.
ii. Downtime shall end when the problem is rectified, and the application/ service is available to the user.
iii. Down time will not be considered for following:
   - Pre-scheduled preventive maintenance and health checks (Scheduled Downtime).
   - Failover time (30 minutes) in case of cluster environment. Beyond which the service would be considered to be not available, and appropriate penalty shall be imposed on the SI.
   - If the DGS elects to continue the operation of the machine / equipment, when a part of the machine is giving problem and leading to downtime, the commencement of downtime shall be deferred until the DGS releases the machine / equipment to the Bidder for remedial action.

1.4.3. Exclusions

The bidder shall be exempted from any delays on SLA parameters arising from the delay in approvals, reviews, suggestions etc. from the DGS's side. Any such delays shall be notified in written by the DGS.

1.5. Non-Adherence to SLA

i. In case the bidder is unable to adhere to the target levels mentioned in the SLA and the percentage of penalty due to defaults exceeds 5 percent for four consecutive months, then the penalty would be doubled in the fourth month and subsequently till the same is rectified for two consecutive months.
ii. In case the bidder defaults in the same category for four consecutive months, then the penalty would be doubled in the fourth month and subsequently for that category till the same is rectified for two consecutive months.
iii. The breach clauses will be relaxed for the two quarters after go-live.

1.6. Breach of SLA

If the penalty continues for 6 consecutive months for the same category or over 10% across all categories, DGS may invoke breach and terminate the contract. The decision of DGS in this regard shall be final and binding on the bidder, the DGS will treat it as a case of breach of Service Level Agreement. The following steps will be taken in such a case: -

- *DGS issues a show cause notice to the SI.*
- *bidder should reply to the notice within three working days.*
- *If the DGS authorities are not satisfied with the reply, the DGS will initiate termination process.*

1.7. Monitoring and Auditing

DGS will review the performance of bidder against the SLA parameters each month, or at any periodicity defined in the contract document. The review / audit report will form basis of any action relating to imposing penalty or breach of contract. Any such review / audit can be scheduled or unscheduled. The results will be shared with the bidder as soon as possible. DGS reserves the right to appoint a third-party auditor to validate the SLA.

1.7.1. Reporting Mechanism

The bidder's representative will submit SLA performance reports from centrally managed web-based SLA monitoring tool in an agreed upon format by the 5th working day of subsequent month of the reporting period. The reports will include "actual versus target" SLA performance, a variance analysis and discussion of appropriate issues or significant events.

1.7.2. Issue Management Procedures

General

This process provides an appropriate management structure for the orderly consideration and resolution of business and operational issues in the event that quick consensus is not reached between DGS and bidder. It is expected that this pre-defined process will only be used on an exception basis if issues are not resolved at lower management levels.

Issue Management Process

i. Either DGS or Bidder may raise an issue by documenting the business or technical problem, which presents a reasonably objective summary of both points of view and identifies specific points of disagreement with possible solutions.
ii. DGS and the SI's representative will determine which committee, or executive level should logically be involved in resolution.
iii. A meeting or conference call will be conducted to resolve the issue in a timely manner. The documented issues will be distributed to the participants at least 24 hours prior to the discussion if the issue is not an emergency requiring immediate attention.
iv. The DGS and the Bidder shall develop an interim solution, if required, and subsequently the permanent solution for the problem at hand. The Bidder will then communicate the resolution to all interested parties.
v. In the event a significant business issue is still unresolved, the arbitration procedures described in the Contract will be used.

1.8. SLA Change Control

1.8.1. General

It is acknowledged that this SLA may change as DGS's s business needs evolve over the course of the contract period. As such, this document also defines the following management procedures:

i. A process for negotiating changes to the SLA.

ii. An issue management process for documenting and resolving particularly difficult issues.

iii. DGS and Bidder management escalation process to be used in the event that an issue is not being resolved in a timely manner.

iv. Any changes to the levels of service provided during the term of this agreement will be requested, documented and negotiated in good faith by both parties. Either party can request a change. Changes will be documented as an addendum to this document and consequently the contract.

1.8.2. SLA Change Process

Both the parties may amend this SLA by mutual agreement in accordance. Changes can be proposed by either party. Normally the forum for negotiating SLA changes will be DGS's monthly review meetings.

1.8.3. Version Control

All negotiated SLA changes will require changing the version control number. As appropriate, minor changes may be accumulated for periodic release (e.g. every quarter) or for release when a critical threshold of change has occurred.

1.9. Management Escalation Procedures

The purpose of this escalation process is to provide a quick and orderly method of notifying both parties that an issue is not being successfully resolved at the lowest possible management level. Implementing this procedure ensures that DGS and Bidder management are communicating at the appropriate levels. Escalation should take place on an exception basis and only if successful issue resolution cannot be achieved in a reasonable time frame.

- All issues would be raised to the project management team, which is completely responsible for the day-to-day aspects of the implementation. The project management team shall classify the issues based on their severity level and resolve them within appropriate timelines.
- If project management team is unable to resolve an issue, the issue would be escalated to the top management with options/ risks detailed for decision. Top management will make decisions based on the options/ risks presented.
- In case one or both the parties are unsatisfied with the decision of the top management of the DGS, the dispute will be resolved as specified in this RFP

1.10. Updating of this Agreement

a) The Parties anticipate that this Agreement shall need to be re-evaluated and modified to account for changes in work environment and technology from time to time. Hence, they herby agree to revise the terms of the Agreement on an annual basis.

b) The Parties hereby agree upon the following procedure for revising this Agreement:

i. Any and all changes to this Agreement will be initiated in writing between the Buyer and the Implementation Agency, the service levels in this Agreement shall be considered to be standard for the Buyer and shall only be modified if both Parties agree to an appended set of terms and conditions.

ii. Only the Buyer or the Bidder may initiate a revision to this Agreement.

iii. A notice of the proposed revision (“SLA Change Request”) shall be served to the Buyer or the Bidder as the case may be.

iv. The SLA Change request would be deemed to be denied in case it is not approved within a period of 45 days.

v. In the event that Buyer/Bidder approves of the suggested change the change shall be communicated to all the Parties and the SLA

vi. Change request would be appended to the Agreement.

The Buyer shall update and republish the text of Agreement annually to include all the SLA Change Requests that have been appended to the Agreement during the course of the year. Such republished Agreement shall be circulated to all the Parties within <***> days of such change taking place

1.11. Document History

All revisions made to this Agreement shall be listed in chronological order as per the format set out below and a copy of the same shall be provided to the Parties:

Version	Date	Description of Changes
<***>	<***>	<***>

1.12. Scope of Services

a) Bidder shall ensure that Services are available as per the requirements of the project;

b) Bidder shall provide support services for addressing problems related to the provision of services through the POC. Such POC shall be available over telephone on <***> number / email 24 hours a day, 7 days a week

c) Bidder guarantees that he shall achieve the Service Levels for the Project;

d) Bidder shall be liable to Service Credits in case of failure to comply with the Service Levels. However, any delay not attributable to the Implementation Agency shall not be taken into account while computing adherence to the Service Levels.

1.13. Performance Review

The POC’s of both the Buyer and the Implementation Agency shall meet on a quarterly basis to discuss priorities, service levels and system performance. Additional meetings may be held at the request of either the Bidder or the Buyer. The agenda for these meetings shall be as follows:

a) Service performance.

b) Review of specific problems/exceptions and priorities; and

c) Review of the operation of this Agreement and determine corrective action to overcome deficiencies.

1.14. Indemnities

The Parties agree to indemnify each other under this Agreement in accordance with the terms and principles set out in the MSA.

1.15. Dispute Resolution

Any dispute, difference or claim arising out of or in connection with the Agreement which is not resolved amicably shall be decided in accordance with the dispute resolution procedure as set out in the MSA.

1.16. Miscellaneous

a) Assignment and Charges

This Agreement shall be binding on and ensure for the benefit of each Party's successors in title. No Party shall assign or declare any trust in favor of a third party over, all or any part of the benefit of, or its rights or benefits under, this Agreement.

b) Governing Law and jurisdiction

This Agreement shall be construed and interpreted in accordance with and governed by the laws of India, and the courts at the State of Maharashtra shall have jurisdiction over matters arising out of or relating to this Agreement.

c) Waiver of sovereign immunity

The Parties unconditionally and irrevocably:

i. agree that the execution, delivery and performance by them of the Agreement constitute commercial acts done and performed for commercial purpose.

ii. agree that, should any proceedings be brought against a Party or its assets, property or revenues in any jurisdiction in relation to the Agreement or any transaction contemplated by the Agreement, no immunity (whether by reason of sovereignty or otherwise) from such proceedings shall be claimed by or on behalf of such Party with respect to its assets.

iii. waive any right of immunity which it or its assets, property or revenues now has, may acquire in the future or which may be attributed to it in any jurisdiction; and

iv. consent generally to the enforcement of any judgment or award against it in any such proceedings to the giving of any relief or the issue of any process in any jurisdiction in connection with such proceedings (including the making, enforcement or execution against it or in respect of any assets, property or revenues whatsoever irrespective of their use or intended use of any order or judgment that may be made or given in connection therewith).

d) Variation

This Agreement may only be varied in writing and signed by both Parties

e) Waiver

Waiver including partial or conditional waiver, by either Party of any default by the other Party in the observance and performance of any provision of or obligations under this Agreement: -

i. Shall be in writing

ii. Shall not operate or be construed as a waiver of any other or subsequent default hereof or of other provisions of or obligations under this Agreement.

iii. Shall not be effective unless it is in writing and executed by a duly authorized representative of the Party; and

iv. Shall not affect the validity or enforceability of this Agreement in any manner.

f) Exclusion of implied warranties

This Agreement expressly excludes any warranty, condition or other undertaking implied at law or by custom or otherwise arising out of any other agreement between the Parties or any representation by either Party not contained in a binding legal agreement executed by both Parties.

g) Survival

- Termination or expiration of the Term shall:

  i. not relieve the Bidder or the Buyer, as the case may be, of any obligations hereunder which expressly or by implication survive hereof; and

  ii. except as otherwise provided in any provision of this Agreement expressly limiting the liability of either Party, not relieve either Party of any obligations or liabilities for loss or damage to the other Party arising out of, or caused by, acts or omissions of such Party prior to the effectiveness of such termination or expiration or arising out of such termination or expiration.

- All obligations surviving termination or expiration of the Term shall cease on termination or expiration of the Term.

h) Entire Agreement

This Agreement and the Annexure together constitute a complete and exclusive statement of the terms of the agreement between the Parties on the subject hereof, and no amendment or modification hereto shall be valid and effective unless such modification or amendment is agreed to in writing by the Parties and duly executed by persons especially empowered in this behalf by the respective Parties. All prior written or oral understandings offers or other communications of every kind pertaining to this Agreement are abrogated and withdrawn.

IN WITNESS WHEREOF THE PARTIES HAVE EXECUTED AND DELIVERED THIS AGREEMENT AS OF THE DATE FIRST ABOVE WRITTEN.

SIGNED, SEALED AND DELIVERED
For and on behalf of the Implementation
Agency by DGS

(Signature)

(Name): Shri.
(Designation):

(Address)

(Fax No.)

SIGNED, SEALED AND DELIVERED
For and on behalf of the Nodal
Agency by:

(Signature)

(Name)
(Designation)

(Address)
(Fax No.)

In the presence of:
1.
2.

Section 8 – General Conditions of Contract (GCC)

1. General Provisions	
1.1 Definitions	Unless the context otherwise requires, the following terms whenever used in this Contract have the following meanings: a) "Completion Date" means the date of completion of the Services by the Bidder as certified by the Client; b) "Contract" means the Contract signed by the Parties, to which these General Conditions of Contract (GCC) are attached, together with all the documents listed in Clause 1 of such signed Contract, **as named in SCC**; c) "Contract Price" means the financial proposal of the successful Bidder duly accepted by the client; d) "Client" means the agency, **as named in SCC**, that signs the Contract for the Services with the Selected Bidder; e) "Bidder" means a legally-established professional consulting firm or entity selected by the Client to provide the Services under the signed Contract **as specified in SCC**; f) "Day" means a working day unless indicated otherwise. g) "Experts" means, collectively, Key Experts, Non-Key Experts, or any other Experts of the Bidder, Sub-Bidder or JV member(s) assigned by the Bidder to perform the Services or any part thereof under the Contract; h) "GCC" means these General Conditions of Contract; i) "Party" means the Client or the Bidder, as the case may be, and "Parties" means both of them; j) "Bidder's Proposal" means the completed Request for Proposals submitted by the Bidder to the Client; k) "SCC" means the Special Conditions of Contract by which the GCC may be amended or supplemented; l) "Services" means the work to be performed by the Bidder pursuant to this Contract, as described in **Appendix A** – Terms of Reference; m) "Third Party" means any person or entity other than the Government, the Client, the Bidder or a Sub-Bidder.
1.2 Applicable Law	The Contract shall be interpreted in accordance with the laws of the Union of India.
1.3 Language	This Contract has been executed in the English language, which shall be the binding and controlling language for all matters relating to the meaning or interpretation of this Contract.
1.4 Notices	Any notice given by one party to the other pursuant to the Contract shall be in writing to the address **specified in the SCC**. The term "in writing" means communicated in written form with proof of receipt. A notice shall be effective from the

	date of delivery or on the notice's effective date, whichever is later. In case of electronic mode of communication, a notice shall be effective from the time of sending of the electronic communication.
1.5 Location	The Services shall be performed at such locations as are specified in **Appendix A** hereto
1.6 Authorized Representatives	Any action required or permitted to be taken, and any document required or permitted to be executed, under this Contract by the Client or the Bidder may be taken or executed by the officials **specified in the SCC**.
1.7 Authority of Member in Charge	In case the Bidder is a Joint Venture, the members hereby authorize the member **specified in the SCC** to act on their behalf in exercising all the Bidder's rights and obligations towards the Client under this Contract, including without limitation the receiving of instructions and payments from the Client.
1.8 Taxes and Duties	The Bidder and their Experts shall pay such taxes, duties, fees, and other impositions as may be levied under the Applicable Law, the amount of which is deemed to have been included in the Contract Price.
1.9 Code of Integrity	a) The Client, the Bidder and their representatives shall strictly adhere to the code of integrity as stipulated under GFR 175. b) The Client requires the Bidder to disclose any commissions, gratuities or fees that may have been paid or are to be paid to agents or any other party with respect to the selection process or execution of the Contract. The information disclosed must include at least the name and address of the agent or other party, the amount and currency, and the purpose of the commission, gratuity or fee. Failure to disclose such commissions, gratuities or fees may result in termination of the Contract
2. Commencement, Completion, Modification, and Termination of Contract	
2.1 Effectiveness of Contract	This Contract shall come into effect on the date the Contract is signed by both parties or such other later date as may be **stated in the SCC**.
2.2 Commencement of Services	
2.2.1 Program	Before commencement of the Services, the Bidder shall submit to the Client for approval a Program showing the general methods, arrangements, order and timing for all activities. The Services shall be carried out in accordance with the approved Program as updated.
2.2.2 Starting Date	The Bidder shall start carrying out the Services thirty (30) days after the date the Contract becomes effective, or at

	such other date as may be **specified in the SCC**.
2.3 Intended Completion Date	Unless terminated earlier pursuant to Sub-Clause 2.6, the Bidder shall complete the activities by the Intended Completion Date, as is **specified in the SCC**. If the Bidder does not complete the activities by the Intended Completion Date, it shall be liable to pay liquidated damage as per Sub-Clause 3.8. In this case, the Completion Date will be the date of completion of all activities.
2.4 Modification	Modification of the terms and conditions of this Contract, including any modification of the scope of the Services or of the Contract Price, may only be made by written agreement between the Parties. However, each Party shall give due consideration to any proposals for modification or variation made by the other Party.
2.4.1 Change Request	Any requirement for Change Requests (CRs) shall be formally communicated in writing by the Competent Authority of the Directorate General of Shipping (DGS) to the selected Bidder / Lead Bidder, in case of a consortium. Upon receipt of a formal CR from DGS, the Bidder / Lead Bidder shall, within a reasonable time as specified by DGS, submit the following to DGS for review and approval: a. Technical feasibility of implementing the Change Request; b. Effort estimation required for the proposed changes; c. Financial implication/cost associated with the same; d. Proposed schedule and timeline for delivery and implementation. The response submitted by the Bidder / Lead Bidder shall be evaluated by DGS. Based on such evaluation, DGS may issue formal approval for incorporation of the CR in the project scope. Only upon receipt of such formal written approval from DGS, the Bidder / Lead Bidder shall proceed with the implementation of the approved Change Request and raise the corresponding invoice as per agreed terms. The cumulative value of such Change Requests shall not exceed twenty percent (20%) of the Contract Value, which shall be computed based on the bid value submitted by the Bidder and accepted by DGS or its nominated agency(ies), or as otherwise decided and approved by DGS or its nominated agency(ies).
2.5 Force Majeure	
2.5.1 Definition	For the purposes of this Contract, “Force Majeure” means an event which is beyond the reasonable control of a Party and which makes a Party’s performance of its obligations under

	the Contract impossible or so impractical as to be considered impossible under the circumstances.
2.5.2 No Breach of Contract	The failure of a Party to fulfill any of its obligations under the contract shall not be considered to be a breach of, or default under, this Contract insofar as such inability arises from an event of Force Majeure, provided that the Party affected by such an event (a) has taken all reasonable precautions, due care and reasonable alternative measures in order to carry out the terms and conditions of this Contract, and (b) has informed the other Party as soon as possible about the occurrence of such an event.
2.5.3 Extension of Time	Any period within which a Party shall, pursuant to this Contract, complete any action or task, shall be extended for a period equal to the time during which such Party was unable to perform such action as a result of Force Majeure.
2.6 Termination	
2.6.1 By the Client	The Client may terminate this Contract, by not less than thirty (30) days' written notice of termination to the Bidder, to be given after the occurrence of any of the events specified in paragraphs (a) through (d) of this Sub-Clause 2.6.1: a. if the Bidder does not remedy a failure in the performance of its obligations under the Contract, within thirty (30) days after being notified or within any further period as the Client may have subsequently approved in writing; b. if the Bidder become insolvent or bankrupt; c. if, as the result of Force Majeure, the Bidder is unable to perform a material portion of the Services for a period of not less than sixty (60) days; or d. if the Bidder, in the judgment of the Client has engaged in corrupt, fraudulent, collusive, coercive or obstructive practices, in competing for or in executing the Contract.
2.6.2 By the Bidder	The Bidder may terminate this Contract, by not less than thirty (30) days' written notice to the Client, such notice to be given after the occurrence of any of the events specified in paragraphs (a) and (b) of this Sub-Clause 2.6.2: a. if the Client fails to pay any monies due to the Bidder pursuant to this Contract and not subject to dispute pursuant to Clause 7 within forty-five (45) days after receiving written notice from the Bidder that such payment is overdue; or b. (b) if, as the result of Force Majeure, the Bidder is unable to perform a material portion of the Services for a period of not less than sixty (60) days.
3. Obligations of the Bidder	
3.1 General	The Bidder shall perform the Services in accordance with the Specifications and the Terms of Reference, and carry out its obligations with all due diligence, efficiency, and economy, in accordance with generally accepted professional techniques and practices, and shall observe sound management practices, and employ appropriate advanced technology and safe methods. The Bidder shall always act,

	in respect of any matter relating to this Contract or to the Services, as faithful adviser to the Client, and shall at all times support and safeguard the Client's legitimate interests in any dealings with Sub-Bidders or third parties.
3.2 Conflict of Interests	3.2.1 The Bidder shall hold the Client's interest paramount, without any consideration for future work, and strictly avoid conflict with other assignments or their own corporate interests. 3.2.2 The Bidder agrees that, during the term of this Contract and after its termination, the Bidder and any entity affiliated with the Bidder shall be disqualified from providing goods, works or non-consulting services resulting from or directly related to the Services for the preparation or implementation of the project, unless otherwise **indicated in the SCC**. 3.2.3 The payment of the Bidder pursuant to GCC shall constitute the Bidder's only payment in connection with this Contract and the Bidder shall not accept for its own benefit any trade commission, discount or similar payment in connection with activities pursuant to this Contract or in the discharge of its obligations hereunder, and the Bidder shall use its best efforts to ensure that any Sub-Bidders, as well as the Experts and agents of either of them, similarly shall not receive any such additional payment. 3.2.4 Furthermore, if the Bidder, as part of the Services, has the responsibility of advising the Client on the procurement of goods, works or services, the Bidder shall comply with the applicable rules and guidelines of the Government of India, and shall at all times exercise such responsibility in the best interest of the Client. Any discounts or commissions obtained by the Bidder in the exercise of such procurement responsibility shall be for the account of the Client. 3.2.5 The Bidder shall not engage, and shall cause its Experts as well as its Sub-Bidders not to engage, either directly or indirectly, in any business or professional activities that would conflict with the activities assigned to them under this Contract. 3.2.6 The Bidder has an obligation and shall ensure that its Experts and Sub-Bidders shall have an obligation to disclose any situation of actual or potential conflict that impacts their capacity to serve the best interest of their Client, or that may reasonably be perceived as having this effect. Failure to disclose said situations may lead to the disqualification of the Bidder or the termination of its Contract.
3.3 Confidentiality	Except with the prior written consent of the Client, the Bidder and the Experts shall not at any time communicate to any person or entity any confidential information acquired in the course of the Services, nor shall the Bidder and the Experts make public the recommendations formulated in the course of, or as a result of, the Services.

	In the event that the Firm or its representatives are requested pursuant to, or required by, applicable law or regulation or by legal or administrative process to disclose any Confidential Information, or where the Firm wishes to disclose to its professional indemnity insurers or to its advisers, the Firm agrees that it will, as far as is legally and practically possible, provide the Client with prompt notice of such request or requirement in order to enable the Client to seek an appropriate protective order or other remedy. In the event that such protective order or other remedy is not obtained, the Firm or its representatives, as the case may be, shall disclose only the portion of the Confidential Information which is legally or professionally required to be disclosed.
3.4 Insurance to be Taken Out by the Bidder	The Bidder (a) shall take out and maintain, and shall cause any Sub-Bidders to take out and maintain, at its (or the Sub-Bidders', as the case may be) own cost but on terms and conditions approved by the Client, insurance against the risks, and for the coverage, as shall be **specified in the SCC**; and (b) at the Client's request, shall provide evidence to the Client showing that such insurance has been taken out and maintained and that the current premiums have been paid. The Bidder shall ensure that such insurance is in place prior to commencing the Services.
3.5 Bidder's Actions Requiring Client's Prior Approval	The Bidder shall obtain the Client's prior approval in writing before taking any of the following actions: a. entering into a subcontract for the performance of any part of the Services, b. changing the Program of activities; and c. any other action that may be **specified in the SCC**.
3.6 Reporting Obligations	The Bidder shall submit to the Client the reports and documents specified in **Appendix A**, in the form, in the numbers and within the time periods set forth in the said Appendix**.**
3.7 Documents Prepared by the Bidder to Be the Property of the Client	3.7.1 All plans, drawings, specifications, designs, reports, and other documents and software submitted by the Bidder in accordance with Sub- Clause 3.6 shall become and remain the property of the Client, and the Bidder shall, not later than upon termination or expiration of this Contract, deliver all such documents and software to the Client, together with a detailed inventory thereof. The Bidder may retain a copy of such documents and software. Restrictions about the future use of these documents, if any, shall be **specified in the SCC**. 3.7.2 If license agreements are necessary or appropriate between the Bidder and third parties for purposes of development of the plans, drawings, specifications, designs, databases, other documents and software, the Bidder shall obtain the Client's prior written approval to such agreements, and the Client shall be entitled at its discretion to require recovering the expenses related to the development of the

	program(s) concerned.
4. Bidder's Experts	
4.1 Description of Key Experts	The titles, agreed job descriptions, minimum qualifications, and estimated periods of engagement in the carrying out of the Services of the Bidder's Key Experts are described in Appendix B. The Key Experts listed by title as well as by name in Appendix B are hereby approved by the Client.
4.2 Removal and/or Replacement of Experts	4.2.1 Except as the Client may otherwise agree, no changes shall be made in the Key Experts. If, for any reason beyond the reasonable control of the Bidder, it becomes necessary to replace any of the Key Experts, the Bidder shall provide as a replacement a person of equivalent or better qualifications. 4.2.2 If the Client finds that any of the Experts have (i) committed serious misconduct or have been charged with having committed a criminal action, or (ii) have reasonable cause to be dissatisfied with the performance of any of the Experts, then the Bidder shall, at the Client's written request specifying the grounds thereof, provide as a replacement a person with qualifications and experience acceptable to the Client. 4.2.3 In the event that any of Key Experts, Non-Key Experts or Sub-Bidders is found by the Client to be incompetent or incapable in discharging assigned duties, the Client, specifying the grounds therefore, may request the Bidder to provide a replacement. 4.2.4 The Bidder shall have no claim for additional costs arising out of or incidental to any removal and/or replacement of Experts. 4.2.5 Notwithstanding the above, the substitution of Key Experts during Contract execution may be considered only based on the Bidder's written request and due to circumstances outside the reasonable control of the Bidder, including but not limited to death or medical incapacity. In such case, the Bidder shall forthwith provide as a replacement, a person of equivalent or better qualifications and experience, and at the same rate of remuneration.
5. Obligations of the Client	
5.1 Assistance and Exemptions	The Client warrants that the Bidder shall have, free of charge, unimpeded access to the project site in respect of which access is required for the performance of the Services. The Client shall use its best efforts to provide the Bidder such assistance and exemptions as **specified in the SCC**.
5.2 Services, Facilities and Property of the Client	The Client shall make available to the Bidder and the Experts, for the purposes of the Services and free of any charge, the services, facilities and property described in the

	Terms of Reference (**Appendix A**) at the times and in the manner specified in said Appendix A.
5.3 Counterpart Personnel	5.3.1 The Client shall make available to the Bidder free of charge such professional and support counterpart personnel, to be nominated by the Client with the Bidder's advice, if specified in **Appendix A**. 5.3.2 Professional and support counterpart personnel, excluding Client's liaison personnel, shall work under the exclusive direction of the Bidder. If any member of the counterpart personnel fails to perform adequately any work assigned to such member by the Bidder that is consistent with the position occupied by such member, the Bidder may request the replacement of such member, and the Client shall not unreasonably refuse to act upon such request.
5.4 Payment Obligation	In consideration of the Services performed by the Bidder under this Contract, the Client shall make such payments to the Bidder for the deliverables specified in **Appendix A** and in such manner as is provided by GCC 6 below.
5.5 Change in the Applicable Law	If, after the date of this Contract, there is any change in the Applicable Law with respect to taxes and duties which increases or decreases the cost of the Services rendered by the Service Provider, then the remuneration and reimbursable expenses otherwise payable to the Bidder under this Contract shall be increased or decreased accordingly by agreement between the Parties, and corresponding adjustments shall be made to the amounts referred to in Sub-Clause 6.1.
6. Payments	
6.1 Contract Price	6.1.1 The Bidder's Contract Price shall be a fixed lump-sum net of all costs incurred by the Bidder in carrying out the Services described in Appendix A. The Contract Price is **set forth in the SCC**. The Contract price breakdown is provided in Appendix C. 6.1.2 Any change to the Contract price specified in Clause 6.1.1 can be made only if the Parties have agreed to the revised scope of Services pursuant to Clause GCC 2.4 and have amended in writing the Terms of Reference in **Appendix A**.
6.2 Taxes and Duties	6.2.1 The Bidder, Sub-Bidders and Experts are responsible for meeting any and all tax liabilities arising out of the Contract. 6.2.2 As an exception to the above and **as stated in the SCC**, the GST is reimbursed to the Bidder.
6.3 Mode of Billing and Payment	6.3.1 The total payments under this Contract shall not exceed the Contract price set forth in Clause GCC 6.1.1.

	6.3.2 The payments under this Contract shall be made in lump-sum installments against deliverables specified in **Appendix A**. The payments will be made according to the payment schedule **stated in the SCC**. 6.3.3 The Client shall pay the Bidder within forty-five (45) days after the receipt by the Client of the deliverable(s) and the cover invoice for the related lump-sum installment payment. The payment can be withheld if the Client does not approve the submitted deliverable(s) as satisfactory in which case the Client shall provide comments to the Bidder within the same forty-five (45) days period. The Bidder shall thereupon promptly make any necessary corrections, and thereafter the foregoing process shall be repeated. 6.3.4 The final payment under this Clause shall be made only after the final report I have been submitted by the Bidder and approved as satisfactory by the Client. The Services shall then be deemed completed and finally accepted by the Client. The last lump-sum installment shall be deemed approved for payment by the Client within sixty (60) calendar days after receipt of the final report by the Client unless the Client, within such sixty (60) calendar day period, gives written notice to the Bidder specifying in detail deficiencies in the Services, the final report. The Bidder shall thereupon promptly make any necessary corrections, and thereafter the foregoing process shall be repeated. 6.3.5 All payments under this Contract shall be made to the accounts of the Bidder **specified in the SCC**.
6.4 Interest on Delayed Payments	If the Client had delayed payments beyond fifteen (15) days after the due date stated in Clause GCC 6.3.3, interest shall be paid to the Bidder on any amount due by, not paid on, such due date for each day of delay at the annual rate **stated in the SCC**.
7. Settlement of Disputes	
7.1 Amicable Settlement	The Parties shall use their best efforts to settle amicably all disputes arising out of or in connection with this Contract or its interpretation.
7.2 Dispute Settlement	Any dispute between the Parties arising under or related to this Contract that cannot be settled amicably may be referred to by either Party to the adjudication / arbitration in accordance with the provisions **specified in the SCC**.
8. Good Faith	
	The Parties undertake to act in good faith with respect to each other's rights under this Contract and to adopt all reasonable measures to ensure the realization of the objectives of this Contract.

9. **Limitation of Liability**	
	The total aggregate liability of the Bidder, whether in contract, tort (including negligence) or otherwise, under or in connection with this agreement, shall in no circumstances exceed a sum equal to 110% of the contract value.
10. **Indemnity**	
	The Bidder shall at all times indemnify and keep indemnified the Client against all claims/damages for any infringement of any Intellectual Property Rights (IPR) while providing its services under the Contract. The Bidder shall indemnify the Client in full for any failure in performance on account of its default or non-fulfilment of its obligations and the same is performed by the client or any other agency engaged by the client. In such case all the costs and expenses incurred by the client are recoverable from the Bidder. The Client shall also indemnify the Bidder for losses/damages suffered due to any fraud, misrepresentation or omission of facts by the Client or any of its personnel.

Section 9 – Special Conditions of Contract (SCC)

Number of GCC Clause	Amendments of, and Supplements to, Clauses in the General Conditions of Contract
1.1(b)	The contract name is Selection of System Integrator for development of Platform for the Indian Global Maritime Safety Platform (IGMSP) for Directorate General of Shipping Govt. of India.
1.1(d)	The Client is *Directorate General of Shipping, 9th Floor Beta Building,i-Think Techno Campus, Kanjurmarg (East), Mumbai - 400 042 (India)*
1.1(e)	The Bidder is _________________
1.4	**The addresses are**: Client: Directorate General of Shipping (DGS), Attention: Capt. Harinder Singh, Member Secretary, Casualty Branch, Deputy Director General, DGS Office E-mail: singh.harinder@gov.in Bidder: Attention: Facsimile: E-mail: _
1.6	**The Authorized Representatives are:** **For the Client:** _________________________________. **For the Bidder:** *[name, title]*_________________________________
1.7	**The authorized member in charge is** _____________________________
2.1	No change to the GCC clause
2.2.2	The Starting Date for the commencement of Services is seven (7) days after contract signing.

2.3	The Intended Completion Date is
3.2.2	The Client reserves the right to determine on a case-by-case basis whether the service should be disqualified from providing goods, works or non-consulting services due to a conflict of a nature described in Clause GCC 3.2.2
3.4	The risks and coverage by insurance shall be: (i) Third Party liability – as stipulated by relevant government law. (ii) Client's liability and workers' compensation – as stipulated in the employees' compensation act. (iii) Professional liability – at least 110% of the Contract Price.
3.5 c.	The Bidder shall follow the protocol stipulated in the Terms of Reference regarding entering-exiting Client's premises and for weighting and carrying the investment powder waste.
3.7	There are no specific restrictions.
5.1	The Client shall provide necessary assistance in providing gate-passes for smooth entry of the Bidder's vehicles and employees.
6.1	The Contract Price is: ________________
6.2.2	The amount of GST reimbursable to the Bidder is: ____________
6.3.2	The payment schedule shall be as stipulated under Appendix A – Terms of Reference.
6.3.5	Bidder's account details for payments under the Contract are: Account Name: Bank Name: Branch Name: IFSC Code:
6.4	The interest rate shall be 6% per annum.
7.2	Disputes shall be resolved by way of arbitration as stipulated under the Arbitration and Conciliation Act, 1996 as amended till date.

Appendix A – Terms of Reference

Refer to Section 5

Appendix B – Breakdown of Price

{*Bidder shall insert the Breakdown of Contract Price in the BoQ (Excell file) uploaded separately in the E- Procurement portal*}

Appendix C – CVs of the Key Experts

{*Bidder shall insert the Key Experts' CVs here*}

Section 10 – Contract Forms

Letter of Acceptance

{*On Client's Letterhead*}

Date:

To: {*Insert Name and Address of the Successful Bidder*}

Subject: Letter of acceptance of your Proposal against tender ref. no.:

This is to notify you that your Proposal dated [*insert date of Proposal submitted by the Bidder*] for the execution of services titled *"Selection of System Integrator for development of Platform for the Indian Global Maritime Safety Platform (IGMSP) for Directorate General of Shipping, Govt. of India."* against RFP Ref. No. [*insert Proposal Ref. No.*] is hereby accepted by the Client for the Contract Price of Rs. [*insert amount in numbers and words*], as evaluated in accordance with the Instructions to Bidders.

You are requested to execute the contract agreement within 28 days of receipt of this Letter. Till a contract agreement is executed, this Letter along with your accepted proposals shall constitute a valid and mutually binding contract.

Authorized Signature: ....

Name and Designation of Signatory: ....

Name of Client: ....

Form of Contract

This CONTRACT (hereinafter called the "Contract") is made the *[number]* day of the month of *[month]*, *[year]*, between, on the one hand, ***DGS, Mumbai*** (hereinafter called the "Client") and, on the other hand, *[name of Bidder]* (hereinafter called the "Bidder").

WHEREAS

(a) the Client has requested the Bidder to provide certain consulting services as defined in this Contract (hereinafter called the "Services");

(b) the Bidder, having represented to the Client that it has the required professional skills, expertise and technical resources, has agreed to provide the Services on the terms and conditions set forth in this Contract;

NOW THEREFORE the parties hereto hereby agree as follows:

1. The following documents attached hereto shall be deemed to form an integral part of this Contract:

   (a) The General Conditions of Contract;
   (b) The Special Conditions of Contract;
   (c) Appendices:
   Appendix A: Terms of Reference
   Appendix B: Key Experts
   Appendix C: Breakdown of Contract Price

   In the event of any inconsistency between the documents, the following order of precedence shall prevail: the Special Conditions of Contract; the General Conditions of Contract, including Attachment 1; Appendix A; Appendix B; Appendix C. Any reference to this Contract shall include, where the context permits, a reference to its Appendices.

2. The mutual rights and obligations of the Client and the Bidder shall be as set forth in the Contract, in particular:

   (a) the Bidder shall carry out the Services in accordance with the provisions of the Contract; and
   (b) the Client shall make payments to the Bidder in accordance with the provisions of the Contract.

IN WITNESS WHEREOF, the Parties hereto have caused this Contract to be signed in their respective names as of the day and year first above written.

For and on behalf of ***Directorate General of Shipping, Mumbai***

____

Shri Shyam Jagannathan, DGS

For and on behalf of *[Name of Bidder or Name of a Joint Venture]*

____

[Authorized Representative of the Bidder – name and signature]

Non-Disclosure Agreement

THIS AGREEMENT is made on this the <***> day of <***> 20--- at <***>, India.

BETWEEN

-- having its office at ------------------ -- India hereinafter referred to as '**DGS**' or '------------------', which expression shall, unless the context otherwise requires, include its permitted successors and assigns);

AND

<***>, a Company incorporated under the Companies Act, 1956, having its registered office at <***> (hereinafter referred to as '**the Bidder/MSP**' which expression shall, unless the context otherwise requires, include its permitted successors and assigns).

Each of the parties mentioned above are collectively referred to as the 'Parties' and individually as a 'Party'.

WHEREAS:

1. DGS/ is desirous to implement the project of -----------------------.
2. DGS/ and Bidder have entered into a Master Services Agreement dated <***> (the "MSA") as well as a Service Level Agreement dated <***> (the "SLA") in furtherance of the Project.
3. Whereas in pursuing the Project (the "**Business Purpose**"), a Party ("Disclosing Party) recognizes that they will disclose certain Confidential Information (as defined hereinafter) to the other Party ("Receiving Party").
4. Whereas such Confidential Information (as defined hereinafter) belongs to Receiving Party as the case may be and is being transferred to the Disclosing Party to be used only for the Business Purpose and hence there is a need to protect such information from unauthorized use and disclosure.

NOW THEREFORE, in consideration of the mutual covenants, promises, assurances, representations and provisions set forth herein, the Parties hereto agree as follows:

IN WITNESS WHEREOF THE PARTIES HAVE EXECUTED AND DELIVERED THIS AGREEMENT AS OF THE DATE FIRST ABOVE WRITTEN.

SIGNED, SEALED AND DELIVERED For and on behalf of the Implementation Agency by: DGS	SIGNED, SEALED AND DELIVERED For and on behalf of the Nodal Agency by:
(Signature)	(Signature)
(Name): Shri. (Designation):	(Name) (Designation)
(Address)	(Address)
(Fax No.)	(Fax No.)

In the presence of:

1.

Service Level Agreement

THIS AGREEMENT is made on this the <***> day of <***> 20---- at <***>, India.

BETWEEN
-- having its office at ------------------ --- India hereinafter referred to as '*DGS*' or '*Buyer*', which expression shall, unless the context otherwise requires, include its permitted successors and assigns);

AND

<***>, a Company incorporated under the *Companies Act, 1956*, having its registered office at <***> (hereinafter referred to as '*the Bidder/MSP'* which expression shall, unless the context otherwise requires, include its permitted successors and assigns).
Each of the parties mentioned above are collectively referred to as the '*Parties*' and individually as a '*Party*'.

WHEREAS:

1. DGS is desirous for Implementation and Operations Management of IT solution.
2. DGS and Bidder have entered into a Master Services Agreement dated <***> (the "*MSA*").

NOW THEREFORE, in consideration of the mutual covenants, promises, assurances, representations and provisions set forth herein, the Parties hereto agree as follows:
The following parties are obligated to follow the procedures as specified by this Agreement:
DGS
Bidder

IN WITNESS WHEREOF THE PARTIES HAVE EXECUTED AND DELIVERED THIS AGREEMENT AS OF THE DATE FIRST ABOVE WRITTEN

SIGNED, SEALED AND DELIVERED For and on behalf of the Bidder by:	SIGNED, SEALED AND DELIVERED For and on behalf of DGS by:
(Signature) (Name) XXX (Designation) XXXX (Address) XXXX (Fax No.)	(Signature) (Name) (Designation) (Address) (Fax No.)

In the presence of:
1.___________
2.___________

Please Enable Macros to View BoQ

information