Request for Proposal (eRFP) for

"Design, development, integration, implementation, operation and maintenance of

National Logistics Portal (Marine) *Ver1.0*

Volume 2

Date: 28/09/2020

Bid Reference: IPA/PGAV/NLP-Marine/2020

Indian Ports Association

1st Floor, South Tower, N.B.C.C. Place, Bhisham Pitamah Marg,
Lodi Road, New Delhi - 110003
Telephone: 24369061, 24369063, Fax: 011-24365866, Email: tender.ipa@nic.in

Acronyms

API	Application Program Interface
B2B	Business to Business
BRS	Business Requirements Specification
CFS	Container FreightStation
CHA	Custom House Agent
CIN	Corporate Identity Number
CONCOR	Container Corporation of India Ltd.
CRIS	Centre for Railway Information Systems
CSP	Cloud Service Provider
CSV	Comma Separated Values
DC/DR	Data Centre and Disaster Recovery
DDoS	Distributed Denial of Service
DGFT	Directorate General of Foreign Trade
DMS	Document Management System
DMZ	De-Militarized one
DSC	Digital Signature Certificate
ECD	Empty Container Depot
EGM	Export General Manifest
EPC	Export Promotion Council
ERP	Enterprise Resource Planning
EXIM	Export Import
FF	Freight Forwarded
FOIS	Freight Operations Information System
FRS	Functional Requirement Specification
FTP	File Transfer Protocol
GIGW	Guidelines for Indian Government Websites
GOI	Government of India
GSTN	Goods and Services Tax Network
HSN	Harmonized System Nomenclature
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
ICD	Inland Container Depot
ICEGATE	Indian Customs Electronic Data Interchange (EDI) Gateway

ICES	Indian Customs Electronic Data Interchange System
IDE	Integrated Development Environment
IEC	Import Export Code
J2EE	Java Platform, Enterprise Edition
KPI	Key Performance Indicator
LDAP	Lightweight Directory Access Protocol
LEO	Let Export Order
LSP	Logistic Service Provider
MHUB	Message Hub
MIS	Management Information System
MOCI	Ministry of Commerce, India
MOM	Message Oriented Middleware
MPLS	Multiprotocol Label Switching
NLP	National Logistics Portal
NOC	No Objection Certificate
OEM	Original Equipment Manufacturer
OTP	One Time Password
PAN	Permanent Account Number
PCS	Port Community System
PGA	Partner Government Agency
PMU	Project Management Unit
REST	Representational State Transfer
RTM	Requirements Tracability Matrix
SALT	Service Architecture Leveraging Tuxedo
MSP	Managed Service Provider
SLA	Service Level Agreement
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
SRS	Software Requirements Specification
SSL	Secure Socket Layer
SSO	Single Sign-On
SWIFT	Single Window Interface for Facilitating Trade
UAT	User Acceptance Testing
UI/UX	User Interface/User Experience
UIDAI	Unique Identification Authority of India
UN/EDIFACT	United Nations/Electronic Data Interchange for

	Administration, Commerce and Transport
USB	Universal Serial Bus
VAS	Value Added Service
VPN	Virtual Private Network
WSDL	Web Service Definition Language
WSS	Web Services Security
XML	Extensible Markup Language
XSLT	Extensible Stylesheet Language Transformations

1. About The Project

1.1 Background

India is one of the rapidly growing economies in the world. The country's marine sector is intricately linked with its economic activity and trade and has been a significant contributor to its competitive position in global trade. 95% of the merchandise trade (by volume) is transported through maritime transport. Indian Ports Association (IPA), an apex body of Major Ports in India, was constituted in 1966 under Societies Registration Act, primarily with the idea of fostering growth and development of all Major Ports which are under the supervisory control of Ministry of Shipping. Over the years, IPA has consolidated its activities and is now considered to be a think tank for the Major Ports with the goal of integrating all the stakeholders of the maritime sector. The functioning body of IPA comprises of Chairmen of all Major Ports and the Secretariat of IPA is headed by the Managing Director who operates from New Delhi. IPA has its Registered Office at 1st Floor, South Tower, NBCC Place, Bisham Pitamah Marg, Lodi Road New Delhi – 11 003 More information about the activities of the IPA can be seen at IPA websitehttp://ipa.nic.in.

During 2006, IPA, at the instance of Ministry of Shipping, on behalf of all the Major Ports in India, established a Centralized Web Based-Port Community System (PCS ver 1.0) intended to integrate the electronic flow of information among the Indian maritime trade community.

In 2018, to augment the existing PCS 1.0, IPA in accordance to the Ministry of Shipping framed a new solution PCS 1x with a vision of:

- Cloud migration for PCS 1.0 and Implementation
- Application support for maintenance and implementation
- Event based Notifications and Alerts at triggers points on key transactions.
- New Development of Value Adds to PCS 1.0 modules
- Development of Mobile Application.
- Frame design that eases use of value-add system (user experience; user interface).
- Set up a central 24/7 helpdesk with locational support

A brief overview of the PCS 1x, its components, scope of coverage, list of current stakeholders, its usage etc. is available at https://indianpcs.gov.in.

Following are some of the benefits of PCS 1x

- Cloud Solution-Allows Access from Anywhere, Anytime
- Tool for collaboration between Internal and external stakeholders
- e-Collection with multiple payment options
- Mobile Approach
- Integration of systems on a Single Platform
- Real Time Status Updates
- Enhanced Customer Delight

1.2 Objectivesof PCS 1x

Centralized Port Community System 'PCS 1x' is an initiative by Indian Ports Association (IPA) intended to provide a single window system for the Port communities in India to securely exchange the documents and information electronically with their stakeholders involved in the maritime transport and logistics chain including the trading partners and government agencies.

The objectives of developing PCS 1x:

- Improve quality and ease of doing business
- Scalable
- Multi-channel service delivery in real time

- Cloud based (24 x7 availability)
- Move towards paperless regime
- Improve efficiency
- Provide status information and control
- Step towards GOI initiative of Digital India, Ease of doing Business & Make in India

1.3 Current Status of PCS 1x

PCS 1x is implemented at all 13 major port and multiple private non major ports / terminals and other stakeholders.

The stakeholders (Category) in the current PCS 1x system are 27.

The list of stakeholders is as follows:

- Port Authorities
- Shipping Agent
- Terminal Operator
- Customs House Agent (CHA), Importer, Exporter
- Container Freight Station (CFS), Inland Container Depot (ICD)
- Customs
- Rail Transport Operator
- Road Transport Operator
- Banks
- Stevedore
- Surveyor
- Port Health Organisation (PHO)
- Plant Quarantine Organisation (PQO)
- Mercantile Marine Department (MMD)
- Immigration
- Tank Farm Operator
- Container Agent
- Barge Owner Operator
- Navy; Coast Guard
- Inland Waterways
- Stakeholders involved in Coastal movement
- Empty Yard
- Freight Forwarders
- Ship Chandler
- NVOCC
- DGLL
- Bunker Supplier

The IT infrastructure required for running the PCS ver 1.x is cloud based augmented with the API Portal, Data Center in Navi Mumbai and DR site is located at Chennai. Help Desk Services (24x7) for PCS is operational from 2018 onwards.

Some of the major functionalities implemented/ under implementation as part of PCS 1.x are:

- 98 EDI messages exchange in XML, Proprietary and UNEDIFACT formats as per the PCS defined formats. (**Annexure III**List of Messages)
- API Gateway enabling the various stakeholder to integrate with PCS1x using API services

API Integration with the ICEGATE, Major Ports, ICD CFSs, and Shipping Lineshas provided following benefits

- Seamless integration with the various service providers providing services like eDO, eVGM etc.
- Refer to PCS Documents section on Indian PCS Web Portal(http://www.ipa.nic.in//)

- Exchange of EDI messages using multiple protocols (SFTP, API, HTTPS)
- Seamless conversion of messages from one format to another
- Intelligent routing of messages to multiple stakeholders as per defined recipient list
- E-Payment of Port Services and integration of bank related messages. Currently PCS integrates with 11 banks directly and 4 payment gateways.
- Web services integration
- Administrative services
- Alerts to the stakeholders using SMS & emails
- Dashboard with important KPIs for port officers and Ministry
- Dashboard &Activity tracker facility for the users.
- PCS is capable of delivering the invoices for port related services, as a value addition e-invoicing for e-DO is under development
- Encryption services for e Invoices for the respective stakeholders
- Entire cycle of eInvoice -ePayment- eDelivery Order

During the present year, 2019-20, more than 18 million messages are exchanged through the PCS ver.1.x system.

1.4 Review of PCS 1x

PCS1x connected to major stakeholders which are required for the EXIM trade and the framework for exchanging messages, standardization of business/ message directories, central repository of knowledge and secure processes for facilitating payments have been established has achieved it's intended objectives.

PCS1x provides for the electronic exchange of information between all port and logistics sectors and is acknowledged as most advanced method for the exchange of information. PCS1x will reduce the duplication of data input through efficient electronic exchange of information. PCS1x has the ability to act as a National Logistics Portal as per Government directives. As Stage I, PCS 1x will be bootstrapped for enhancement and implementation of Nation Logistics Portal – Marine as per directives

PCS1x's ability to integrate seamlessly with various other systems makes it possible to become as National Logistics Portal Marine

IPA has decided to appoint a partner that can:

- Development and Commissioning of National Logistics Portal – Marine
- Operation and Maintenance of National Logistics Portal – Marine
- Continue API integration onboarding efforts,
- On Development and Implementation of National Logistics Portal – Marine, to support and Maintain the same
- The Period for Development and Implementation of National Logistics Portal – Marine will be one year from signing of the contract
- The support and Maintenance will be for four years thereafter
- Therefore, the Project is for five years from signing of contract

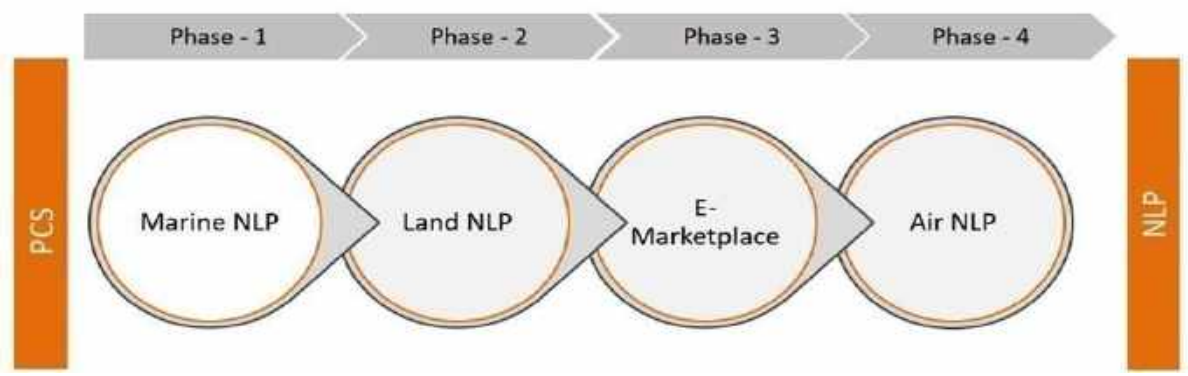
1.5 Information Details of PCS 1x

S.No.	Parameter	Data
1	Number and List of Stakeholders part of PCS 1x	Refer **Annexure VII**
2	Latch on services in PCS 1x	

3	Total users count under each Stakeholder	
4	API Integration with existing stakeholder application	
5	Information on Data exchange with various each user (Different Formats such as XML, PDF, EDI Messages etc.)	
6	Existing system details ▪ Solution Architecture ▪ DC/DR Infra Configuration ▪ Information Security ▪ Existing modules ▪ Latch on services	Refer **Annexure VI**

1.6 Journey of PCS towards NLP

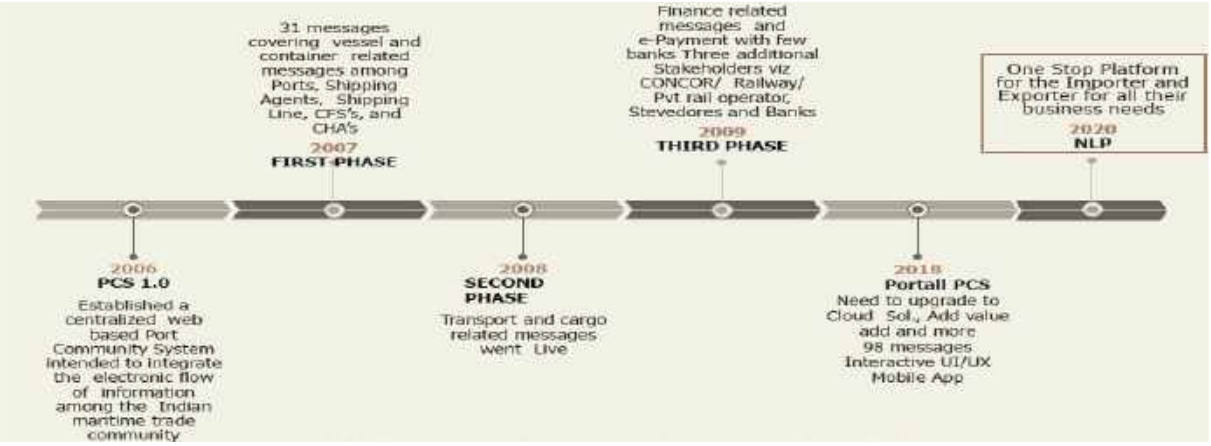
Ministry of Commerce, Ministry of Shipping and Indian Ports Association have envisaged a National Logistics Portal which would integrate the Marine National Logistics Portal, Land National Logistics Portal, e-Marketplace and Air National Logistics Portal. The implementation is envisaged in a phased manner as depicted in the diagram below:



To address the challenges faced in PCS 1x, as the first phase, IPA has decided to rollout the National Logistics Portal (NLP)- Marine which will in conjunction with the existing PCS1.x platform and will offer the following for the Maritime stakeholder community.

- Regulatory bodies and PGA services
- Banking and Financial Services
- Cargo and Carrier services

Once NLP-Marine is developed and operated, it will be ultimately get merged/integrated with the I-log platform (single window) being developed by Logistics Division of Ministry of Commerce which embraces by Logistics portals viz. marine, land, air and e-market place.



The journey of how PCS has evolved and the vision how PCS will be transformed into NLP is depicted below:

2. Proposed National Logistics Portal - Marine

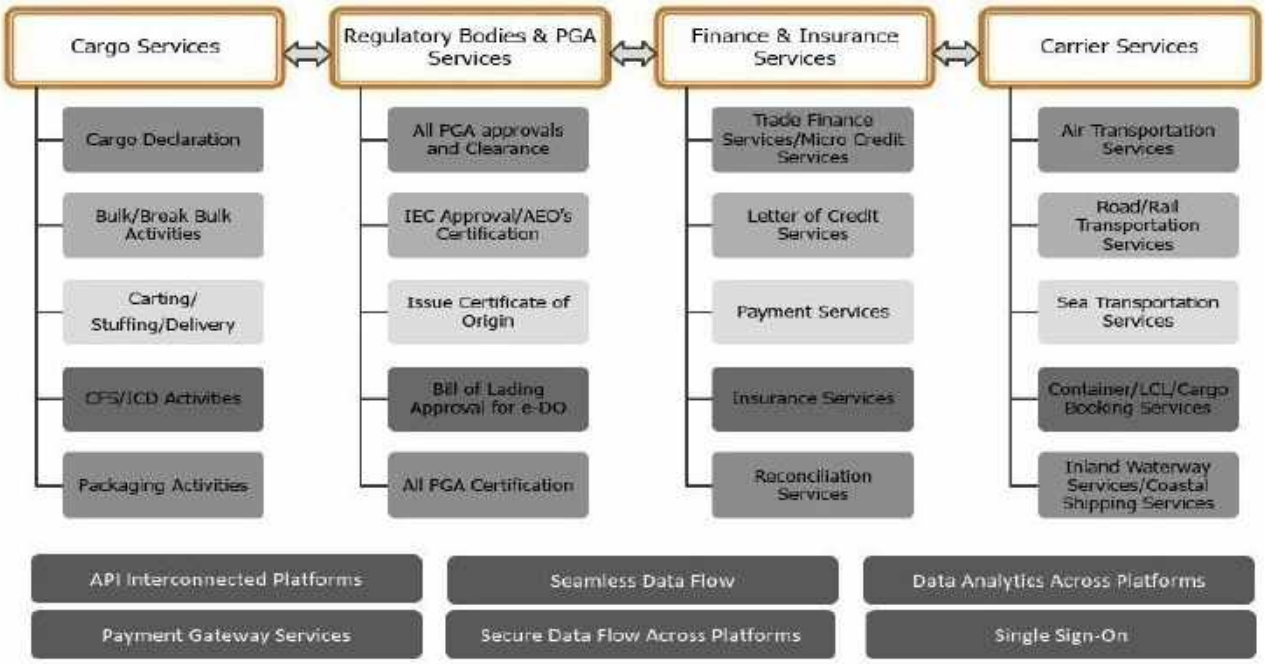
2.1 Overview of Proposed NLP-Marine

PCS 1x is currently operational for nineteen port communities, predominantly the messages being exchanged are between the Ports, and the Customs, that too mostly vessel related. **Annexure I** in this document shows the total identified stakeholders under the PCS 1x program.

Due to the prevalent scenario, following are the challenges faced by Trade on a daily basis.

- Absence of standardised formats across stakeholders;
- Limited levels of automation among various stakeholders;
- Manual process for documentation and duplication of paperwork as required for various agencies and stakeholders;
- Lack of real time information;
- Lack of standardised operating procedures and timeframe for giving approvals;
- No standardisation and harmonization of processes and Documentation;

The NLP-Marine is designed in order to offer the following for the maritime stakeholder community.



2.1.1 Cargo Services

The services under this platform will be related to the activities of the Cargo / Goods

- These services will include activities which are performed at Custodians' premises, such as Port / Terminal / ICD / CFS etc.
- Other than the custodian services, operations performed at the Warehouses will be covered
- Activities / services for handling non-containerized cargo will be included in the same

2.1.2 Regulatory Bodies and PGA Services

In the logistics certification platform, the exporter and importer shall be user of the platform, which will interchange data with PGAs and EPCs.

- For different goods, and origin destination pair, NLP-Marine shall display the different certification requirement
- NLP-Marine shall also include a common application form (CAF) to simplify regulatory process
- Different information from the CAF shall be shared with the respective PGA/ EPC for certification process. The integrated regulatory platform will witness data interchange with customs, PGAs and EPCs and will allow exporters and importers to access facilities like digi-lockers and check status of compliance.
- Functionality which is performed with Regulatory authorities will be included.
- Application of IEC and other application for procuring other licenses will be provided
- Commodity-specific bodies such as FASSAI / Coffee Board / Textile Committee etc. can provide certificate / clearance for the shipments

2.1.3 Carrier Service Platform

Activities related with Shipping Lines / Shipping Agents / Airlines will be provided as per the following

- Shipping will include EXIM as well as Coastal movement
- Inland Waterways will be integrated to provide their services on NLP-Marine
- Services such Container Booking / Slot booking can be performed
- Services involved under Rail / Road movement of goods will be available

2.1.4 Finance and Insurance Platform

The banking and financial services module will have banks, insurance companies and traders as main users

- The module shall help users find insurance and LOC service providers
- Shall help bank access documents for payment and authentication checks
- Transaction activities such as e-payments to any stakeholder within the system will be available
- Services offered by Bank such as LC process, Bank Guarantee Process can be done
- Reconciliation service to benefit the Services provider and consumer for easy tracking of the payment history and faster reconciliation process
- Onboarded Insurance providers to provide insurance for Domestic / International transportation of Cargo

2.2 Concept of NLP Marine

NLP Marine shall be designed as an “open platform” and in a manner that allows coexistence of multiple service providers to provide EXIM related services independently or by using connectivity options and data as authorized byIPA.

The design shall enable business users to amend and manage business rules relating to routing of messages, workflows etc. through a suitable rules engine and service catalogue should be configurable; without the aid of technicalpersonnel.

The proposed solution shall be highly configurable through dynamic forms, list grids, layouts etc. Changes to these components shall be achievable without code modification. For example, all list grids provide selectable fields to be displayed, export to excel/ pdf/ print/ XML function, filtering etc. which is configurable. New changes on existing modules shall be faster to incorporate and mostly achieved with minimal code changes. E.g. adding a new field to an existing form is more of aconfiguration.

The proposed solution shall have the capability to integrate with various Port Operating Systems/ Terminal Operating Systems and other stakeholder(s) systems in the ecosystem.
All documents generated by the proposed solution will be in line with global best practices and standards

Some of the benefits of the NLP-Marine platform are as follows:

- Single Platform to perform all core activities of the Importer / Exporter / Customs Broker / Freight Forwarder
- Complete domestic tracking of the shipment with notifications on each stage
- End-to-end functionality to perform self-clearance digitally Online transaction with custodians
- Remote EDI System Package – For Bill of Entry and Shipping Bill checklist + EDI file generation
- Document Management System to store all the important documents securely on Cloud Storage. Which helps in any time retrieval
- Real time information of the activities which are generally not in reach of Importer / Exporter / Customs Broker. For instance, Vessel related information, Terminal Gate Transaction, CFS Gate Transaction etc.
- Digital transaction for all the payments which are required for the clearance process (Import + Export). e.g. CFS Charges, Line Charges, Transportation Charges etc.
- ERP system like User Interface gives overview and tracking of the current status of the shipment.
- Paper-less transaction, as all the stakeholders like CFS and Lines can exchange the digital documents over the platform
- Data Lake and analytics
- A National Logistics Portal must allow for importers, exporters and service providers within the community to be able to seamlessly exchange documents and transact in transparent and quick manner. Some of the considerations for the NLPMarine are:

- Ease of Business – get India to be the one of the most cost effective plus competitive countries in terms of carrying international trade.
- Transparency – enables access to information across the supply chain for all stakeholders.
- Remove Bottlenecks – caused by lack of timely and date visibility.
- Empower end users – with real-time decision-making tools.
- Providing a level playing field to relevant stakeholders (large & small) thus increasing the competition
- Promote digital entrepreneurship by providing robust digital ecosystem on which multiple latch on can be built.
- NLPMarine mainly aims to function as central system for electronic sharing and exchange.
- Interoperability across Ocean, Coastal, Inland Waterways Land Rail, Air,
- Secured Data Access cross all stakeholders; Trusted networks
- Compliance and Accreditations
- Market Place
- Reduced costs and timeframes for execution of trade and logistics operations
- Improved port / terminal logistics chain efficiency
- Process automation enhancing goods clearance
- Simplified and accelerated procedures for goods entry, exit or transit
- Enhanced transparency in Government to Business relations
- Ease of doing business

The overarching NLPMarine Vision is to cater to various stakeholders in G2G, G2B and B2B model. As such the key stakeholders of an effective Single Window system would be

- Exporters
- Importers
- Customs
- Regulatory Authorities
- Immigration
- Banks
- Ports (Sea, Land and Air)

PCS 1x is live and functional since 11th Dec 2018 and serves as single platform for exchange of data and documents between Shipping Agent / Lines and Sea Ports.

It facilitates the vessel related filling of data by Shipping Agents, facilitates e-Payments between Ports and Stakeholders, Dissemination of Customs Messages, Release of Cargo process and connects all maritime stakeholders on to one platform.

PCS 1x, taking advantage of advances in technology, also implemented an open architecture; one that allows bringing in various trade solutions/ software's and integrating the same into the EXIM process flow.

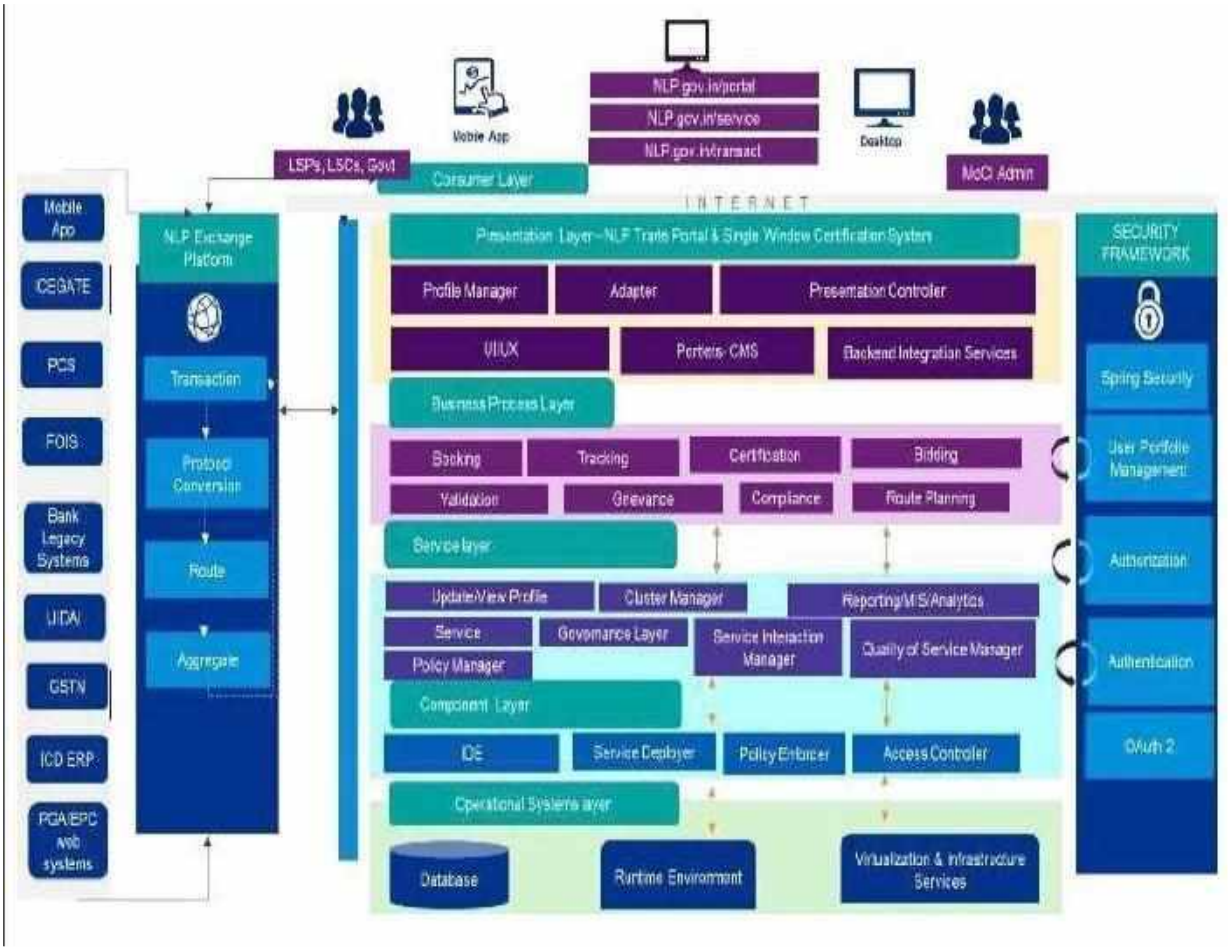
This makes the PCS 1x platform assimilative and inclusive. It offers leveraging existing technology solutions rather than build new solutions from scratch. This approach also ensures easy buy-in from stakeholders as their existing investments are protected. These solutions are called latch-on solutions.

The implementation of an 'Open Platform' in PCS 1x facilitates various time-tested solutions to connect with PCS and provide an unparalleled ability to enhance services to various stakeholders. The "Latch On" feature is a unique concept built in and delivered with PCS 1x.

The Latch On feature facilitates the trade in providing the required features that cannot be directly embedded into any Single Window Platform even though the features/ functionalities are required for seamless data and document exchange. Latch-on achieve this without duplicating the effort.

It is envisaged that many standalone applications, developed by multiple vendors, users and other stakeholders may be integrated with NLP MARINE. Keeping this in mind the system shall be able to provide data on subscription-publication basis. as provided for in the Latch On services agreement developed by IPA. The organization of the information exchange between modules is fundamental to publish- subscribe (PS) systems. The PS model connects anonymous information producers (publishers) with information consumers (subscribers).

Figure below shows a pictorial depiction of how latch-ons function within the architecture of PCS 1x.

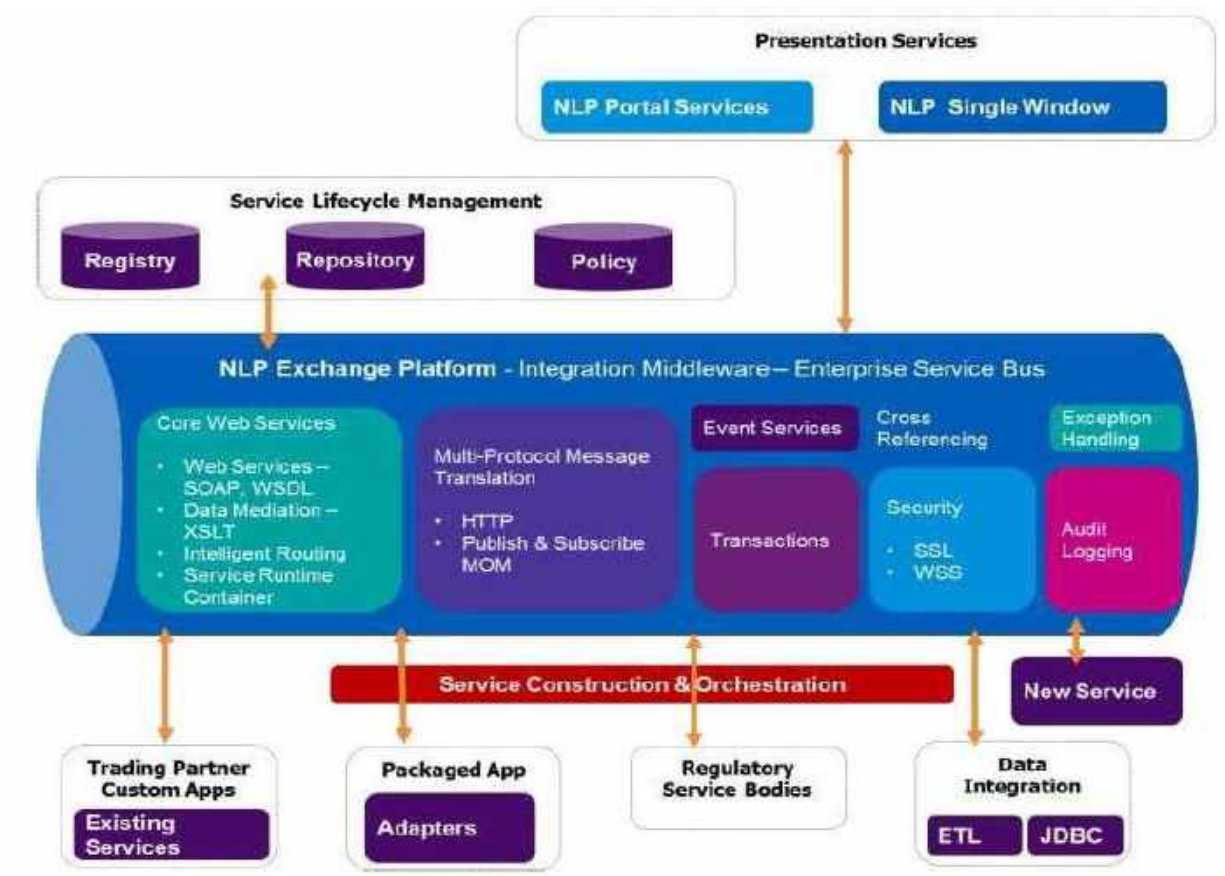


The proposed architecture will be depicted across various viewpoints like functional, logical and deployment based on the following architectural principles.

The above NLPNLP Marine Portal application architecture diagram shows service oriented architecture system diagram underlying the NLPNLP Marine Portal application. The architecture envisages four components of the system ‗NLP Marine Trade Portal, NLP Marine Single window Certification System, *e-Marketplace*and Mobile app UI for stakeholders. The NLP Marine URL is segregated into portal, service and transaction. Components in each successive layer are implemented based on the services provided by the previous layer. The diagram also shows how each layer is hosted in the different software components used for the NLP Marine Portal application. It also shows the communication between the different layers and the software components. An overview of each layer is provided below. Each layer is then discussed in much more detail in the following sections.

2.3 NLP Marine Exchange Platform Architecture

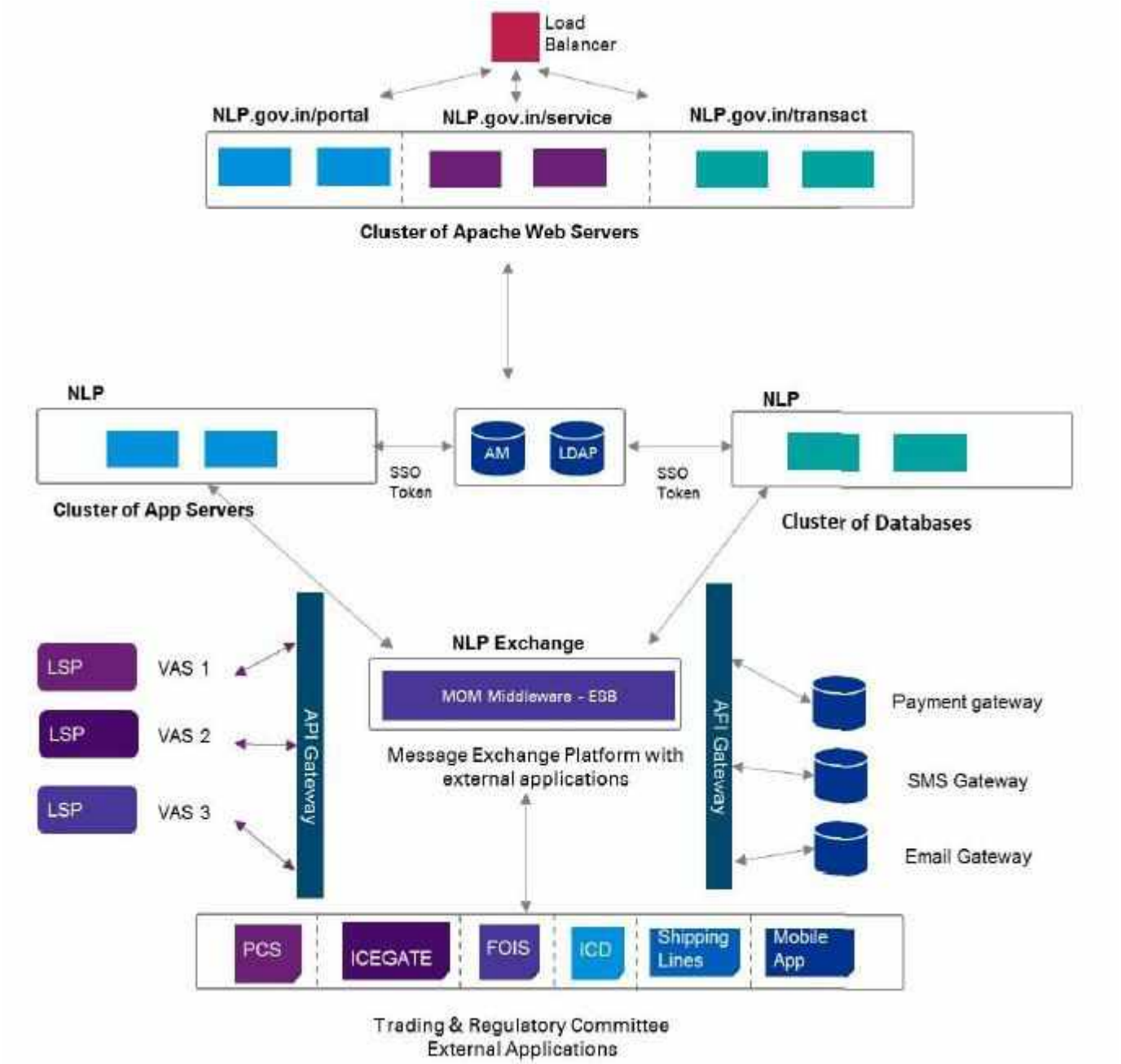
The NLP Marine Exchange Platform will be developed on Message Oriented Middleware which is capable of facilitating the transportation of asynchronous messages from one component to other. We shall be using the Publish Subscribe MOM Model. This method is used when there is necessity of communication between many to many components. Below we have provided a representation the NLP Marine Exchange Architecture.



The architecture of NLP Marine Exchange Platform is divided into three layers- Presentation, Integration and Service Orchestration Layer. The integration layer shall consist of core web service components, message translation protocol, security protocols, exception handling, translation, audit logging and cross referencing services. The layer will be mainly responsible for message exchange between different components. The Presentation service layer will be responsible to access the NLP Marine Portal and NLP Marine Single Window Services. The service Construction & orchestration layer shall expose the functionality of NLP Marine platform

in form of APIs which can be then used by end users to interact with NLP Marine Exchange Platform or develop their own value-added services.

2.4 NLP Marine DeploymentArchitecture



KEY ATTRIBUTES FOR THE NATIONAL LOGISTICS PORTAL

- Single window for certification and compliance
- Simplified access to certification process
- Coordination among stakeholders
- *Logistics e-marketplace*
- Cater to all exporters, importers, domestic traders
- Seamless movement of goods across multiple modes
- Paperless trade
- User friendly
- Transparent
- Integrated IT infrastructure

KEY OBJECTIVES FOR THE NATIONAL LOGISTICS PORTALMARINE

Most sought platform for exporters, importers and domestic traders

- Reduce regulatory complexities
- Logistics cost reduction
- End-to-end logistics time reduction
- Improve accountability
- Introduce professional standards and certification for service providers Improve logistics skilling

PROPOSED BENEFITS TO STAKEHOLDERS

TRADERS:

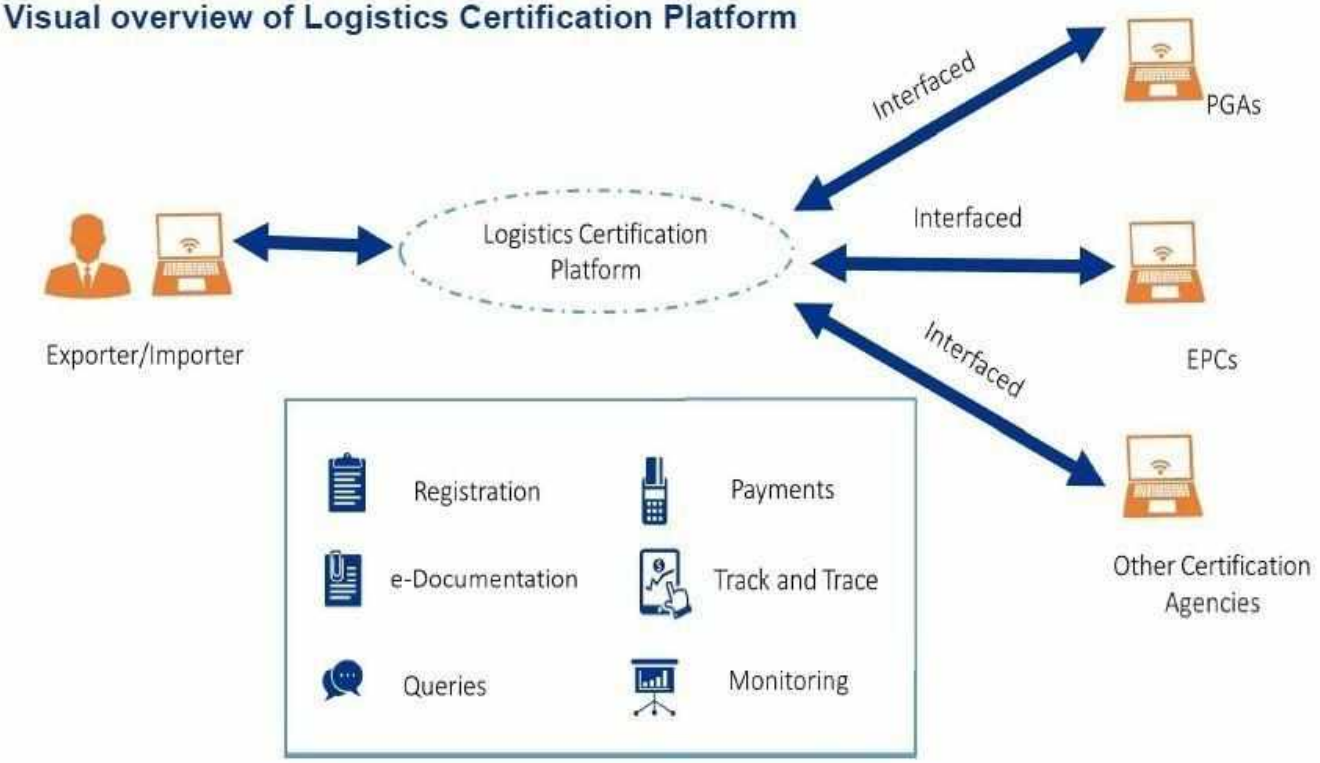
- Increased visibility and access to various Logistics Service Providers from all over the country
- Simplified discovery of competitive rates for various logistics services Seamless end to end logistics services available through a single platform with features like route planning and multi mode selections.
- Background verification and rating of Logistics Service Providers to ensure quality and credibility
- Assistance in EXIM certification through NLP Marine single window certification system
- Access to useful statistics about the market for efficient business planning

LOGISTICS SERVICE PROVIDERS

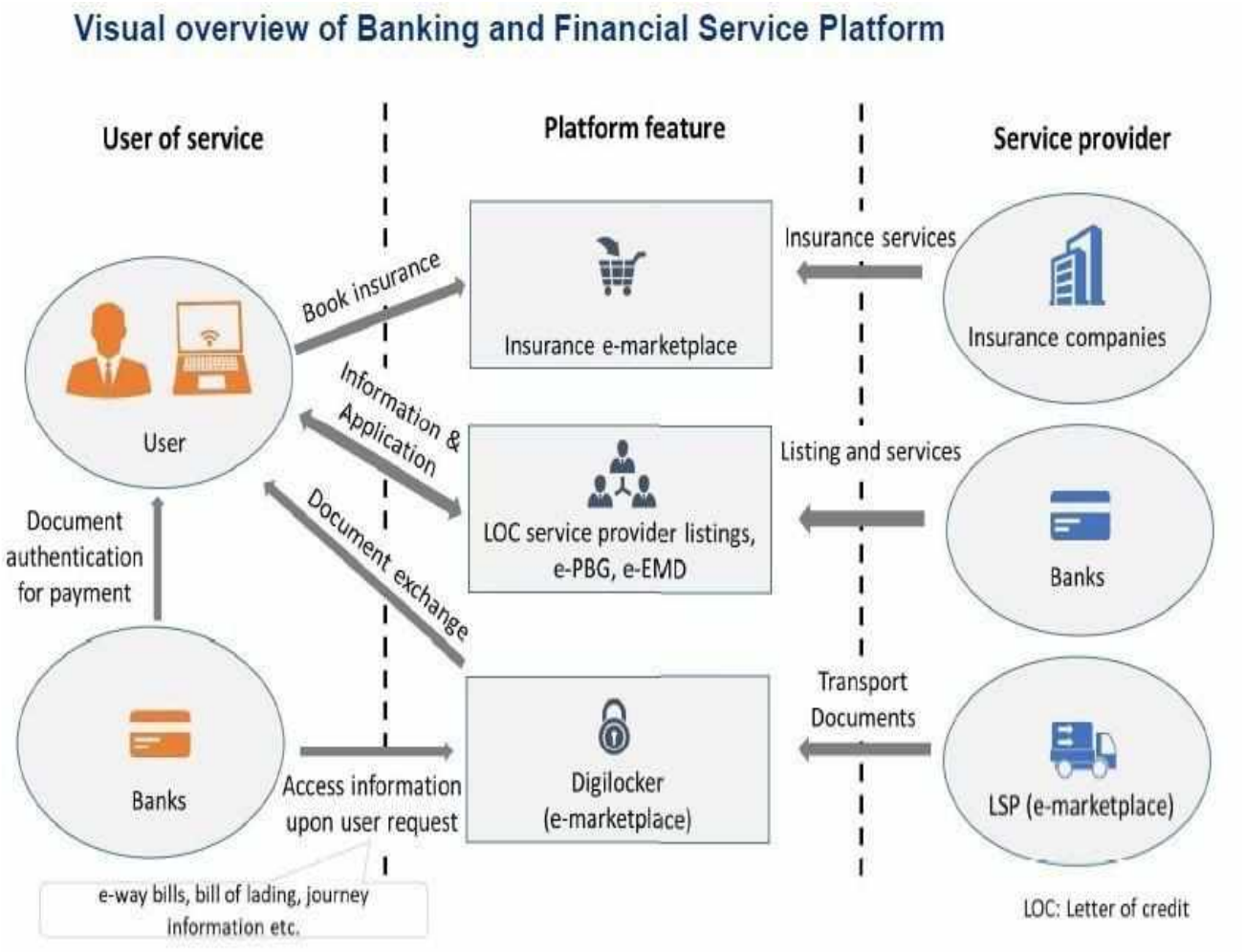
- PAN India visibility of services and access to prospective users from across the country
- Opportunity to build brand or enhance LSP brand image
- Increased capacity utilization and potential to increase LSP business volume
- Increased prospects for collaboration amongst LSPs for providing end to end solutions to users
- Accessibility to business statistics
- Reduction in time and effort for obtaining regulatory clearances

OVERVIEW OF FUNCTIONAL COMPONENTS

Visual overview of Logistics Certification Platform



Visual overview of Integrated Regulatory Platform



2.5 Solution Design Considerations

The NLP Marine solution is a multilayer architecture of the front-end web tier, security layer, the middle business tier, integration layer and the backend database layer. The key conceptual layers of the system are described below:

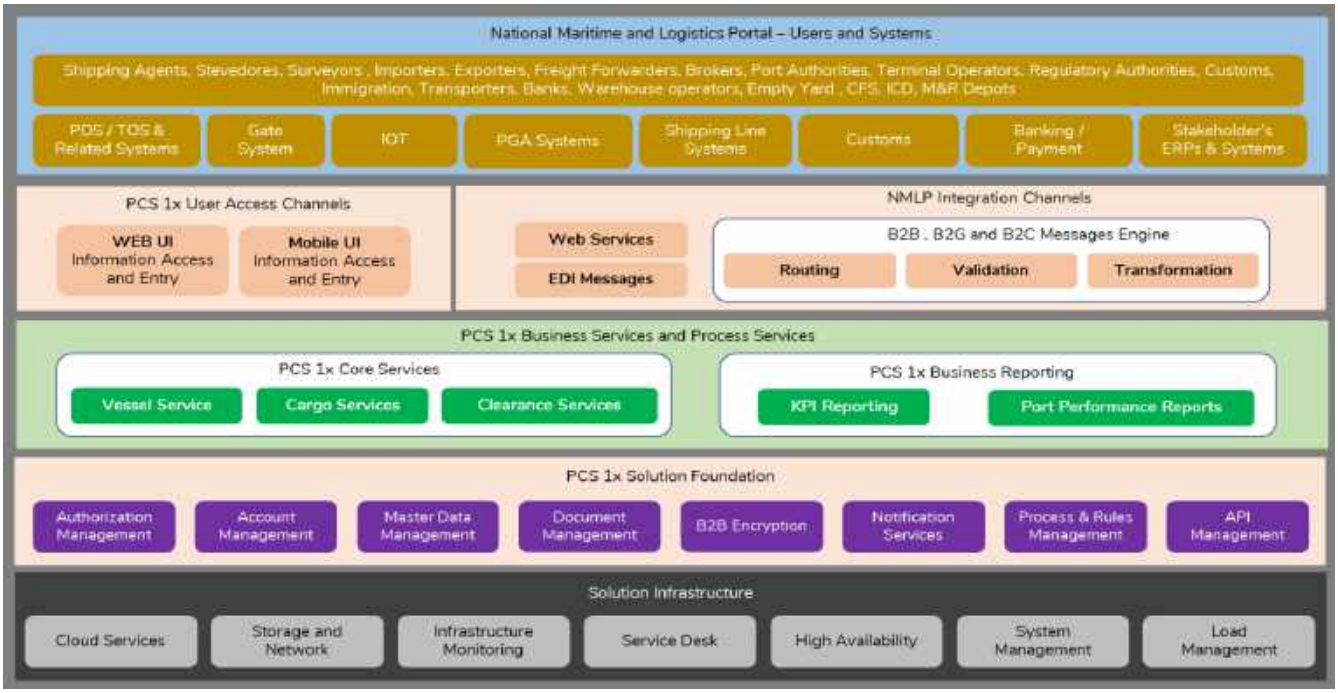
Presentation Layer – It provides user interface to connect securely to NLP Marine solution using Web Interface (HTTPS) – via Internet. The user interface provides functionalities based on the roles and permissions configured for those.

Application Layer – This layer encapsulates all Application related components mostly technical components which are responsible for the system like Notification Manager, Audit, Logger, Business processing.

Middle / Business Layer – This layer encapsulates all Business logic components required to support the underlying functionality for transformation and routing of business information to relevant stakeholders' basis the rules defined.

Data Layer – The data layer comprises of the Data Store which is a logical representation of the data files where the data is being stored in the database. This layer also includes the File Store

Integration layer – This layer is used for integrating NLP Marine with other 3rd party applications of other PGAs, Stakeholder systems, Payment Gateways, Insurance companies, SMS and Email gateways etc. as well as through API Gateway and SFTP servers.



Refer **Annexure IV** for Software Stack and other Technical Architecture Considerations

The proposed solution shall have provisions for translating messages of different standards (EDIFACT, XML, ANSI etc) to facilitate meaningful exchange of messages with multiple external systems in required formats.

The proposed NLP Marine shall have the functionality and features such as message transmission, message translation, authentication and authorization, single sign-on, communication gateway, customer management system (CMS) & component of event handler. The data transacted by the stakeholders must be through Digital Data Exchange (hereinafter referred as DDx) module of NLP Marine. The stakeholder needs to have requisite hardware / software as specified by the IPA. The same will be communicated by IPA once the bid has been awarded to the qualifying bidder.

Architecture should be scalable (to cater to increasing load of internal and external users and their transactions) and capable of delivering high performance for the entire life cycle of the applications.

Data model, interface designs, and other components should be designed as per industry standards and best practices.

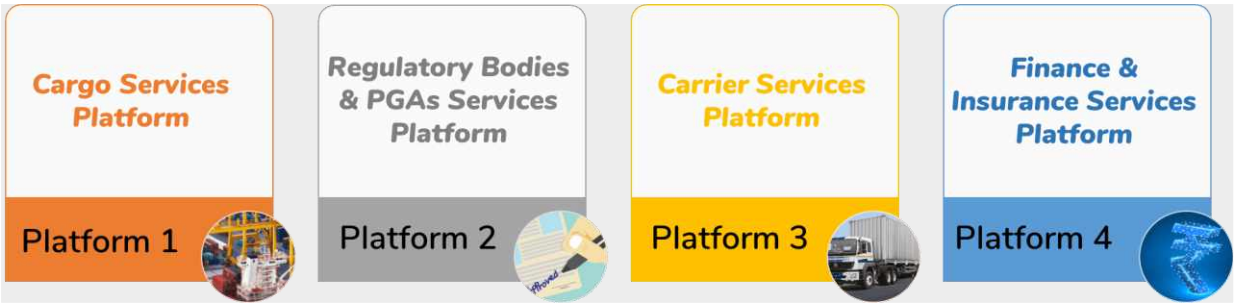
Solution design shall include, the design of the application architecture, user interface, database structures, security architecture, network architecture, deployment architecture etc.

The components/ services should be designed in a manner that ensures ease of implementation and maintenance.

The proposed solution should be able to scale up for user volume, data volume, transaction volume and functionality; as and when required.

The proposed solution should comply with security guidelines as defined and required by the Government of India.

In view of the conceptual framework of NLP Marine + PCS Ver 1x, The platforms becomes the central hub in all interactions with various stakeholders viz. Port, Terminals Shipping Lines/ Agents, CFS and Customs Brokers, Importer / Exporter etc. These interactions are expected to take place in real time. The communication among the stakeholders should be fast, reliable, recordable and device independent. Furthermore, the value-add system should be able to provide audit trail of all processed transactions.



Cargo Service Platform:

- This services under this platform will be related to the activties of the Cargo / Goods
- This services will include activities which are perfomed at Custodians' premises, such as Port / Terminal / ICD / CFS etc
- Other than the custodian services, operations performed at the Warehouses will be covered
- Activities / services for handling non-contenarized cargo will be included in the same

Regulatory Bodies and PGAs Service Platform

- Functionality which is performed with Regulatory authorites such as Customs will be included.

Carrier Service Platform

- Activities related with Shipping Lines / Shipping Agents / Airlines will be included
- Shipping will inclue EXIM as well as Coastal movement
- Inland Waterways will be integrated to provide their services on NLP Marine
- Services such Container Booking / Slot booking can be performed
- Services involved under Rail / Road movement of goods will be avaiable

Finace and Insurance Service Platform

- Transaction activites such as e-payments to any stakeholder within the system will be available

The value adds provided by the solution provider would be oriented towards each stakeholder of the platform and not to the Ports only.

Key objectives proposed to be achieved through the project under this RFP are as follows:

- Use data as provided by PCS 1x; NLP Marine shall be the primary source of data
- Improve upon what has been already established; i.e neutral and open electronic platform enabling intelligent, easy, efficient, and secure exchange of information between public and private stakeholders facilitating re-use and centralisation, available 24/7/365;
- Move towards a paperless regime i.e to optimise, manage and automate port and logistics processes by connecting transport and logistics chains i.e. electronic handling of key processes regarding import and export of containerised, general and bulk cargo

- Facilitate the stakeholders to improve their efficiency through exchange of business-related information with their trading partners accurately and quickly through their normal mode of business communication – multi-channel service delivery through mobile devices, portal etc
- Enable the usage of the vast amount of business-related knowledge of the platform through appropriate tools for processing of maritime and related statistics;
- Improve the quality of service and ease of doing business.
- Provide status information and control, track and trace to the stakeholders

The proposed solution design for value-add services software should take into account the following:

- **Open and Industry Standards for Interoperability**
- **Service Oriented Architecture (SOA)**
- **Integration and Support for API Driven Design**
- **Master Data Migration**
- **Ease of Management**

The solution must factor capabilities and features that allows for ease of management and troubleshooting. The underlying technology needs to support user friendly design. By having easy to use principle, training can be kept to a minimum thereby aiding IT change management and the risk of using a system improperly can be minimized.

The solution shall provide support for:

- E Monitoring of services using monitoring tools like Enterprise Management i.e. Ability to provide backup and restore of data
- Support maintenance, enhancement and refactoring the solution without architectural changes
- Administering the solution with minimal user intervention and using role based administration, well defined user interfaces and access policies
- Ability to log and report at a sub-system level state, health of the solution. It shall also encounter by the subsystem

1. **N-Tier Solution Design**
   Various layers of the solution i.e. application user interface, logic, data must be separate. The logical design of components, subsystems, application systems and databases will be ideally partitioned. These partitions shall have well-defined interfaces established. Logical boundaries are needed to separate components from each other. Modular design is more adaptive to changes in internal logic, platforms, and structures. It is easier to support, more scalable and supports interoperability.

2. **High Availability, Failover and Load Balancing**

3. **Cloud Enabled Deployment**
   Application should be hosted in a MeitY empanelled Cloud Service Provider.

4. **Virtual Private Network Deployment**

   The IT Infrastructure will have multiple security layers to secure the infrastructure from external threats. The proposed deployment should have different security zones as briefed below. The firewall policies shall be configured based on zone-based requirements.
   - **Militarized security Zone (MZ)** for Production Servers (Database and Application server Farm will securely host all critical application, Data Base server, Storage etc.
     This Zone shall not be accessible from Internet directly. All user traffic will have to enter in this security zone after firewall only. The proposed solution will have provision of dedicated Internal Firewall to secure the critical production (Data base and Application) environment.
   - **Demilitarized Security Zone (DMZ) for Web server Farm**

This security zone will host all servers that can be accessed from external users after authentication and traffic filtering. This zone shall host the Web servers, Access control and sign on servers etc.

- **Test, development and Staging zone (TDSZ)**
  This zone will host all servers required for test and development for applications. This zone will have limited access and it will not have any direct access to Production zone (MZ).
- **IT infra Management zone**
  The technical manpower proposed by Service Provider for DC and DR infrastructure will use this facility and will be able to access the infrastructure from this zone only.
  The activity shall be monitored in all the zones.

5. Backup and Recovery

Service provider shall prepare a backup policy which shall be approved by IPA.
Service provider shall be required to design detailed backup and recovery policies which shall be implemented at the time of deployment and the responsibility of taking backups and testing the backups as per the backup policy shall be for the entire project period.
Service Provider shall ensure that the data is replicated at the backup and DR Site.
Service Provider shall be responsible for complete data

- Data at rest and Data in motion Encryption
- Information Security: Log Monitoring and Correlation
- Disaster Recovery
- Policy and Documentation

Service provider shall develop, document and implement the following:

- Data Backup, Archival and Retention Policy
- Security Policy
- Disaster Recovery Policy

All the policies and procedure which will always ensure availability and security, these policies will have to be updated every six months (twice a year) or as per requirements of IPA. Service provider MUST design and implement the policy (with IPA inputs) in compliance to the related ISO standards.

Design of Information Security Policy shall necessarily include but not limited to the following policies to ensure IT security:

- IT Risk Management Policy
- Information Classification Policy
- Access Control Policy
- User ID and Password Management Policy
- Asset Management Policy
- Incident Management Policy

6. Technical Obsolescence

The systems including communication technologies, which are at risk of technical obsolescence over the next few years and over the operating life of the system shall be identified and reported. This may also include end-of-sale and end-of-support policies governing the proposed technologies. The compatibility between the various elements of the system need to be considered and mitigation options, not be limited to periodic update from OEM/system supplier, shall be indicated in detail.

2.6 Technology Framework

The NLP MARINE system shall be built following the below design considerations:

2.6.1 Provision of a Sustainable, Scalable Solution

One of the key motives of a community platform like NLP MARINE is to provide a system that would be sustainable for the next few years. The expectation is that the system should sustain at least 10 years from GO-Live. The solution would be done keeping in mind the scalability of the system. The NLP MARINE platform is expected to deliver value by reducing costs, increasing throughput by decreasing dwell-times and increasing convenience for all stakeholders in the Maritime supply chain. These benefits are expected to lead to substantial growth in transaction volumes. Every component of NLP MARINE needs to be designed to scale horizontally to larger volumes of data.

2.6.2 Distributed Access and Multi-channel service delivery

With high penetration of mobile devices and increasing internet usage using mobile devices, it is imperative that the NLP MARINE platform provides multiple channels of service delivery to stakeholders. An important consideration is that the access devices and their screen capabilities (including browser variations) are numerous and constantly evolve. Hence, it is imperative to design the system such that an ecosystem of integrated apps also evolves. One of the design considerations is to provide multiple channels/interfaces to stakeholders to interact with the NLP MARINE system with the aim is to reduce load on portal layer.

2.6.3 Security & Privacy

Security and privacy of data is fundamental in design of NLP MARINE without sacrificing utility of the platform. When creating a system of this scale, it is imperative that handling of the sensitivity and criticality of data are not afterthoughts but designed into the strategy of the system from day one.Security and Privacy services allow for access control as well as maintaining privacy of user profiles and data.

- **Authorization and Access –** Authorization and access layers would allow the right users to access the right areas of the data architecture. It consists of various elements that control access over the application, database and infrastructure (network and server) layers
- **Data and User Privacy –** These services allow the users to distinguish between the data they want to share versus the data they wish to keep as private. Similarly, these services will allow users to share their profiles or keep them as private

2.6.4 Latch on Services

It is envisaged that many standalone applications, developed by multiple vendors, users and other stakeholders may be integrated with NLP MARINE. Keeping this in mind the system shall be able to provide data on subscription-publication basis. as provided for in the Latch On services agreement developed by IPA. The organization of the information exchange between modules is fundamental to publish- subscribe (PS) systems. The PS model connects anonymous information producers (publishers) with information consumers (subscribers).

2.7 Solution Architecture

For NLP MARINE to be able to conform to stakeholder requirementsandatthesametimebeabletomeettimelines/milestones,arobustarchitectureis requiredtobedefinedtocatertotheimmediateandfuturerequirementsofanagile,modularand scalablesolution.

2.7.1 Guiding Architectural Principles

The IT architecture principles defined in this section are the underlying general rules and guidelines that will drive the subsequent development, use and maintenance of architectural standards, frameworks and future state target architecture.

The overall system will be build based of the following architectural principles which will be the backbone of the overall system architecture:

Performance:

A best of the breed solution using leading technologies should be proposed in the solution ensuring the highest levels of performance. It will also ensure that the performance of various modules is independent of each other and enhances the overall system performance. Moreover, in case of a disaster/outage, the performance of one module should not impact the performance of other modules.

The solution should be designed in a manner such that the following design considerations are met:

a) Modular design to distribute the appropriate system functions on web and app server
b) Increase in-memory Operations (use static operations)
c) Reduce number of I/O operations and N/w calls using selective caching.
d) Dedicated schemas for each function making them independent and avoiding delays due to other function accessing the same schema.

Scalability:

ThearchitectureofNLP MARINEshouldbecapableofbeingscaleduptomoreuserrequestsorhandling more no. of input resources in various modules. Even inclusion of additional application functionalities should be catered to by upgrading the software editions with minimaleffort.

The design of the system to consider future proofing the systems for volume handling requirements:

a) The application functions to be divided logically and developed as Modular solution.
b) The system should be able to scale horizontally & vertically **Functionality** – Ability to extend functionality of the solution without significant impact to the existing functional components and infrastructure.
c) Scalability could be achieved by adhering to the following architectural principles:
d) Loose coupling through layered modular design and messaging
e) The architecture would promote modular design and layered approach with clear division of responsibility and separation of concerns at the data storage, service and integration layer in order to achieve desired interoperability without any affinity to platforms, programming languages and network technologies. The architecture has to be scalable, maintainable and flexible for modular expansion as more services are provided through NLP MARINE. Each of the logical layers would be loosely coupled with its adjacent layers
f) Data partitioning and parallel processing
g) Horizontal scale for compute, Network and storage

Security:

The security services will cover the user profile management, authentication and authorization aspects of security control. This service would run across all the layers since service components fromdifferentlayerswillinteractwiththesecuritycomponents.Allpubliccontentshouldbemade availabletoallusers without authentication.Theservicewillauthenticateusersandallowsaccess to other features of the envisaged application for which the user is entitledto.

The system should be designed to provide the appropriate security levels commiserate with the domain of operation. Also, the system must ensure data confidentiality and data integrity. The application system should have the following:

a) Data security policies and standards to be developed and adopted across stakeholders.
b) In order to adequately provide access to secured information, security needs must be identified and developed at the data level. Database design must consider and incorporate data integrity requirements.
c) Role based access for all the stake holders envisaged to access and use the system
d) Appropriate authentication mechanism adhering to industry best practices regarding Password Policies etc.
e) Ability to adopt other authentication mechanism such as Electronic Signature Certificates
f) Authorization validity to be ensured for the users providing the Data to the system. Data should be accepted only from the entity authorized
g) Data should be visible only to the authorized entity
h) Audit trails and Audit logging mechanism to be built in the system to ensure that user action can be established and investigations (if any) can be aided. (E.g. Logging of IP Address etc.)
i) Data alterations etc. through unauthorized channel should be prevented.
j) Industry best practices for coding of application so as to ensure sustenance to the Application Vulnerability Assessment

User Interface:

The architecture and application solutions should promote simplicity and ease of use to the end users while meeting business requirements. The solution should be simplistic, cost-effective, reduce development time and be easier to maintain when changes in requirements occur.

Thiswillbeaccomplishedbytheimplementationofrichuserinterfacesalongwithitsintegration with the DMS, Relational Data Store, Messaging and other externalapplications.

a) Efficient and layout design are the key considerations that enhance usability which should be factored in while designing the application. Standard and consistent usability criteria must be defined. An intuitive, user friendly, well-articulated navigation method for the applications greatly enhances the usability of the application.
b) Effective information dissemination
c) Enhanced functionalities including personalized delivery of content, collaboration and enriching GUI features
d) The load time for all web page user interfaces must satisfy both the following response time targets on 1 MBPS connection: 2 seconds for all pages 99 % of the time

Reliability:

NLP MARINE isacrucialsystemwithdataofhighsensitivityanditisimperativethat datatransferand data management should be reliable to keep stakeholder confidence aligned. The system should have appropriate measures to ensure processing reliability for the data received or accessed through theapplication.

It may be necessary to mainly ensure the following

a) Prevent processing of duplicate incoming files / data
b) Prevent unauthorized alteration to the Data uploaded on NLP MARINE
c) Ensure near zero data loss

Manageability:

It is essential that the application architecture handles different failures properly; be it a hardware failure, network outage, or software crashes. The system must be resilient to failures and have the ability to restart and make human intervention minimal. All layers of the system (application, infrastructure etc.) must be managed through automation and proactive alerts rather than deploying people for manual management.

Availability:

Thesolutiondesignanddeploymentarchitecturewillensurethattheapplicationcanbedeployed in a centralized environment offering high availability and systemfailover.

The solution should meet the following availability requirements

a) Sizing requirements based on load (balanced across web servers to avoid single point of failure - to be proposed by the vendor)
b) Deployment of multiple application instances should be possible
c) Distributed or load balanced implementation of application to ensure that availability of services is not compromised at any failure instance.

SLA driven solution:

Data from connected smart devices should be readily available (real-time), aggregated, classified andstored,soasnottodelaythebusinessprocessesofmonitoringanddecisionmaking,andwill enable appropriate timely sharing across theorganization. Readily available and consumed device data will facilitate timely access of analytics reports at every level and department of the organization and provide timely analysis of data as well as monitoring of KPIs through SLAs resulting in effective service delivery and improved decision making.

Master Data Management:

Systemshouldnotallowdatabase/systemadministratorstomakeanychangestodata.Itshould ensure that the data and file (data at rest) that is kept in the systems has tamper resistance capacity and source of truth (original data of cargo movement) could be used to reconstruct derived data such as ledgers and system generated returns. System should be able to detect any data tampering through matching of hash value and should be able to reconstruct thetruth.

The following Solution Architecture Framework is required to be adopted by the BIDDER to consistently define and deliver well-architected solutions that provide the desired value to all stakeholders and meet changing business needs. The framework ensures a strong architecture definition and it's governance across the lifecycle of the platform development and its operations & maintenance.

The Solution Architecture approach guided by this framework include the following key activities:

- ✓ Understanding stakeholder value
- ✓ Defining desired qualities that correlate with value
- ✓ Creating architecture that achieves qualities
- ✓ Selecting processes & methodology based on the qualities
- ✓ Ensuring that project delivers the qualities

Theframeworkensuresthefollowingqualitiesarebuiltinasqualitiesofthesystemalignedtothe most modern-day bestpractices–

- ✓ Identification of current and provisioning for potential Users of the System
- ✓ Digital Access and Delivery Mechanisms
- ✓ Service Oriented & Modular Architecture
- ✓ Alignment to MVC (Model View Controller) Design Pattern
- ✓ End to End Security
- ✓ Open Integration Framework
- ✓ System Management & Support
- ✓ Data store partitioning
- ✓ Improved Performance & Response Time
- ✓ Automated Monitoring & Alerts

NLP-MARINE is envisaged as a best in class digital service delivery platform. **Requirements at each of the layers and its components are detailed in this section.**

2.7.2 Data Architecture

The reference data architecture for NLP MARINE is described below :

Visualization and HumanInterface: The Visualization and Human Interface Layer allows for alerts, reports, dashboard as well as ad- hoc querying:

Web based GUI/ Real Time Reports - The reporting application would comprise a web-based GUI with certain real time reports depending on the needs of different stakeholders using the system. These couldinclude:

- Staticreports
- Analytical reports with drill downcapability
- Variance Reports (e.g., performancereports)

Alerts and Notifications –The alert and notification engine would enable real time or batch-based publishing of alerts and notifications across multiple channels (email,SMS)

Real Time Trace & Track – The real-time trace and track feature would provide a tracing mechanism not only for physical movement of cargo but also for EDI messages exchanged amongst stakeholders. This would enable all stakeholders to have a single- window view of real-time status of documentation and physical movement ofcargo.

DataLake – TheData Lake is the universal set of all data available to the enterprise, sorted into logical and manageable repositories

Structured Data –Structureddata components like data marts, data warehouses, ECM and metadata stores provide holistic, end-to-end transparent view across data silos on customer interactions, products and services**.** These also enable structuring of data to perform specific analysis as well as overall structured datastorage

Unstructured and Semi-structured data – Thesecomponents provide capability to store and manage large volumes of fast changing unstructured data over distributed file systems and fit-for-purpose NoSQLrepositories.These repositories will hold both external and internal data

DataAggregation –Dataaggregation layer allows extracting data from sources and making it suitable for loading it into the data lake

ETL (Extract, Transform and Load) - ETL provides for three capabilities and is suitable for structured data in batchmode:

- Extracting data from structured data sources
- Transforming data to make it suitable for loading into the Data Lake
- Routines to load the transformed data in the Data Lake

ESB (Enterprise Service Bus) –ESBis a transportation layer for real time data and messages. It also provides synchronous as well as asynchronous connection between variousapplicationsformessage-basedcommunication.Itcanalsobeusedtohostvarious SOAservices.ESB technical enhancements like Queue is also part of this document

API(ApplicationProgrammingInterface)–Externalsystems/applicationsprovide would APIs to communicate with these. The API connections would enable extraction of data from theseapplications.

Syndication - This provide easy data consolidation and management of information through integrated data feeds as necessary**.** Data syndication uses standardized communication protocol and standardized metadata vocabulary (e.g., Information and Content Exchange(ICE))

DATASOURCES

Mostvalueiscreated,wheninternalandexternaldatasourcesareconnectedinameaningfulway. Structured data sources (e.g., RDBMS databases) for information exchange prevalent to the NLP MARINEenterprise system are listed here:

Internal Data Sources:

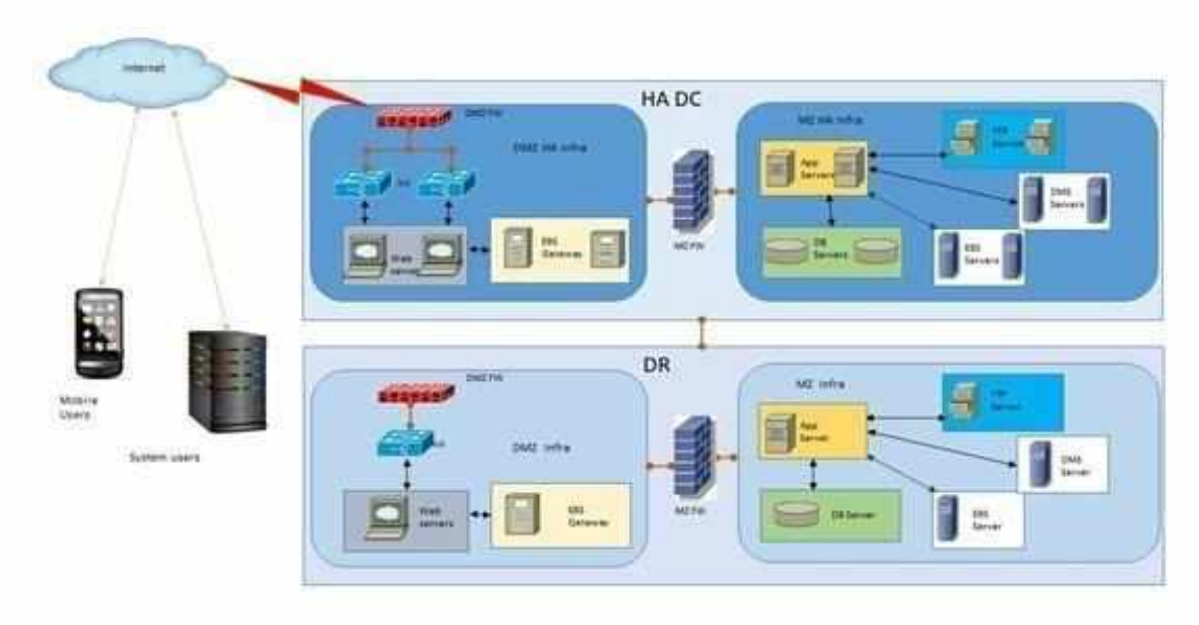
- **Master DB -** The master database contains all of the system level information for Server – all of the logins, linked servers, endpoints, and other system-wide configuration settings. The master databaseisalsowhereServerstoresinformationabouttheotherdatabasesonthisinstanceandthe location of theirfiles.
- **Transaction DB** – Transactional databases are used to store, manage and track real-time business information.
- **Reporting DB** – It takes a copy of the essential operational data but represents it in a different schema. The structure of the reporting database can be specifically designed to make it easier to writereports.
- **Audit DB** - Database auditing involves observing a database so as to be aware of the actions of database users. Database administrators set up auditing for security purposes, for example, to ensure that those without the permission to access information do not accessit.

2.7.3 Infrastructure Architecture

The Service Provider shall customize, integrate, implement, operate and maintain “NLP Marine Integration Platform” for the Indian Shipping eco systems and provide technical support to the solution.

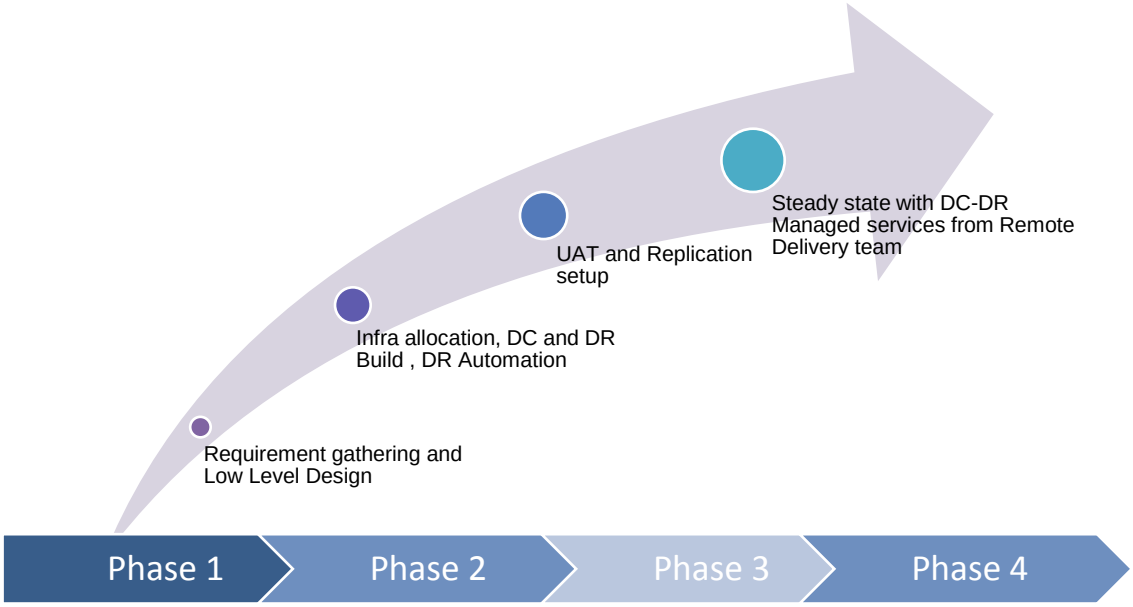
Cloud hosting is a robust, stable and integrated cloud platform on which enterprise can build e-Business applications, including complex, high volume e-Commerce sites instantaneously. Cloud hosting enables to accelerate e-Business initiatives and gets to market faster by reducing the time currently devote to "cobbling together" infrastructure components required to support business's IT requirements. With modular, secured and scalable components in the platform upgrade scalability is click away without any requirement for "forklift upgrade".

Every component in the platform has been designed and developed keeping the requirement of mission critical workloads of production environment. It includes scalable compute resources, enterprise class storage, multi-layer integrated security options and services, access network with special network offerings like Internet etc along with 24 *7 monitoring, management support. Cloud platform helps organizations take advantage of, virtualization, massive scalability, integrated scalable components with enterprise security and intelligent management with granular control.



Indicative Solutions Design: NLP Marine Cloud Infrastructure

Infrastructure Implementation Approach



Infrastructure Solution Baseline

- Cloud Hosting Model to provide Virtual Servers, Firewalls, Data Base & Load balancer
- Security Services for the infrastructure SIEM (Security information and event management, DDoS protection, PIM (Privileged identity Management) & MFA (Multi Factor Authentication).
- Multi-layer security infrastructure to prevent unauthorized access to the Data Centre.
- Networking and other associated IT Components in the Data Centre of Cloud Service provider.
- Storage requirements as per server specifications.
- 24 * 7 monitoring and management services.

- Authorize person from IPA member will has virtual access to the Cloud Data Centre 24 X 7 to each hosted server.
- Solution has proper cloud backup with a mechanism for restoring data to check the backup consistency as per the mutual understanding with IPA on SLA.
- Solution should be able to meet RPO (Recovery Point Objective) i.e. acceptable Data Loss and RTO (Recovery Time Objective) i.e. time to bring back system defined in SLA.
- All services and licenses procurement and implementation will be done by Service Provider for IPA, IPA will be the owner.
- Facilitate for the maintenance and support – L1, L2 and L3 support for the Application as per the mutual understanding with IPA on desired SLA.
- Facilitate for seamless application of Firmware upgrades, Hot fixes and updates on hosted Infrastructure/ Applications.
- Solution should have centralized identity management for all defined users.
- Solution should facilitate seamless exchange of information/ data in multiple formats and in electronic form.
- Solution should be capable of integration with external modules as defined by IPA or which can be envisage in future so that the stakeholders can be benefited.
- Solution should provide Decision Support Tools to all stakeholders.
- Solution is expected to be leverage a reliable, scalable and flexible infrastructure to cater the on-demand requests as per IPA Business Continuity Plan guidelines.
- Cloud Service Solution provider is expected to provide infrastructure hosting, managed services as approved by IPA.
- Solution is based on SLA (response and resolution) support as per the following:
    - Ticketing System for capturing incident and record of closure
    - On site resources for L1 & L2 Support
    - Off Site resources for L3 and above

Infrastructure Software Licensing baseline

Cloud Service provider will enable IPA to subscribe to available Software options within catalogue. The following table of options will be applicable.

Category	Pricing option	Description
Open source	No Charge	IPA can run unlimited versions of the same, except limited by number of VMs allowed per Cloud
BYOL (Only DB)	No Charge	IPA can bring their own Licenses and run the same, the Licensing is governed by the IPA with the Software vendors. IPA needs to certify and meet the conditions of the respective Software Vendors
Subscription from Cloud Service Provider (CSP) Under SPLA	Different options	IPA can subscribe for the licenses through SPLA model and pay monthly or Annual Payments, depending on the subscriptions. Note – IPA cannot combine in one Cloud host, with Subscription based and BYOL, either IPA will have to opt for subscription based or BYOL.

2.7.4 Security Architecture

The basic tenets of NLP MARINE security architecture are the design controls that protect confidentiality, integrity and availability of information and services for all the stakeholders. The security architecture must include Web Application Firewall (WAF), Intrusion Prevention System (IPS), Internet Connection Sharing (ICS) Firewall as well as antivirus. A diagrammatic representation of the security framework for the envisaged NLP MARINE system is provided below:

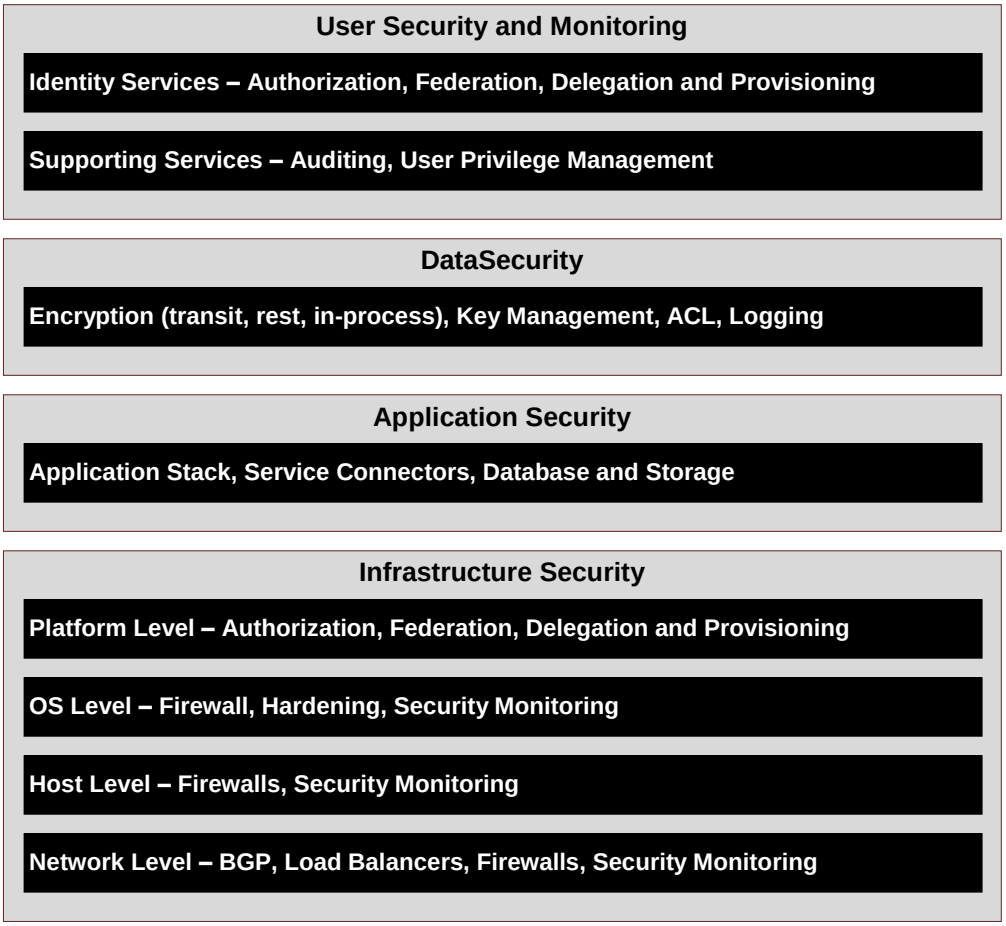


Figure 2: Security Architecture

Governance:

- All IT and IS operations should be governed by the IT and IS Policy which will be provided to the vendor. Detailed procedures for such operations should be prepared and implement accordingly. All project documentation should be prepared by the SI as per the policy and related regulations.
- SI has to adopt technical, physical and administrative measure in order to protect personal data from loss, misuse or alteration based on global best practices for privacy and security like OECD, APAC, IT act, Indian act compliance, NIST cloud computing reference model, CSA security guidance, ISO 27000 standards.

Network and Data Security:

- Infrastructure and Application Access should be protected via Two Factor Authentication such that the MPLS should be a private and dedicated network only providing connection between required and identified entities. The Network layer must have in depth packet inspection and intelligence in blocking attacks. There should also be a provision for DDOS Free Bandwidth as a part of its solution.
- All the Databases and Data stores should be encrypted to reduce the impact, in case of a potential compromise which in turns increases the complexity of attack by adding a layer of security.
- Data security life cycle should be used as a principle in securing data while creating, storing, sharing, archiving or destroy. Database protection can be implemented by database activity monitoring and file activity monitoring

Audits and Reviews

A vital part of any successful information security management system are regular reviews of the established security measures and data security processes.Audit shall focus on reviewing the effectiveness of the implementation of cyber security. Any/all audit activities must be agreed upon prior to executing.

Security Audit shall include:

- Application security assessment – Web applications testing, Source code review of web apps
- Vulnerability assessment & Penetration testing – VAPT of entire network, vulnerability closure guidance
- Infrastructure Security Assessment – Network security assessment, Review of configuration of various devices
- Report on Threat intelligence feed
- Support on Security gap implementation – with respect to ISO 27001/27017

Based on an information security review (IS review), statements can be made about the effective implementation of security measures and their currency, completeness and adequacy and hence about the current information security status. The IS review is therefore a tool for identifying, achieving and maintaining an adequate level of security within an institution.

The Audit should be focussed on review of the IT security status of their business processes, services and platforms, as well as improving and upgrading them on an ongoing basis. Periodic audits should be conducted to assess the security and ISO 27001/27017 as the reference and submit the audit report and action plan to purchaser. Regular security reviews must be carried out in the case of both public and private security services. However, it is typically easier for operators to pass the results of security reviews, e.g. penetration tests, on to users in the case of private clouds, because the users are all within one common institution.

To review the effectiveness of existing technical measures, penetration tests are a suitable tried and tested method. They are used to assess in advance the probabilities of success of a deliberate attack on an information domain or an individual IT system, to derive the necessary supplementary security measures from this, and to review the effectiveness of security measures already been taken. Prospective SI should carry out regular penetration tests on the networks, systems and applications they run.

Bidder shall get the Vulnerability Assessment (VA) and Penetration Testing (PT) and Application Security Audit conducted by CERT-In empanelled agency before deployment/ Go-Live of each project phase.Bidder shall be responsible for all payments to engage such agencies. MSP shall be required to make necessary changes in the BRS as well as other documents based on the changes made during testing and UAT.

IPA will also involve third party auditors to perform the audit/review/monitor the security testing carried out by Bidder. Cost for such auditors to be paid by IPA.

In general, all types of security test should be carried out by individuals with suitable skills. These should not, however, have been involved in drawing up the strategies and plans being tested, in order to avoid conflicts and business blindness. The testers and auditors should be as independent and neutral as possible.

Scope	Frequency
Security Audit	Quarterly

SLA Audit	Half yearly
VAPT	Quarterly
Inventory Audit	Once in a year
Secure Configuration Review	Quarterly
Information Security Controls like ISO27001	Half yearly
Privacy Audit and review	Half yearly
Privacy Impact assessment templates and library	Annually
Incident reporting & management	Annually
Data Protection Policy	Annually

Table: Audit Scope & its Frequency

2.7.5 Levels of Authentication

A strong authentication mechanism should be considered to protect unauthorized access to NLP MARINE. Consider use of at least two of the following forms of authentication mechanism:

- Something you know, such as a password, PINetc.
- Something you have, such as a smart card, hardware security tokenetc.
- Something you are, such as a fingerprint, a retinal scan, or other biometric methods

Based on the security requirements the following levels of authentication should be evaluated.

a) For applications handling sensitive data it is recommended that in the least one factor authentication key in the form of a password is essential. Strong password complexity rules should be enforced to ensure confidentiality and integrity of the data

b) For applications handling highly sensitive data it is recommended that two factor authentication mechanisms should be considered. The first line of defence is the password conforming to the 'password complexity rules. Along with the password next user has to provide a one-time password which varies for each session. One-time passwords are valid for each session and it is not vulnerable to dictionary, phishing, interception and lots of other attacks. A counter synchronized One-Time Password (OTP) solution could be used for this purpose.

2.7.6 Centralized Identity and Access Management Model

It is recommended to adopt an enterprise level centralized authentication model that is secured and ensures that user has a single credential to access the all the services.

In this model there will a centralized authentication services with provision for centralized user registration and user credential store. A centralized user repository (directory services) for the storageofusercredentials willalsostoretheauthorizationinformationfortheuserwhichwillbe used in differentapplication.

The proposed centralized Identity and Access Management solution is depicted below –

1. Central Access ManagementService

a) This service will provide the central authentication service for the users/groups created by verification of the user credentials against the central LDAP user repository. When a user tries to login to any centralized application e.g. single window portal, departmental sub-, the user credentials will be validated through the central authentication service.

b) Single Sign-On service will centrally maintain user session thus preventing userfrom multiple login when trying to access multiple applications

2. Central Identity Management Service

a) This service will handle user life cycle management that will enable NLP MARINE to manage the lifespan of the user account from its initial stage of provisioning to the end stage of de-provisioning. Typically, user provisioning and de-provisioning is workflow driven that will require approval.
b) User management service will cover user administrative functionalities like creation, propagation and maintenance of user identity and privileges.
c) Self Service feature will allow end users (e.g. members) to maintain their user identity account including self-password reset which will significantly reduce helpdesk/admin effort to handle password reset requests.
d) The central user repository will store the user identity data and deliver it to other services (e.g. central authentication service) for credential verification. Adherence to LDAP v3 standard has been the dominant standard for central user repository. Enforce a robust and strong password policies that will allow users to change/reset password with password expiry and account lockout features, define and implement complex password rules and session timeout policy.

3. Authorization

Authorization of system users should be enforced by access controls. It is recommended to develop access control lists. Consider the following approach for developing access control list -

a) Establish groups of users based on similar functions and similar access privilege.
b) Identify the owner of each group
c) Establish the degree of access to be provided to each group

4. DataSecurity& Privacy

- For Data Security of Infrastructure and Application Data Access should be protected via Two Factor Authentication such that the MPLS should be a private and dedicated network only providing connection between required and identified entities. The Network layer must have in depth packet inspection and intelligence in blocking attacks. There should also be a provision for DDOS Free Bandwidth as a part of its solution.
- All the Databases and Data stores should be encrypted to reduce the impact, in case of a potential compromise which in turns increases the complexity of attack by adding a layer of security.
- Data security life cycle should be used as a principle in securing data while creating, storing, sharing, archiving or destroy. Database protection can be implemented by database activity monitoring and file activity monitoring

Data Privacy and Data Protection are increasingly in the spotlight and undergoing a paradigm shift considering new regulations being introduced by developing countries such as General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), Personal Information Protection and Electronics Documents Act (PIPEDA- Canada) etc. Globally, 108 countries have come up with either comprehensive or partial privacy regulations. Regulatory frameworks of different countries for data privacy are distinct around the world vary from country to country and region to region. There are many challenges faced by organisations on data protection due to dispersed data protection regimes, no national level regulation on

data protection and technological developments which form new types of threats for an organisations/individual's data privacy.

Being an apex body of Indian major ports, IPA collects and exchanges huge number of messages and data through Port community system (PCS), which might lead to corruption, data or information leakage during its flow from internal to external or vice versa with its maritime stakeholders. IPA needs to identify what is the minimum amount of data they need to process in order to perform certain analysis or provide a service. IPA relates to external partners in its ecosystem for communication and data sharing where data security and privacy during processing of personal data is of utmost importance. As per the GDPR, following are few of the requirements for processing personal data and sensitive personal data:

- Draft, review and update existing data protection policies and standards
- Deploy tools and technology for data classification from privacy point of view
- Integrate privacy controls in the ecosystem and control testing
- Implement and enhance (existing) tooling to support data flow mapping
- Implement Risk register based on privacy
- Implement procedures for assessing risk of data flows
- Perform Privacy impact Assessments (PIA's) on new processes
- Support on enhancing security architecture to support privacy by design
- Describe procedures in information security policy and standards on data protection and implement such procedures
- Implement tooling to encrypt data on different technology layers, i.e., network, end-user, server, database, application, e-mail and unstructured documents
- Include data breaches in existing incident response procedures
- Implement procedures and tooling for monitoring third party and vendors by binding them to data protection principles

2.7.7 Traditional Structured Enterprise Data

Department should protect NLP MARINE System information against unauthorized access, denial of service, and both intentional and accidental modification. Data security, audit controls and integrity must be ensured across the data life cycle management from creation, accessed, viewed, updated and when deleted (or inactivated). This provides a proactive way to build defencesagainstpossiblesecurityvulnerabilitiesandthreats,allowingerrorstobecorrectedand system misuse to beminimized.

The implications for adhering to an effective data security and integrity guideline related to NLP MARINE are the following:

- Data security policies and standards to be developed and adopted in the NLP MARINE application
- Data security controls to be put in place to restrict access to enterprise data based on roles and access privileges. Data audit logs should be maintained for audit trail purposes. Security controls will be able to be reviewed or audited through some qualitative or quantitative means for traceability and to ensure that risk is being maintained at acceptable levels.
- In order to adequately provide access to secured information, security needs must be identified and developed at the data level, not the application level. Database design must consider and incorporate data integrity requirements.
- Procedures for data sharing need to be established. Data integrity during data synchronization needs to be ensured across the enterprise.
- Audit Capabilities: The system provides for a system-wide audit control mechanism that works in conjunction with the RDBMS.
- Maintaining Date / Time Stamp and User Id: Every transaction, with a date and time and User ID, is captured. The system allows generating various audit reports for verification.
- Access Log: The NLP MARINESystem should have extensive inbuilt security and access control mechanisms. Based on this, the system keeps track of the various functions accessed by any users.

2.7.8 Enterprise Manageability and Operations Architecture

The architecture can be divided into mainly the following components

- ✓ **ITSM Tools and Practices:** It is strongly recommended to use the ITIL best practices for the IT service management of NLP MARINE The key areas that are recommended to be setup for management of day to day operations of NLP MARINE as per ITIL best practices are:
  - **Event Management:** Any events that are captured in the application monitoring tools such as info, warnings and alerts need to be captured, correlated and processed by event management tools. Based on the result of correlation, tools can pinpoint to root cause of error / failure conditions and such events can be sent to incident management tools to create incident tickets
  - **Incident management:** Incidents refer to conditions of errors, breakdowns etc. which need support for corrections. Incidents can be manually created or created automatically by event management tools, or by application monitoring tools. The best recommended architecture is where all applications are monitored by a combination of infrastructure, security and application performance monitoring tools. These tools on generation of any kind of events create incidents of priority depending on severity of alerts.
  - **Problem Management:** In case incidents are closed with a workaround without a permanent resolution, deep dive investigations are followed up by opening of a problem record. Problem record documents the ongoing investigations and workaround available till the permanent resolution is achieved.
  - **Release and Deployment management**: Deployment of applications or application changes/components etc. in a complex enterprise such as NLP MARINE needs a seasoned deployment management process and tools. It is recommended to also use advanced capabilities such as DevOps which has capabilities such as continuous integration and continuous deployment to reduce the time it takes to commit a change in development and move the change to production.
  - **Access Management:** Access to grant authorized users is controlled using the access management process. Access management needs to be managed in a controlled manner and hence identity and access management suite is part of the Enterprise architecture of NLP MARINE. A clear definition of privileges associated with different roles needs to be defined where access to different application components, workflows etc. is well documented and maintained in the identity and access management system. A clear policy of upgrade and removal of identities needs to be also defined. Audit trails of any change in privileges need to be maintained in identity management system.
  - **IT Change management:** Any change to the system needs to be done via the regular change management process of ITIL. Change management requires the creation of a change management board who would be the different process/application owners. Periodic meeting of change request board would approve, reject all the changes to be carried out to any system after a detailed impact analysis and making sure all stakeholders are aware of their roles and responsibilities in carrying out their changes.
  - **Performance management:** A regular performance management process needs to be established where performance of key applications (customer facing and internal) needs to be regularly reviewed and any changes needed to ensure the scalability of the applications evaluated and recommended for change requests.
- ✓ **Application/Infrastructure Monitoring Tools and Practices:**
  - It is strongly recommended to have application monitoring in place for all applications where application performance is continuously recorded and evaluated. Application monitoring would enable quick troubleshooting of any issues related to application performance and also give a continuous end user experience measurement. Since the envisaged application is a community system, end user experience measurement is extremely critical to ensure any issues in application are caught and handled early before stakeholders on the community system take notice and complain.NLP Marine is a national platform and for user experience data assimilation layer is required.

- It is also recommended to have infrastructure level monitoring in place to keep a vigil on the health of theIT infrastructure on which the various application architecture layers are deployed. Infrastructure monitoring is a critical component of overall enterprise manageability and operations.

✓ **Security management and tools:**

- It is extremely important to have a set of IT security management processes and tools to ensure that the IT security of NLP MARINE is always maintained. It is recommended that an IT security policy, framework and operational guidelines be maintained by the BIDDER and Cloud service provider (CSP) as an overall guideline to all forms of IT security – Physical, application, data, network and cloud.
- The IT systems maintained should be regularly audited and subject to different IT security testing. The system should also maintain regular detailed audit records of all data changes made to critical systems. There should be tools to mine these audit records and gather intelligence from these tools to not only alert BIDDER and CSP of any breaches but also predict any security mishaps that can occur. Latest security tools like IPS, IDS, Malware protection, Data loss protection, DB change audit observation kits etc. need to be in place. All the security management processes, tools and usage should be well documented in security policy for NLP MARINE and guide the security processes to be followed to maintain IT security of the NLP MARINE system.

2.7.9 User Interface (UI) Design

User Interface (UI) Design will focus on what users might need to do and ensuring that the interface has elements that are easy to access, understand, and use to facilitate those actions.

Interface Elements

Interface elements should include but are not limited to:

- **Input Controls**: buttons, text fields, checkboxes, radio buttons, dropdown lists, list boxes, toggles, date field
- **Navigational Components**: breadcrumb, slider, search field, pagination, slider, tags, icons
- **Informational Components**: tooltips, icons, progress bar, notifications, message boxes, modal windows
- **Containers**: Accordions are useful when there is need to toggle between hiding and showing large amount of content. Each item can be "expanded" or "stretched" to reveal the content associated with that item.

Key pointers for designing a User Interface

Following parameters will be considered while designing the interface:

- **Simple interface and aesthetic:** Avoid unnecessary elements and clear in the language being used on labels and inmessaging.
- **Consistency and common UI elements:** By using common elements in UI, users should feel more comfortable and are able to get things done more quickly. It is also important to create patterns in language, layout and design throughout the site to help facilitateefficiency.
- **Purposefulpagelayout:**Spatialrelationshipstobeconsideredbetweenitemsonthe page and structure the page to be based on importance. Careful placement of items will help draw attention to the most important pieces of information and can aid scanning andreadability.
- **Strategic use csolor and texture:** Attention can be directed or redirect away from items using color, light, contrast, andtexture.
- **Typography to create hierarchy and clarity:** Different sizes, fonts, and arrangement of the text to help increase scan ability, legibility andreadability.
- **System communication:** Users should be informed of location, actions, changes in state, or errors. The use of various UI elements to communicate status and, if necessary, next steps will help theuser.

- **Defaults.** Defaults can created to reduce the burden on the user. This becomes particularly important when it comes to form design where an opportunity to have some fields pre-chosen or filled out can beprovided.
- **Usercontrolandfreedom**:UIshouldofferusersadigitalspacewherebackwardsteps are possible, including undoing and redoing previousactions.
- **Help users recognize, diagnose and recover from errors:** Designers should assume users are unable to understand technical terminology, therefore, error messages should almost always be expressed in plain language to ensure nothing gets lost in translation.
- **Help and documentation:** Users to navigate the system without having to resort to documentation.However,dependingonthetypeofsolution,documentationmaybe necessary. When users require help, ensure it is easily located, specific to the task at hand and worded in a way that will guide them through the necessary steps towards a solution to the issue they arefacing.

  Guidelines for Indian Government Websites (GIGW) Compliance 2018 should be strictly followed while designing User Interface (UI) and User Experience (UX) for NLP Marine**:** https://guidelines.gov.in/

2.7.10 Continuous adoption of rapidly evolving Technology

Technology evolves rapidly and it is imperative for a project like NLP MARINE to naturally adapt to new technologies. Typically for projects similar to NLP MARINE, any changes to existing implementations require contract changes, new RFP (Request for Proposal), etc. Hence the entire system would be built to be open platform standards (open API, plug-n-play capabilities), components coupled loosely to allow changes in sub-system level without affecting other parts, architected to work completely within a heterogeneous compute, storage, and multi- stakeholder environment. New technology interventions like Block Chain, 5G, AI/ML, RPA,Blockchain based smart contracts, Contract gateway, API gateway service bus etc should be considered by the BIDDER wherever relevant. Make in India policy to be adhered to.

2.7.11 Integration Framework

Responsibility of SI in Integration:

a. Developing SOPs (Standard Operating Procedures) for integrations of various types;
b. Coordinating with the IPA on all common issues relating to integration and undertaking Policy Advocacy for putting in place appropriate technological and administrative policies for the effective creation and management of all Integrations.
c. Standardization of interfaces, protocols and Interface maintenance procedures in consultation with the SIs and undertaking Capacity Building thereon.

Proposed Integration Solution/Integration Tool

The proposed Integration solution/EA Tool should be able to perform as per requirements mentioned below but not limited to:

1. Perform complex data mapping and transformations
2. Support active/active clustering
3. Provide built-in transformation functions
4. Perform the transformation of message content based on pre-defined conditions
5. Logging and auditing capabilities
6. Support alerting via SNMP and e-mail
7. Support the concept of synchronous publish-and-wait for event notification
8. Should be scalable to support increases in transaction volume

9. Can handle large data volume
10. Can support the following standards
    i. SOAP 1.1
    ii. SOAP 1.2
    iii. SOAP over JMS
    iv. SOAP over MQ
    v. SOAP over SSL
    vi. XSLT 1.0
    vii. XSLT 2.0
    viii. XSLTC
    ix. WSDL
    x. SAML
    xi. JAAS
    xii. WS-I BP
    xiii. WS-Addressing
    xiv. WS-Security
    xv. WS-I BSP
    xvi. SOAP with Attachments
    xvii. MTOM
    xviii. Log4j
    xix. UDDI v2
    xx. UDDI v3
    xxi. WS-Security SAML Token Profile
    xxii. SOAP with Attachments API for Java (SAAJ)
    xxiii. XML/HTTP(s)
    xxiv. REST
    xxv. Generic XML/HTTP

Operations and Governance

The SI need to operate the system for a period of contract duration. They will ensure the overall standardization. They will be the authority to certify that whether the application meets the functional/non-functional requirements: Their responsibility will be as per mentioned below but not limited to:

1. Make sure that system is according to the requirements.
2. Develop the guidance documents for Integration Architecture
3. Prepare best practices in the Government sector.
4. Develop Project Value Evaluation Methodology
5. Develop the guidelines
    - ✓ Develop ESB Guideline
    - ✓ Develop API Management Guideline
    - ✓ Develop Policy Management Guideline
    - ✓ Develop Monitoring & Management Guideline
    - ✓ Develop Service Versioning Guideline
    - ✓ Develop Configuration Management Guideline
    - ✓ Develop Release Management Guideline

Roles and Responsibilities

The Roles and Responsibility of Integrator and Other application's owner are as follows:

System Integrator	Other applications Owner
Gather the requirements for systems to be integrated	To provide functional/non-functional requirements for the Integration

Design and Build the Interfaces	To support during SIT
System Integration Testing	To support during UAT
User Acceptance Testing	To support during Cut over and deployment
Cut over and Deployment	
Warranty Support	

Integration Guidelines

This section is to guide the SI for integration

Key Integration Approach

Integration Approach	Integration Mechanism
Web Services based integration	The applications which have the capability to send SOAP request and expose web services shall use this approach. In this approach any application which requires data sends a SOAP request. ESB shall act as a SOAP client and invoke the appropriate web services and send the required data as a SOAP response. These soap messages can be sent either using HTTP(S) or JMS as a transport. It is recommended to integrate all the third-party applications using this approach, as it offers platform independence, flexibility and reusability. Wipro's proposed solution would leverage web services based integration (using real time where applicable) to integrate with the solution.
File/FTP based integration	For bulk data extract or import using file transfers in a batch mode, the application will be integrated using file integration approach. In this approach a file/ftp adapter is configured to read the files, transform or enrich the content and publish the messages to the target applications. In cases where transformation is not required, a secure form will be used to transfer the file without enriching the contents.
Database (EAI) Integration	When the integration interface requires data to be fetched from a database or sent to a database this approach will be used. Depending on the requirement, a messaging solution or a bulk-transform solution may be used. In the messaging approach, a database adapter read service is configured to fetch the data from the database and publish the message to the ESB layer for consumption by one or more downstream systems. Further downstream, the ESB consumes the message, enriches and transforms these messages to the target application format. The bulk-transform approach applies to high-volume batch interfaces that involve heavy transformation rules and have a low re-use potential.
API Management	API Management manages complete lifecycle of API from definition to monitoring and tracking of API transactions for integration to different applications and devices. It enables dissemination of information exchange over a heterogeneous NLP Marine application

	landscape and provides common technical standards between all the system integrators and suppliers working on NLP Marine integration work

Reference Architecture of Integration Platform

Below is the reference architecture of the Integration platform. The SI is required to enhance it in line with industry best practices in application integration and integration management.

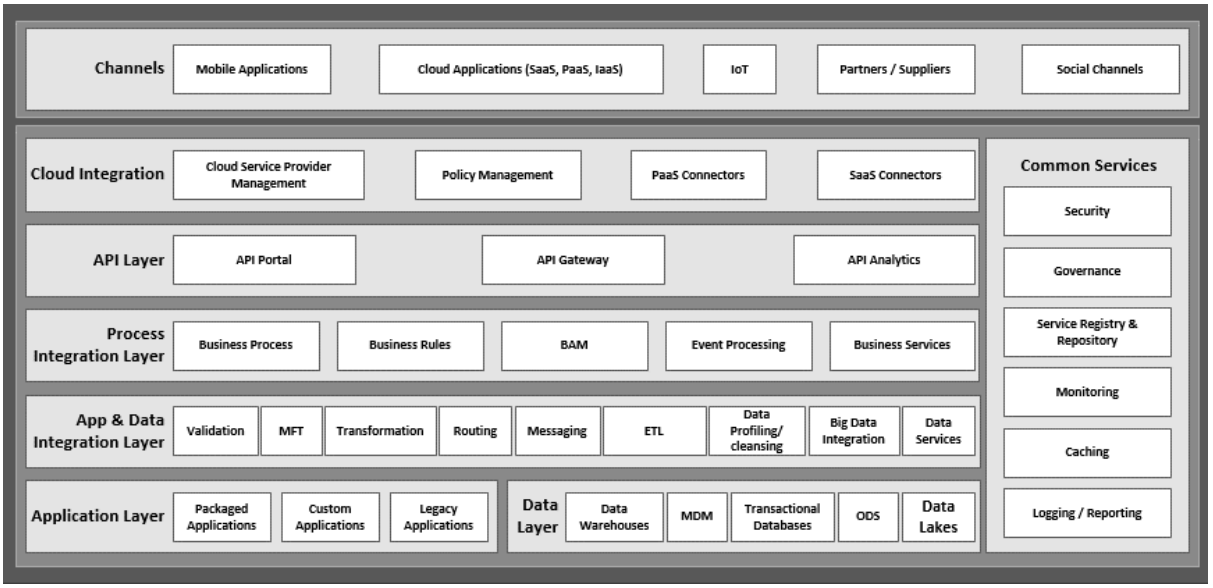


Figure 1: Reference Architecture of Integration Platform

API Layer (API Management)

An API (or a Service) is a business capability delivered over the internet to internal/ external consumers

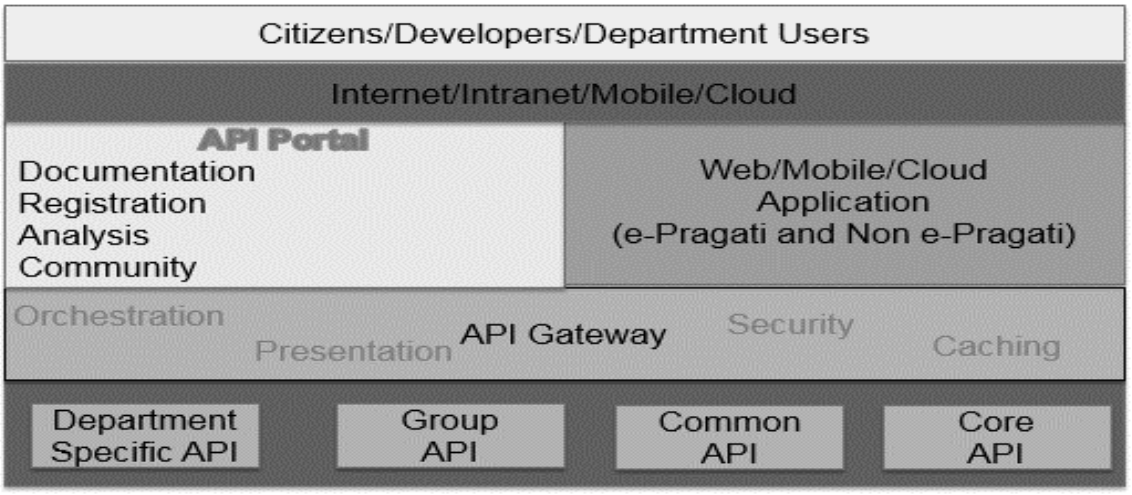
1. Network accessible function
2. Available using standard web protocols
3. Well defined Interface
4. Designed for access by third parties

Web API can be defined as any software interface exposed over the HTTP protocol in order to facilitate the development of Web, mobile and cloud application. API is not a new concept. But as the complexity of computer systems has increased, the need for APIs has increased.

API Layer (API Management) architecture components should minimally consists of API Portal, API Gateway and API Analytics.

SI to design, develop and Implement the API Management Layer based on the indicative building blocks of Code Management, Mobile Management, Developer Account, Environment, Support, Documentation, Deployment, Authentication, Legal, Monetization and Legal.

API Layer Logical View



Objectives

1. Single stop shop of all the API from various departments will be made available to publish and use.
2. Management of API through a centralized gateway.
3. Monitoring and tracking
4. Analysis of API

API Gateway

The core component of a full-featured API Management solution is an API Gateway. This is a networking appliance (either hardware or virtual) that acts as a proxy so that APIs do not have to directly interact with client applications. The Gateway represents a central point where all the abstracted API functionality is located and managed via a set NLP Marine governance policy

Functional Requirements

1. Provides a lightweight API gateway for securing and managing APIs
2. Connects mobile devices to brown filed and green filed enterprise systems
3. Significantly lowers integration costs, decreases total cost of ownership
4. Should leverage integration with NLP Marine identity and access management platforms
5. Should Streamline regulatory compliance through authentication, authorization, and audit capabilities

API Portal

While Gateways cover most of the technical features needed for layered API architecture, additional functionality is required to make the APIs themselves user-friendly for developers. This will normally involve integrating a Web-based API Portal into the Gateway, through which developers can register for APIs, access educational resources and monitor app/API performance

Portal enable developers to get started in minutes with an easy-to-navigate portal that surfaces interactive docs, tutorials, code snippets and examples. The API Portal takes the guesswork out of onboarding developers and provides a best-practices framework for rapidly delivering the tools they need to successfully use your API.

1. Web API

API that exposes backend systems over the Web, using the HTTP protocol, specifically to facilitate the creation of Web, mobile and cloud applications of NLP Marine

2. API Management

Ensuring that APIs perform consistently and do not impact the security or performance of the backend systems they expose

3. API Publisher

An organization that uses APIs to expose its backend systems to internal, partner or third-party developers of client applications

4. API Design/API Architecture

Developing and implementing application programming interfaces in order to expose backend data and application functionality for reuse in new applications.

5. Client Application

An application (including but not limited to Web, mobile and cloud apps) that relies on data and functionality accessed via APIs

3 ScopeofWork

The scope of work for the BIDDER includes implementation of the NLP-Marine systems for IPA. PCS 1x will be bootstrapped for enhancement and implementation of Nation Logistics Portal – Marine as per directives. Refer Annexure I , Annexure III , Annexure VI , Annexure VII, Annexure VIII for information details of PCS 1x.

3.1 Scope Overview

The scope of work for the SI includes implementation of the NLP-Marine system for IPA. The scope includes:

#	Category	Scope of Work
1	Development and Commissioning of National Logistics Portal (Marine)	System Requirement Study Solution Analysis & Design Solution Development NLP Marine integration with other applications Development of Mobile App Analytics and Business Intelligence API Gateway Services User Acceptance testing Solution Documentation Go-live
2	Cloud Provisioning and 3rd Party Security Audit	NLP Marine Estimates Cloud Computing Size – DC / DR Establishment of Network Connectivity Deployment and commissioning of requisite Hardware /Network Infrastructure components at Cloud for DC/ DR 3rd Party Security Audit and Certification
3	Operation & Maintenance of NLP Marine	Application Support & Maintenance Cloud Infrastructure Maintenance Technology Upgrade /Refresh User Profiles and Account Management IT Infrastructure Asset Management Information Security Services
4	Setting up & management of helpdesk	Call Centre for help desk service

5	Training, Capacity Building & Onboarding of Stakeholders	Transition Management/Change Management and Capacity Building Planning and execution of trainings Road Shows and Events to Onboard Stakeholders

- Study the application architecture and systems architecture of the existing PCS 1x platform and propose a suitable cloud environment as per guidelines of the Government of India and as per requirements of IPA.
- Prepare a cloud upgradation roadmap for PCS 1x and implement the same. The cloud solution should meet the following criteria:
    - The Infrastructure layer will provide the underlying basis for hosting, connectivity and provisioning of all components:
        - **Connectivity -** Connectivity services enable highly available, redundant and scalable connections via existing WAN (FedNet). They further enable secure connection mechanisms for trusted external parties via VPN andDMZ
        - **Hosting -** Multi-tenant hosting architectures support shared hosting, Co-Location and virtualization. Disaster Recovery and back up services provide uninterrupted access to systems andinfrastructure
        - **Provisioning -** Automated and consistent (template-based) provisioning of users, servers and services. Reliable and transparent metering and service usage monitoring used for billing or performancemeasuring
        - **Storage -** Storage services should provide highly available, redundant and scalable storagecapabilities
    - Facilitate for seamless upgradation of the existing Application hosting at MeitY Certified Cloud Service provider with DR capabilities as per the mutual understanding with IPA on SLA and deliverables on various aspects of Uptime of Infrastructure, Application, Connectivity, Information Security & Compliance, etc.; as per the implementation guidelines of the incumbent solution provider of PCS 1x solution.
    - Bandwidth guidelines for access of the PCS 1x application for locations of IPA to the chosen MeitY Certified Cloud Service provider.
    - IPA will have complete ownership and will transact directly with the MeitY Certified Cloud Solution provider while the Service Provider will facilitate the management of the solution. Solution provider to propose the optimum model for rules of engagement and ownership to IPA.
    - Solution should have Onsite and Offsite proper backup mechanism with a mechanism for restoring data to check the backup consistency as per the mutual understanding with IPA on SLA.
    - Solution should be able to meet RPO (Recovery Point Objective) i.e. acceptable Data Loss and RTO (Recovery Time Objective) i.e. time to bring back system defined in SLA.
    - All services and licenses procurement will be proposed by successful bidder and responsibility of procurement and cost shall rest with IPA, who will be the owner.
- Create an application support and maintenance strategy and implementation of the same as per the SLAs agreed to with the IPA. The support activities should meet the following criteria:
    - Facilitate for the maintenance and support – L1, L2 and L3 support for the Application as per the mutual understanding with IPA on desired SLA.
    - Facilitate for localization 24x7 Ticket logging support with proactive monitoring of hosted infrastructure on the MeitY Certified Cloud Solution.
    - Facilitate for seamless application of Firmware upgrades, Hot fixes and updates on hosted Infrastructure/ Application; as per the implementation guidelines of the incumbent solution provider of PCS 1x solution.
- Study the existing Port Community System (PCS 1x) and conduct business process discovery on the implemented platform.
- The system should be capable of integrating multiple service platforms integrated with each other.
- To undertake a detailed assessment of the functional and technical requirements for the NLP Marine project based on but not limited to the information provided in this document

- Prepare a Business Requirements Specification (BRS) document identifying the list of processes that are proposed to be modified due to the proposed NLP Marine; their existing flow (AS IS) and the recommended proposed flow (TO BE) to incorporate NLP Marine.
- To detail out all the Business process functional requirements (TO BE Process) for the NLP Marine project including portal and document it as part of the Software requirement specifications (SRS)
- Prepare brief functionality listing of the TO BE process categories as per the type of the functionality
- Create a Business Requirement Specification (BRS) document, to encapsulate the functionality of the proposed value add solution. The value-add solution should meet the following criteria:
    - Value added solution shall utilize data provided by/ derived from PCS 1x system.
    - Solution should adopt Auto filling/ Population of data to eliminate duplication and multiple entries by various stakeholders.
    - Solution should link data among various stakeholders with quick response mechanism.
    - Solution provider to maintain the data security by encryption and decryption the data.
    - Solution should eliminate the dependency on multiple data entries by bringing in more efficiency through automation.
    - Solution to enable access independent of form factor of devices and operating system there by increasing the level of accessibility for customers to seamlessly connect and interact from anywhere, anytime, securely making it a valuable tool for the modern business
    - Solution should provide payment tracking and payment-transaction mapping.
    - Solution should have centralized identity management for all defined users.
    - Solution should facilitate seamless exchange of information/ data in multiple formats and in electronic form.
    - Solution should be capable of integration with external modules as available in market or which can be envisage in future so that the stakeholders can be benefited.
    - Solution shall cater to industry standards of quality and information security with certifications like ISO 27001 and ISO 9001
    - Solution should adhere to Government mandated accessibility standards such as W3C Markup Validation Service.
    - Solution should provide Decision Support Tools to all stakeholders.
    - Solution should have the ability to provide end users to search for their relevant system information of various categories and types in a simplistic manner.
    - Solution to be capable enough to handle integration with existing PCS 1x. Solution provider is expected to extend handholding services to stakeholders for integration of their internal systems with the proposed value add solution.
    - Solution should provide Notifications in the form of SMS, Email, WhatsApp and In App Notifications.
    - Solution should have the capability of providing Invoicing to the users of value-added solutions in multiple formats and against multiple parameters related to the transaction.
    - Solution should have the capability to automate capture of data.
    - Solution is expected to be leverage a reliable, scalable and flexible infrastructure to cater the on-demand requests as per customers Business Continuity Plan guidelines
    - Solution provider is expected to provide infrastructure hosting on partners approved by Ministry of Electronics and Information Technology.
    - Solution provider is expected to carry out end user training in the following:
        - Training Workshops for Application users (Train the Trainer concept)
        - Workshop for customer IT Team
        - User Standard Operating Procedure (SOP) documents
        - Video SOP
        - Tool Tip with the guidelines
        - Mockup Presentations
- Solution provider should provide SLA based (response and resolution) support as per the following:
    - Ticketing System for capturing incident and record of closure
    - Location-wise On-site resources for L1 & L2 Support

- Off-Site resources for L3 and above

- To prepare Data Analysis report that captures the data points required from the PCS 1x platform for value-add solution to function as desired.
- To prepare design strategy that eases use of value-add system (user experience; user interface).
- To prepare a reporting/ dashboarding application design strategy for various stakeholders.
- To prepare a Notifications and Alerts strategy for event-based triggers on key transactions.
- To prepare mobile application strategy.
- Providing relevant documentation for the value-add solution.
- Provide training to various stakeholders on a “train-the-trainer” basis.
- Set up a central 24/7 helpdesk with locational support as per SLA
- Provision for users of NLP Marine to make use of DSC
- Provide value added services which will benefit the users of NLP Marine; such as Bidding Module, Chat Bot
- Integration with ERP / Latch-ons via API Gateway as per the Latch On Services agreement signed between IPA and Latch On Service Provider
    - It is expected that the communication of the MOCI, GOI system with external interface will happen through an API layer. An API gateway should be used to manage the API communication with the external interfaces.
    - All data transfer to happen through APIs, File transfer mechanism is not encouraged
    - App signature authentication will be through the license key + time stamp + app version and other Meta Data
    - All the APIs would be stateless in nature, thus easy to load balance, even if hit through portal is very high and this requires high end processing.
    - The API Platform should be allowed to manage all your enterprise initiatives from a single solution.
    - The API platform should support existing APIs and developer preferences and provide the following transformations and developer preferences.
    - The API Platform should provide clustering and ensure reliability, scalability and single point of administration.
    - The API Platform should provide for enterprise grade encryption
    - The API platform should provide secure access to all APIs and provide ALL the forms of authentication, access control and certificate/credential support.
    - The API platform should provide comprehensive threat protection for all API traffic.
- Implementation and Onboarding of stakeholders conduct road shows and events.
- Bidder has to consider both the options for on-boarding PGAs through SWIFT as a latch-on or individual API integration with PGAs shall be incorporated in the tender.
- The system has to provide a centralized intelligent electronic message switching facility to exchange messages in XML, UNEDIFACT and proprietary standards in multiple protocols to and from members of maritime community.
- The bidder has to provide EDI engine system software for seamless translation from one format to another format using translation service
- Bidder is expected to market NLP-Marine in order to onboard maximum number of stakeholders so that all the transaction envisaged under NLP-Marine are carried out through the system. The success of this could also result in incentivisation of the bidder, which would be decided by IPA at a later stage.
- IPA, post 2 years of Go-Live, could get into an agreement with the bidder basis the per transaction fees for the customer on an agreed revenue sharing model as agreed by both the parties.
- When NLP-Marine is integrated with latch-on application, no charges shall be collected from the latch-on partner initially for 2 years. IPA would get into an agreement with the Latch-on partner as per the **Annexure IX**
- Indicative list of Latch-on functionalitiesis given in **Annexure VII**. The bidder needs to estimate based on 50 Latch-on applications for the commercials as part of this scope of work in the RFP. However, if during implementation it is realised that a functionality is not being integrated as a latch-on and is made available through API integration, then the bidder shall be paid as per the discovered unit rate per API integration.

- Additionally, if the bidder, during the project duration, plans to integrate latch-on applications beyond 50, then the bidder will be paid on actuals. For additional latch-on applications, beyond 50, the bidder can raise a single invoice for all the additional latch-on applications.

3.2 Scope for Implementation

The successful bidder needs to smoothly implement the project pan India. NLP Marine consists of many interrelated and interdependent, integrated or interfaced information systems that together form it

Information systems of the participating stakeholders provide the automation of business processes and data to fulfil the business objective of the Government agency or Private Sector organization. For the purpose of theNLP Marine implementation, it is assumed that these systems already exist. And stakeholders are at ease of operating these systems.

During Implementation of the NLP Marine it is recommended to have the sample users from each stakeholder type - to create specific requirements of each type of stakeholder. It is required to identify and ensure availability of these resources is crucial part of successful implementation of NLP Marine.

- Create and submit detailed implementation plan with timelines for the above set scope -- change management strategies and communications plans should be holistic in their scope and coverage
- Mobilization and indoctrination of stakeholders
- conduct the early customer engagement surveys and understand the pain points and requirements for better gap analysis
- Set mechanism for customer feedbacks and suggestions while maintaining records and implementation timelines as per SLAs –
- Build the ability to analyse and address incoming inputs under the governance
- Create viral and revolutionizing plan including all media
- Implementation oversight with accomplishment Tracker
- Prepare the progress reports of implementation in coordination with all relevant bodies
- change management plan needs to complement the implementation plan
- Request and release of necessary trade notices through appropriate channels and observe reach and awareness
- Supplement with aggressive media campaigns
- Creation of content for Training, customer engagement, media coverage and customer interactions: Preparing artefacts and customized value benefit demonstrations; Success stories and testimonials as a medium of building trust among various users
- Handle user presentations, demos, onboarding, user training, roadshows, etc. and generate reports on customer feedback and change requests.

Responsibilities of the Successful Bidder:

- Direct responsibility for creation/approval of training material, customer engagement material, media coverage, customer interaction plans and progress report of implementation as well as raise issues needing resolution.
- Customer engagement plans driven along with various APEX bodies
- Provide necessary onboarding support, training and encouragement to those who need it.
- Be persistent – maintain progress and continue momentum.
- When the change has been implemented continue to articulate the relationship between new behaviours and organizational success.

Meetings

- Quarterly review meetings of the successful bidder, trade representatives along with senior Ministry officials will be conducted to get additional approvals, support and handle roadblocks that may appear.
- Successful bidder along with other APEX bodies will hold accountability for adoption and be empowered to achieve it.

NLP Marine Training and Support: 24x7 Support

- For streamlined operations NLP Marine will formulate the 24x7 support centre.
- NLP Marine will provide full application support with strict SLAs.
- Provision of Interactive agent(s)

3.3 Other Key Requirements

This section details the NLP Marine requirement and details requirement of sizing of NLP marine refer **Annexure VIII**

The implementation of NLP Marine is envisaged as a phased approach, as described below:

3.3.1 Cargo and Carrier Platform

S. N.	Service	Sub types/ processes
Exporter, Importer		
1	Route Planning	Route options for selected origin destination pair Estimated time calculation for different options Estimate cost calculation
2	Vendor management List	Maintain list of preferred vendors Check Vendor Information including GSTN, certifications, contact details, associations, number of trips completed, ratings, reviews etc.
3	Less than container load or less than truck load booking services	Consolidation of load to be done via freight forwarders
4	Regulatory information submission and bill generation exchange	E-way bill generation Exchange of e-bill of lading Exchange of virtual contract documents Exchange of e-invoice Exchange of booking note from shipping line
5	Shipping bill generation	Submit form, upload document, download shipping bill
6	Booking of freight forwarder	Cargo related services
7	Booking of Warehousing services	Cargo Specific Warehousing Module
8	Booking of packaging services	Cargo Specific Packaging Services
9	Tracking	Tracking of goods and compliance
10	Payment services	Online payment services
11	Grievance redressal	Query submission, processing and tracking
12	MIS	User based dashboards to view trade statistics
Domestic trader		

S. N.	Service	Sub types/ processes
1	Route Planning	Route options for selected origin destination pair Estimated time calculation and cost calculation
2	Vendor list Management	Maintain list of preferred vendors Check Vendor Information including GSTN, certifications, contact details, associations, number of trips completed, ratings, reviews etc.
2	Less than container load or less than truck load booking services	Consolidation of load to be done via freight forwarders
4	Regulatory information submission and bill generation and exchange	E-way bill generation Exchange of virtual contract documents Exchange of e-invoice
5	Booking of freight forwarder for full service	Door to door service
6	Booking of Warehousing services	Warehouse price check and booking from marketplace
7	Booking of packaging services	Packaging services booking from marketplace
8	Review and rating	Ratings and reviews of different service providers
9	Tracking	Tracking of goods and compliance
10	Payment services	Online payment services
11	Grievance Redressal	Query submission, processing and tracking
12	MIS	User based dashboards to view trade statistics
Truck Operator		
1	Track and Trace	Sharing of shipment movement and delivery status Distance and route planning through map integration
2	Invoice Generation	Invoice Generation Invoice Sharing
3	MIS	User based Activity Dashboard
4	Grievance Redressal	Query submission, processing and tracking
Shipping Lines/agent/ Container , NVOCC operators		
1	Allot Container	Post survey and container allotment request with container depot
2	Document generation and sharing	Exchange of invoice Receipt of shipper's documents Sharing Form 11, Form 13 with CHA/ exporter/ FF Electronic sharing of TP1, TP2 for inland transport of import with ICD Sharing electronic Master Bill of Lading with the exporter (if applicable)
3	Track and Trace	Sharing of shipment movement and delivery status
4	MIS	User based Activity Dashboard
5	Grievance Redressal	Query submission, processing and tracking
Container Freight Stations , Inland Container Depot		
1	Track and Trace	Sharing of shipment movement and delivery status
2	MIS	User based Activity Dashboard
3	Grievance Redressal	Query submission, processing and tracking
Empty Container Depot		
1	Accept Allotment request	Accept allotment request
2	Track and Trace	Sharing of shipment status movement and delivery
3	MIS	User based Activity Dashboard
4	Grievance Redressal	Query submission, processing and tracking
Truck aggregators/ 3PL/ 4PL		
1	Track and Trace	Sharing of shipment status Distance and route integration movement planning and delivery through map
2	Invoice Generation	Invoice Generation Invoice Sharing
3	MIS	User based Activity Dashboard
4	Grievance Redressal	Query submission, processing and tracking
Railway Custodian (long term objective)		

S. N.	Service	Sub types/ processes
1	Respond request to service	Accept booking request from shipper/exporter/ importer Sharing electronic Contract between stakeholders Request for mandatory document sharing
2	Document exchange	Receipt of shipper's document Exchange of Equipment Interchange Report Exchange of Railway Receipt
3	Track and Trace	Sharing status of shipment movement and delivery
4	MIS	User based Activity Dashboard
5	Grievance Redressal	Query submission, processing and tracking
Warehouses		
1	Track and Trace	Sharing of shipment status Distance and route integration movement planning and delivery through map
2	Invoice Generation	Invoice Generation Invoice Sharing
3	MIS	User based Activity Dashboard
4	Grievance Redressal	Query submission, processing and tracking
Packaging Owner		
1	Invoice Generation	Invoice Generation Invoice Sharing
2	MIS	User based Activity Dashboard
3	Grievance Redressal	Query submission, processing and tracking

3.3.2 Finance and Insurance Platform

Selected features of banking and financial services are expected to be added in the NLP Marine.

S. No	Service	Sub types/ processes
Exporter/ Importer/ Domestic Trader		
1	Price discovery of insurance service	Price discovery of insuranceservice Relevant information submission for selected insurance service
2	Requesting banks for Letter of Credit fromlist	Listing of banks providing Letter of Credit, along with local contactdetails
1	Insurance and Trade Finance Module	Selection of service provider for obtaining the Letter of Credit and/or other relevant documents
2	Document sharing for authentication	Dispatch documents generated as available in digilocker shall be shared with bank for document authentication and initiation of payment process
3	E-PBG and E-EMD	Integration with banks to enable acceptance of Electronic Performance Bank Guarantee and Electronic Earnest Money Deposit from LSPs, as per contractualrequirements

Scope Limitation

NLP Marine shall not integrate itself with the process of issuance of Letter of Credit. For the issuance of such LOC, banks require significant due diligence including financial check of the trader, checks on credit rating and existing relationships among many other aspects. It is envisaged that traders trading through NLP Marine shall complete these processes through the current banking channels. However, banks and users shall use NLP Marine for dispatch document sharing to help ease authentication process.

3.3.3 Regulatory Bodies and PGAs platform

The regulatory platform planned under the proposed national logistics portal plans to ensure submission of generated certification documents to the ICEGATE for regulatory compliance of the consignment and generation of the Let Export Order.
Various services proposed in this module is detailed in below table.

S. No	Compliance Service	Sub types/ processes
Exporter and importer		
1	Listing compulsory compliance requirement	Compulsory compliance requirement for origin/destination and product pair
2	Interface with ICEGATE for submission of Certificates / NoC/ Authorisation	Compulsory compliance document submission
3	Track and Trace	Mobile and web based notification Visibility of ETA for different clearance milestones.

Scope Limitation

- NLP Marine shall only exchange messages with ICEGATE and SWIFT systems and shall not influence or alter the internal process of these systems.
- The data exchange will be in the form of API (preferable) and / or XML based Web Services.

3.3.4 Integration with PGAs/EPCs

OfflinePGAs/EPCs:

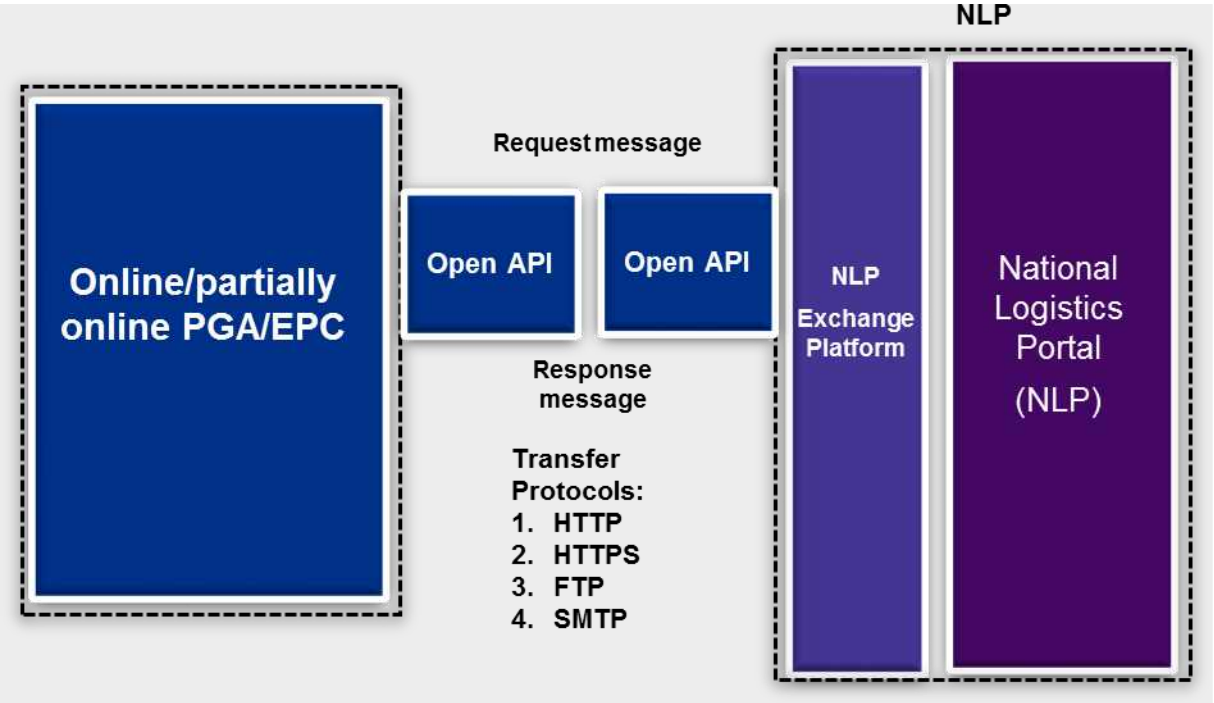
The EPCs/PGAs that works on physical certification process. As a result, integration with such organizations can be facilitated by the development of a new module in the system. Users can authenticate themselves using individual IDs and passwords, after which the system provides them with the required services such as capturing and uploading of documents. The interaction with NLP MARINE will happen via NLP MARINE Exchange platform

3.3.5 Online/ partially online PGAs/EPCs and other agencies

TheapproachusedinthiscasecanbethatofanopenAPItointegrateexistingportalswith NLP MARINE. The open API can be JSON based if it is a service-oriented portal and/or XML-based in case it is a object-oriented portal. The application package interface can facilitate two-way communication over one of the popular, widely accepted protocols from: HTTP, HTTPS, SMTP,FTP.

However, with this approach there are two major factors which have to be ensured:

a) ProperdocumentationfortheOpen APIintegration,alongwithitslimitations
b) Messageformatshavetobedefinedclearlysothatparsing,andvalidationis easy



TheNLP MARINEintegrationwithotheragenciessuchasACCS,DLDSystembyDMIDC,Certification ofOriginsystembyExportInspectionCouncil(EIC)shallbeconsideredwhilepreparationof SRS document by the implementationagency

3.3.6 CertificationsPlatform

The certification platform planned under the proposed national logistics portal plans to consolidate process of applying and tracking various certification requirements required for EXIM trade of commodities. Currently the concerned agencies can be broadly classified into four major subheads:

- PGAs which are currently **integrated withSWIFT**
- PGAs/ EPCs which are not integrated with SWIFT, but have their own **onlinesystem**
- PGAs/ EPCs which have **partial onlinesystem**
- PGAs/ EPCs which **do not have online system** and deal only in physical documents exchanges

On account of various operational challenges and multiplicity of agencies involved, the process is extremely complex. To streamline and ease the process, the proposed platform plans to incorporate certification application through common application form based on system identified mandatory certification requirement. Subsequent to filing of common application format by the trader, customized application forms can be generated by the system as per individual certification field requirements for the submission.

Various services proposed in this module is detailed in below table:

S. No	Certification Service	Sub types/ processes
Exporter and importer		
1	Listing compulsory certification requirement	Compulsory certification requirement for origin/destination and product pair
2	Online certification system	Common Application Form for all certificates Obtainingcertificates/ license/ authorization from the concerned PGA/ EPC
3	Track and Trace	Mobile and web based notification Visibility of ETA for different certifications

4	Payment Module	Payments for certificates
5	Integrated Regulatory Module	Integration with customs and services

Scope Limitation

- NLP Marine shall only feed and access information to and from EPC and PGA systems and shall not influence or alter the internal process of these bodies. Certain bodies which do not have online systems, NLP Marine shall create the required interface.

The NLP Marine platform is divided on the basis of four components:

- Cargo Services Platform
- Carrier Services Platform
- Finance and Insurance Platform
- Regulatory Bodies and PGA's Services Platform

Please note: The NLP Platform shall be multi-lingual i.e. shall support both Hindi and English language. The system modules are mapped with respective business services below:

Additionally latch-on modules to be provided which can work as plug-n-play. These modules can work independently as well as work as integral part of the NLP Marine

Digital Document Exchange

- Solution to provide functionality and capability to store and manage different types of documents which will be backed by reading and generating capabilities of digital codes such as QR / RFID / Barcode etc.
- The service provider to provide a latch-on product inclusive of necessary hardware requisite tools for Scanning of RDIF, QR etc with readable capacity.
- The cost to provide same is exclusive of the quote to be submitted.
- The stakeholder needs to ensure that service provider of this project to be one of the vendor in selection criteria.
- The stakeholder is required to have fair selection process so as to engage vendor for hardware and installation

Scope

- To provide services related to document / information exchange via:
    - QR Code Scanning
    - Barcode Scanning
    - RFID Scanning
    - OCR Functionality
    - QR Code Generation
    - Digital Signing Tool
- Integration with Hardware used at different locations for extraction of data from digital medium
- Integration with official sources of data to capture / validate the information available on NLP Marine
- Systems readiness for displaying information captured from documents share by Customs in digital format
- To introduce workflow enhancement for Custodians to bring efficiency in Gate Process
- To provide authenticated data to the concern stakeholders as per requirement
- To verify details with official sources of information such as (DGFT, EPCs, Digi-Locker etc)
- To provide document repository for storage of digital documents
- Additionally latch-on modules to be provided which can work as plug-n-play. These modules can work independently as well as work as integral part of the NLP Marine. The list of existing Latch-on system is attached in Annexure VII

S. No.	Module Name	Mapping with Services
1	Digital Document Exchange	QR Code Scanning Barcode Scanning RFID Scanning OCR Functionality QR Code Generation Document Management System Digital Signing Tool Integration with Authorised Data providers (such as DGFT for IEC, e-Vahan for Vehicle Details)

3.3.7 Software Components – NLP Marine

- The bidder may acquaint them self to the existing functions of the software components of PCS 1x and along with their detailed description for their reference before bidding from the IT Department of IPA.
- The IT department of IPA will ensure that the incumbent service provider will transfer all the documents along with the source code and certify Go Live status of each module.
- The "Policy on Collaborative Application Development by Opening the Source Code of Government Applications", notified by Ministry of Electronic and Information Technology, Government of India, in the Gazette of India on 6thMay 2015, must be adhered.
- The proposed NLP Marine shall have the functionality and features such as message transmission, message translation, authentication and authorization, single sign-on, communication gateway, customer management system (CMS) & component of event handler. The data transacted by stakeholders must be through DDx module of NLP Marine.
- CMS and other features shall include;
    - Role-resource based authorization including 2F authentication
    - Password end to end encryption
    - UI/API mode of integration
    - Configurable and flexible password policy
    - SSO
    - UI for password reset
    - Compatibility with all popular open source OS, middle tier and DB software
    - Prompt for Password change upon first login
    - Locked Account after multiple failed attempts (configurable)
    - Enforce periodic changing of passwords (configurable)
    - Maintain password history (configurable)
    - Flexibility to choose password complexity (simple/medium)
    - Passwords encryption in database
    - Flexibility to choose user commencement date

- The bidder needs to mention the software and hardware specifications required for DDx module exclusively.
- The stakeholders shall strictly adhere to the specifications provided by the bidder only through the requisite exclusive hardware and software.

3.3.8 Master Data Management

System should not allow database / system administrators to make any changes to data. It should ensure that the data and file (data at rest) that is kept in the systems has tamper resistance capacity and source of truth (original data

of cargo movement) could be used to reconstruct derived data such as ledgers and system generated returns. System should be able to detect any data tampering through matching of hash value and should be able to reconstruct the truth.

3.3.9 Business Intelligence and Data Analytics

For Maritime Trade, a Port/Terminal Operations accumulates huge amount of data such as terminal berthing, vessel sailing arrangements and actual arrival/sail out of cargo vessels, scheduling information on road and rail transport, categories and destinations of Import & Export goods, transportation routes, etc. The volume of this data would increase manifolds in foreseeable future, with contributing factors such as adoption of leading technologies such as IoT, RFID and sensors capturing the operational level data; growing integration with hinterland transport; integration with industries such as Insurance, Manufacturing, etc

This data may be structured, semi structured or unstructured. The data footprint is generated across various ports, terminals and is fragmented among multiple stake holders. The potential value of the data lies in the attempt made to synthesize and collate the information, identify patterns in the data, and reference such insights to facilitate trade related decision making.

Data thus acquired from this complete supply chain of Maritime Trade, may need to be further complemented with external data sources such as Manufacturing, Weather, Spatial Geography, etc. Such data, may be used for smart decision making, such as:

- Connected Port Planning
- Multimodal Transportation Planning, entry and exit of trucks, rail at the Port Yards
- Optimization of transport routes for container trucks
- Scenario Analysis and decision making based on different logistics plan
- Early warning for loading/unloading, and transport of dangerous goods
- Consolidation services for cargo shipments
- Regional consumer demand preferences and category prediction for Import/Export goods
- Predictive Asset Management
- Insurance Industry Integration: Personalized insurance products
- Dwell Time monitoring related to Import & Export

The MSP should ensure that the NLP-Marine system shall provide a facility for generating and viewing online, real-time project and MIS reports for transactions handled during a specified period, transaction density trends for any specified periodicity (hourly, daily, weekly, monthly) and any bottleneck situation creating dependency at any stage. The Reporting functionalities shall be an integrated system which shall provide user-friendly reporting functionalities.

3.3.10 Cloud Services

It is expected by IPA that the bidder who qualify to provide clouds services will also comply with the mandatory information security requirements applicable for cloud deployment models of “MeitY’s “Provisional Empanelment of Cloud Service Offerings of Cloud Service providers (CSPs)”.

Annexure II refers to detail of functionality desired in NLP Marine

3.3.11 Mobile application

- As part from application development, BIDDER shall also develop a mobile app for both internal and external users of MOCI, GOI
- The BIDDER shall study the requirements for the development of mobile app in consultation with MOCI, GOI
- The BIDDER shall design, develop, test and deploy the mobile app on cloud for MOCI, GOI
- The GUI of the mobile app should be user friendly and compatible on all latest and 3 versions below of Android and IOS platform
- Mobile app for the respective platforms must be hosted at their official platforms namely Apple app store and Android play store and should be downloadable from official platforms only
- The mobile apps shall not be hosted or mirrored elsewhere
- There should be minimum use flash contents so that home page should be loaded quickly
- The BIDDER shall design, develop, test and host at platforms including approval by platform owner and updates
- The BIDDER shall be responsible for regular updates and modifications to the mobile app for individual platform
- The mobile app shall be provided free of cost at platforms and should be clearly highlighted as official app of MOCI, GOI
- Mobile app should have separate GUI for internal and external users and should provide Role Based Access control and should allow importers/ exporters and internal users of MOCI, GOI to register on mobile app to avail the services based on their access rights

3.3.12 API management and usage

- Data exchange between the MOCI, GOI System and other Internal/External Systems will be carried out through APIs. The SI, in consultation with the MOCI, GOI, will also be required to set up a process for issuance of standards for the MOCI, GOI System APIs as well as for other systems APIs
- The SI needs to set up, operationalize and maintain system for APIs
- Since other systems may transmit data in CSV/other format; the SI would build a converter/adapter to convert XML into the desired format or vice versa. The convertor/adapter will reside in the MOCI, GOI system environment and will parse the data as and when received. A utility will also need to be built to push or pull information to or from the other departmental systems based on event triggers. The exchange of information with other departments shall be real-time information exchange. In case of no feasibility of real-time information exchange, batch exchange of data may be used on a transactional basis. The utility should reside in the NLP Marine environment may reside both in the department environment as well as in the MOCI, GOI environment based on requirement for data exchange and feasibility to change in department side application.
- API Gateway Services
    - It is expected that the communication of the MOCI, GOI system with external interface will happen through an API layer. An API gateway should be used to manage the API communication with the external interfaces.
    - All data transfer to happen through APIs, File transfer mechanism is not encourage
    - App signature authentication will be through the license key + time stamp + app version and other meta data
    - All the APIs would be stateless in nature, thus easy to load balance, even if hit through portal is very high and this requires high end processing.
    - The API Platform should be allowed to manage all enterprise initiatives from a single solution:

- The API platform should support existing APIs and developer preferences and provide the following transformations: and developer preferences
- The API Platform should provide clustering and ensure reliability, scalability and single point of administration:
- The API Platform should provide for enterprise grade encryption:
- The API platform should provide secure access to all APIs and provide ALL the following forms of authentication, access control and certificate/credential support:
- The API platform should provide comprehensive threat protection for all API traffic.

3.3.13 Solution Testing

1. The BIDDER shall carry out its testing process as per the Quality Assurance Plan and testing strategy (including test plan and test cases) prepared and provided by it as per Solution Analysis & Design stage. The objective of testing is to ensure that the entire system in totality, including all hardware, software and human components, which are part of this project, perform as per the objectives laid down in this document. The software solution testing shall include (but not limited to) the following activities:

- The BIDDER shall perform the testing of the solution based on the approved test plan and criteria; document the test results and fix the bugs found during testing.
- The application shall have to undergo comprehensive testing and must minimally include Unit Testing, System Testing, Integration Testing, Performance Testing, Regression Testing (in case of any change in the software), VAPT and Load & Stress testing.
- The testing of the application system shall include all components vis-à-vis the functional, operational, performance and security requirements of the project, as mentioned in this document.

2. Though the IPA is required to provide the formal approval for the test plan, it is ultimately the responsibility of the BIDDER to ensure that the end product delivered meets all the requirements specified in this document and the signed off SRS. The responsibility of testing the system shall therefore lie with the BIDDER.

3. The BIDDER shall create a staging area and ensure that all the application software upgrades/releases are appropriately tested in the staging area and are applied on live instance only after such comprehensive testing. Any downtime/system outage for Application system caused by applying such patches shall be attributed to the BIDDER as system downtime and shall attract penalties as per SLA.

3.3.14 Audit

1. Bidder shall engage a CERT-In empanelled third-party agency for conducting Audit prior to Go-Live of each phase of the project or major change of Information technologyinfrastructure.
2. Security Audit shall include penetration testing, vulnerability assessment, application security assessment, web security testing and implementation of information security controls.
3. IPA may also hire a third-party auditor to conduct security audit, and in such scenario, Bidder shall provide full access andsupport.
4. Half-yearly penetration testing and web applications security assessment (both authenticated and unauthenticated scans) shall be conducted by third party agency and security certificate stating that the application is free from all the vulnerabilities shall be submitted to IPA management in every sixmonths.

3.4 Full Functional Scope

NLP MARINESYSTEM

The functional requirement specification (FRS) provides the details of the functional requirements for the NLP MARINE platform. The FRS for the NLP MARINE platform is divided on the basis of four components:

1) Carrier and Cargo Services
2) Single window certificationsystem

3) Integrated Regulatory Platform
4) Banking and InsurancePlatform

Single windowcertification:

S. No.	Module Name	Mapping with Services
1	Listing Module	• Information about the list of certificates, supporting documents, estimated time etc. on the basis of commodities, source location, destination locationetc.
2	CommonApplication Form(CAF)Module	• Apply forcertification • Upload supportingdocuments
3	Payment Module	• Payments forcertificates
4	EPC/PGAInterface Module	• EPC/PGA simple interface for digitalenablement
5	Generated Certificates Module	• Receive and store generatedcertificates

Integrated RegulatoryPlatform

S. No.	Module Name	Mapping with Services
1	Integrated Regulatory Module	• Integration with customs andservices

Trade FinancePlatform

S. No.	Module Name	Mapping with Services
1	Insurance Module	• Price discovery of insurance service from different serviceprovider.
2	Trade Finance Module	• Selectionofserviceproviderforobtainingthe Letter of Credit and/or other relevant documents
3	Document Sharing Module	• Document exchange through NLP MARINE exchange platform
4	E-BG Module	• Online BankGuarantee

Thissectionpresentsthekeyandminimumfunctionalrequirementsspecificationsforthe National Logistics Portal(NLP MARINE)

3.4.1 Cargo and Carrier Services

List of services to be included in NLP-Marine as part of API based integration

S.No.	Type of Service	Service Description
1	Cargo/Container Services	NLP to provide functionality for Customs related filing at Customs server viz. Shipping Bill, Bill of entry, IGM etc.,
2	Shipping Line Services	Discharge report (discrepancies between manifested vs actual discharged)
3	Port Authorities	Updates in preferred Berth Allocation Request
4	Transport related services	Barge Planning Service: Service for pre-notifying barges (lighter agreements) and container cargo (discharge/loading lists) at terminals, including status feedback from the terminal.
5	Exit Summary Declaration (Export)	The Exit List is prepared by SA and submitted to Customs, for loading permission
6	Notification - Ships Stores	A declaration made by SL/SA to the Port/Customs on the vessel's store list.
7	Notification - Verified Gross Mass	Using a single gateway, notify shipping companies of the verified gross mass (VGM) of export containers.
8	Vessel Related Services	Harboring Services
9	Vessel Related Services	Freshwater Supply: Freshwater services consist of any fresh (sweet) water provided by the port to any vessel within the boundary of the port services area.
10	Regulatory Services	Regulatory inspection services for the PGAs
11	Request for examination of cargo before stuffing	The Exporter provides the shipment related details such as: Invoice, items of export, quantity, value, container allocated, net weight, gross weight, consignee/buyer name, port of discharge, gateway port, etc.
12	Port/Terminal Service	Approval for deposit in PD Account
13	Port/Terminal Service	Payment of deposit in PD Account
14	Port/Terminal Service	Confirmation of receipt of deposit in PD Account
15	Port/Terminal Service	Submission of Import Advance List
16	Port/Terminal Service	Final Tally Report for the Vessel
17	Port/Terminal Service	Request for Empty Container Movement
18	Port/Terminal Service	Gate Out of Empty Containers from CFS
19	Port/Terminal Service	Gate In of Empty Containers at ECY
20	Port/Terminal Service	Yard Plan
21	Port/Terminal Service	Daily Discharge Report
22	Port/Terminal Service	Ingress/Egress Permission – movement by barges
23	Port/Terminal Service	PDA Account adjustment for the CB/ Confirmation of receipt of charges
24	Port/Terminal Service	Cargo Gate-Out Permission
25	Port/Terminal Service	Delivery Permission for Bulk, Liquid or Break-bulk cargo

26	Port/Terminal Service	Permission for cargo for Customs Examination
27	Port/Terminal Service	Green Boat Note – permission for discharge by barges
28	Port/Terminal Service	Survey Report – Liquid/Dry Bulk
29	Port/Terminal Service	Mate Receipt of Export Cargo
30	Port/Terminal Service	Back To Town Permission
31	Port/Terminal Service	Request for Back to Town
32	Port/Terminal Service	Gate Pass for Back To Town
33	Regulatory Service	Request for Health Inspection (Form/Application)
34	Regulatory Service	Certificate of Inspection of Medicine, Medical Stores and Appliances
35	Regulatory Service	De-ratting Exemption Certificate

List of services to be included in NLP-Marine as part of Latch-on system/application

S.No.	Type of Service	Service Description
1	Cargo/Container Services	System integration for making payments like duty payments directly to ICEGATE system through NLP
2	Shipping Line Services	Slot Booking Requests for multiple agents, booking information & status
3	Shipping Line Services	Real time tracing of goods status and movements
4	Shipping Line Services	Collection of the B/L information entered by freight forwarders
5	Shipping Line Services	Waste disposal request & compliance
6	Terminal Operators/Ports related services	Engagement of Surveyor for Services
7	Notification - Waste Disposal	Service to report waste on board of a vessel to the Harbour Master
8	Vessel Related Services	Vessel Related Services workflow – Request, Response, Order, Service, Payment. • Tug • Water supply via boat • Pipeline water • Bunker via bunker boat • Bunker vie pipeline • Waste Disposal • Other Vessel related services
9	Vessel Related Services	Ship Maintenance & Repairing
10	Cargo/Container Related Services	Cargo / Container Documentation (Import): Authorize Delivery

	(Import)	After customs and carrier have authorized release After all port charges paid
11	Cargo/Container Related Services (Import)	Cargo / Container Documentation (Import): Transport Instruction (used only if Carrier Haulage mode): Freight forwarder issues instruction to carrier for delivery trucking requirement
12	Cargo/Container Related Services (Import)	Cargo / Container Documentation (Import): Container Storing order Instruct trucker to return empty container to depot after un stuffing
13	Cargo/Container Related Services (Export)	Cargo / Container Documentation (Export): Freight Booking: While placing a request for freight, the Shipper will provide details like the items of export, quantity, value, Net Weight, Gross Weight, Type of Packaging, Port of delivery, Consignee Details, etc.
14	Cargo/Container Related Services (Export)	Cargo / Container Documentation (Export): Freight Booking Confirmation: The response from the FF/SA, will include the allotment of containers and container numbers
15	Cargo/Container Related Services (Export)	Cargo / Container Documentation (Export): Container booking (confirmed) · Advance info for export loading · To be used as basis to create downstream documents
16	Cargo/Container Related Services (Export)	Cargo / Container Documentation (Export): Shipping note providing details of containers to be loaded onto the vessel.
17	Cargo/Container Related Services (Export)	Cargo / Container Documentation (Export): Shipping Agent Authorization for loading
18	Cargo/Container Related Services (Export)	Cargo / Container Documentation (Export): Authorize for Loading - After customs and carrier have authorized for loading
19	Cargo/Container Related Services (Export)	Cargo / Container Documentation (Export): Transport Instruction (used only if Carrier Haulage mode) Freight forwarder issues instruction to carrier for sending in containers to terminal
20	CFS sends indent to the Port / Terminal	CFS sends indent to the Port/Terminal
21	Providing shipment details to CHA by Importer/Exporter	Providing shipment details to CHA by Importer/Exporter for preparation of customs declaration - Invoice, Packing List, license details, exchange rate, etc
22	Empty container drop-off	Empty container drop-off
23	Movement of Empty Containers from the	Through PCS, the SA/SL is able to requisition the movement of empty containers to a specific yard (optimum availability, location, pricing) and

	Port/CFS to Empty Container Yards	an acceptance of the order is submitted back in PCS.
24	Intimation of Booking	Intimation of Booking
25	Placement of Booking	Placement of Booking
26	Confirmation of Booking	Confirmation of Booking
27	Booking of vessel slot by the Exporter	Booking of vessel slot by the Exporter
28	Empty Pick up Letter	Empty Pick up Letter
29	Requisition for allotment of empty containers by the Exporter/CHA to the SL/SA	The Exporter/CHA will place the container request through PCS. The SL/SA will allocate the container, and provide details like the container number, empty container from where the container is to be picked. The same is also communicated to the Empty Container Depot.
30	Surveyor services, in the case of export of Break Bulk/Liquid Cargo	The Surveyor provides the final examination report (confirming the quantity of export) to CHA, CHA gets the Shipping Bill amended if required, and fresh LEO is issued by Customs.
31	Container Related Services	Container Related Services workflow – Request, Response, Order, Service, Payment • Container cleaning • Container Repair • Empty Container Storage (covered under Empty Container Management) • Delivery of Empty containers (covered under Empty Container Management)
32	Container Shifting Services	Onboard shifting, moving a full or empty container from one location aboard a vessel to another on the same vessel and Vessel/ alongside/ vessel shifting, unloading a container from a vessel onto the dock alongside & loading it back onto same vessel again at another time
33	Lashing/Unlashing Services	Lashing Services, consisting of securing a container loaded aboard a vessel in place in line with the captain's wishes by means of bars, bridges, or rods and Unlashing Services consists of the removal of such stabilizing restraints.
34	Opening/Closing Container Vessel Cargo Hatch Covers	Opening/Closing Container Vessel Cargo Hatch Covers: Cargo hatch covers on container vessels will be opened, removed to the dock, and later removed from the dock and closed again by the port.
35	Container Interior Scavenging	Agents will be responsible for the cleanliness of containers that are to be packed in the port area and of containers that arrive empty at the port. At the agent's request the interiors of containers will be scavenged (swept out) against payment of a charge. All containers that are unpacked within the port area must be properly

		scavenged and the agent will be billed for the cost of this service.
36	Container Repair	Containers that arrive in port in damaged condition will be repaired by the port against payment of charges to be specified by the port and insofar as circumstances allow. The port is under no obligation to certify compliance with international rules in the case of such repairs. The port will not allow outside parties to repair damaged containers within the port area. Damaged containers may only be repaired by others if they are removed from the port area first.
37	Electricity for Reefers	The port will supply electricity against a charge for containers that require it both inside and outside the port area. The port maintains a supply of electricity sufficient to meet such needs and it is obliged to provide such electricity when requested by the owner of the goods or container.
38	Port/Terminal Service	Request for Movement of Container to CFS
39	Port/Terminal Service	Gate-in Permission in CFS
40	Port/Terminal Service	Application for resources at CFS
41	Port/Terminal Service	Stevedoring Report
42	Port/Terminal Service	Vessel/Tank Survey Report – Initial
43	Port/Terminal Service	Vessel/Tank Survey Report – Final
44	Port/Terminal Service	Container lifting order
45	Port/Terminal Service	Container received report
46	Port/Terminal Service	Allocation for survey operation
47	Port/Terminal Service	Draft / final survey report
48	Rail Transport Operator Service	Forward Note
49	Rail Transport Operator Service	Container Status Report (Damaged/tampering)
50	Rail Transport Operator Service	Empty Removal Permit

3.4.1.1 Registration Module

Functional Module	Registration Module
Overview of Module	Registration Module shall enable registration of Exporters/ Importers and Logistics Services Providers (LSPs) with NLP MARINE, to participate in EXIM trade transactions, and also manage their profiles (including contact person details, company details, business type, GST details, Bank account number etc.)

Registration Module	
Functional Requirements	
General	
EMREG.REQ.001	System shall provide single interface for registration to all exporters/ importers and LSPs who intend to do EXIM trade business using NLP MARINE
EMREG.REQ.002	System shall provide facility to register according to the business type: Exporters, Importers, and LSPs
EMREG.REQ.003	System shall provide facility/forms/tools for online filing of user registration forms
EMREG.REQ.004	System shall implement the validation controls to ensure that all the mandatory fields are filled by the user
EMREG.REQ.005	Facilitate the applicants to save a partly filled application form for registration in 'Save Draft' mode for a period of 7 days. Further, once the basic profile is created, the System shall also have 'Auto-Save' functionality to ensure that additional information already entered by the user does not have to be re-entered in case of any outages/ navigation errors.
EMREG.REQ.006	System shall submit registration information to the background verificationagencyforreview.Thereshallbethetimelinefor7daysfor anyadditionaldocumentrequired.Ifnodocumentisreceivedfromthe applicant within 7 days, then the verification status will be 'rejected' and verification window will get closed. The notification/alerts shall be sent for any additional documents requirement, along withtimelines
EMREG.REQ.007	System shall allow the NLP MARINE administrator to activate or reject the registration on basis of report received from Background Verification Agency via E-mail to Competent Agency
EMREG.REQ.008	System shall generate and send profile activation link through e-mail, once the registration has been successful and activated by the NLP MARINE Administrator
EMREG.REQ.009	System shall facilitate creation of new user ID and password through e- mail activation link
EMREG.REQ.010	Systemshallprovidealertstothecompetentauthorityforthenewuser registration requests received in thesystem

Registration Module	
Functional Requirements	
EMREG.REQ.011	System shall capture the following minimum information of the applicant: Contact Information, Company Information, LocationDetails and Company Bank AccountDetails
EMREG.REQ.012	System shall capture Aadhaar number, GSTIN and Import Export Code (IEC) from the applicant
EMREG.REQ.013	System shall provide the facility to capture multiple location details such as Communication address, Billing Address, Manufacturing Address, Service Centre Address and Godown Address
EMREG.REQ.014	System shall provide standard template for capturing all generic information of the company including mandatory and non-mandatory fields.MandatoryinformationmayincludeAadhaarnumber,GSTIN,IEC Code, Bank Account information, Location information and Business type
EMREG.REQ.015	IftheuserisLSP,thenthesystemshouldbeabletomandatorycapture all the route details. Also System should be able to capture all the vehicle numbers from the LSP. The LSP shall be able to upload the list of vehicle numbers in the standard excel file or standard text file. The standard template shall be provided by theSystem
EMREG.REQ.016	System shall maintain the master route database and master vehicle details for all the LSPs
EMREG.REQ.017	System shall capture list of certifications and Associations from the LSP (Optional). Also, the LSP shall provide at least two reference of the clients, along with the contact details (mandatory)
Integration with external gateways	
EMREG.REQ.018	System shall be integrated with UIDAI gateway to retrieve and pre-fill minimumcontactdetailsoftheapplicantsuchasName,Address,E-mail and Mobilenumber
EMREG.REQ.019	System shall verify Aadhaar details via OTP
EMREG.REQ.020	SystemshallbeintegratedwithGSTNandDGFTgatewaytoretrieveand pre-fill minimum company details of the applicant from GSTIN and IEC such as Legal Business Name, Registered Address of the Company, Business Type: Proprietary, Public, Private etc., Date of Incorporation, Company Bank Account and PANnumber
EMREG.REQ.021	If required, system may capture the CIN details of the applicant's company and retrieve company details from Ministry of Corporate Affairs gateway

Registration Module	
Functional Requirements	
EMREG.REQ.022	System shall be integrated to E-mail and SMS gateway for email and SMS notifications and alerts
EMREG.REQ.023	System shall be flexible to integrate with other external gateways depending upon the requirement of user's or user's company information
EMREG.REQ.024	The information retrieved from the external gateways should not be editable by the user. For changing such information, the system shall implement workflow and approval process, which must require approval from the government.
EMREG.REQ.025	System shall be integrated to the payment gateway. Also, System shall beintegratedwithVahaangatewaytocapturevehicleinformationsuch as Private/Commercial Vehicle, Name of owner, RC Expiry date, Model number of Vehicleetc.
Validation & Controls	
EMREG.REQ.026	System should ensure that all the mandatory information for registration is provided by the user and system shall highlight all registrationfieldsthathavenotbeenfilledincompletely&correctlyby user. Systemshallhave'Auto-Save'functionalitytoensurethatthedatafilled in the online forms is not lost due to page re-load, system outage etc. Thus, the System should not require the user to enter the details already entered and shall only require the user to submit incremental data.
EMREG.REQ.027	System shall perform validations for the information supplied by the user (including verification of mandatory fields, usage of same e-mail address and existence of same username, existence of same company etc.).
EMREG.REQ.028	Uponcompletionoftheinformationentry,systemshalldisplaythedata entered by the user in a consolidated view for verification and confirmation by theuser.
EMREG.REQ.029	Systemshallinformuserofafailureincasethesameusernamealready exists in the system, inform the user of the failure through an appropriate message and propose alternativeusernames
EMREG.REQ.030	System to validate and match the information retrieved from external gateways such as GSTIN, IEC and if required, PAN

Registration Module	
Functional Requirements	
Security Management	
EMREG.REQ.031	Registration shall be carried out in a secure and encrypted session in the NLP MARINE
EMREG.REQ.032	User credentials (e.g.: passwords, Aadhaar number) must be stored in an encrypted/hashed format and access to such information must be restricted from all categories of users, including DBAs.
EMREG.REQ.033	Registrationprocessmustensuretheconfidentiality,integrityandnon- repudiation of the user and user's organization credentials during information transfer andstorage
EMREG.REQ.034	System shall maintain the detailed audit trails for the registration application submitted in the system including the date and time of receipt of the application form
EMREG.REQ.035	System shall adopt the best practices of secure portal design and development and database management
EMREG.REQ.036	System shall follow the standard guidelines from the respective authorityforexternalintegrationsuchasAadhaarrulesandregulations, GSTN integration guidelinesetc.

3.4.1.2 Login Module

This section presents the key and minimum functional requirements specifications for the National Logistics Portal (NLP MARINE)

Functional Module	Login Module
Overviewof Module	Login Module shall enable the registered user to login into NLP MARINE using threeways:a)AadhaarnumberandOTPverificationb)Mobilenumber and OTP verification c) Username andPassword

Login Module	
Functional Requirements	
General	
EMLOG.REQ.001	System shall provide single interface for login to all registered exporters/ importers and LSPs
EMLOG.REQ.002	System shall provide facility/forms/tools for online user login
EMLOG.REQ.003	System shall implement the validation controls to ensure that all the mandatory fields are filled by the user
EMLOG.REQ.004	System shall provide the facility to reset password through 'Forgot Password' option, in case the user forgets the password
Login in NLP MARINE	
EMLOG.REQ.005	System shall facilitate three types of login: a) Login using mobile numberandOTPb)LoginusingAadhaarnumberandOTPc)Loginusing registered username andpassword
EMLOG.REQ.006	In 'Login using Aadhaar', the system shall request for OTP generated on mobile/e-mail after entering Aadhaar number as User ID
EMLOG.REQ.007	In 'Login using mobile number', the system shall request for OTP generated on mobile after entering mobile number as User ID
EMLOG.REQ.008	System shall validate the user ID: username/mobile/Aadhaar number and password/OTP entered for successful login
EMLOG.REQ.009	System shall open the user instance – Homepage after successful login
Validation & Controls	
EMLOG.REQ.010	System shall perform field validations for the login information (For example: mobile number, password etc.)
EMLOG.REQ.011	System shall use masking for password/ OTP input in login form

Login Module	
Functional Requirements	
EMLOG.REQ.012	System shall inform user of a failure in case the wrong login credentials, inform the user of the failure through an appropriate message
EMLOG.REQ.013	In case of Login through mobile and through Aadhaar, the maximum time allowed to enter OTP should not be more than 180 seconds
Security Management	
EMLOG.REQ.010	Login shall be carried out in a secure and encrypted session in the NLP MARINE
EMLOG.REQ.011	System shall maintain the detailed audit trails for the user login in the system including the date and time of login
EMLOG.REQ.012	System shall be highly secure and the security measures should be up- to-date to prevent existing/new cyber attacks
EMLOG.REQ.013	User credentials (e.g.: passwords, Aadhaar number) must be validated in an encrypted/hashed format (secured mechanism)

3.4.1.3 Documents Exchange Module

This section presents the key and minimum functional requirements specifications for the National Logistics Portal (NLP MARINE)

Functional Module	Documents Exchange Module
Overview of Module	Document Exchange Module shall facilitate the documents exchange between LSP and Exporter/Importer or Shipper

Documents Exchange Module
Functional Requirements
General

Documents Exchange Module	
Functional Requirements	
EMDEM.REQ.001	System shall provide different interface for LSPs and Exporters/Importers andShipper
EMDEM.REQ.002	System shall provide facility/forms/tools for document exchange
EMDEM.REQ.003	System shall allow the documents exchange between the LSPs and Exporters/Importers/Shippers through NLP MARINE Exchange Platform
EMDEM.REQ.004	System shall allow document exchange of document type: pdf/jpeg/jpg and maximum size of 5MB
EMDEM.REQ.005	Systemshallprovidethefacilitytotheusertoexchangedocuments anytime after the LSP is selected by the exporter/ importer and shipper
EMDEM.REQ.006	System shall scan and check the document for spyware/adware or viruses. In case the document is infected, system shall delete the document immediately and shall notify the uploader through email and SMS.
EMDEM.REQ.007	Document exchange between one LSP and Exporter/Importer and Shipper shall not be visible to the other LSP. The document exchange shall be one-to-one exchange only
LSP interface	
EMDEM.REQ.008	System shall allow LSP to view the list of documents which needs to be shared with the exporter/importer/shipper
EMDEM.REQ.009	System shall provide the facility to LSP to uploaded relevant documents using direct upload or selecting the documents from document management system (DMS)
EMDEM.REQ.010	Systemshallprovidethedocumentsstatusinthelistofdocuments. The color codes shall be used. a) Green color: Document shared b) Red color DocumentPending
EMDEM.REQ.011	For EXIM trade, relevant documents needs to be shared with the exporter/ importer and shipper
Exporter/ importer and shipper Interface	

Documents Exchange Module	
Functional Requirements	
EMDEM.REQ.012	SystemshallallowExporter/importerandshippertoviewthelistof documents which needs to be shared with each selectedLSP
EMDEM.REQ.013	System shall provide the facility to Exporter/ importer and shipper touploadedrelevantdocumentsusingdirectuploadorselectingthe documents from document management system(DMS)
EMDEM.REQ.014	Systemshallprovidethedocumentsstatusinthelistofdocuments. The color codes shall be used. a) Green color: Document shared b) Red color DocumentPending
EMDEM.REQ.015	SystemshallenabletheExporter/importerandshippertoenterthe requiredinformationanduploadsupportingdocumentstoICEGATE to obtain Shipping Bill number and Let Export Order (LEO). This interaction shall be done through Integrated RegulatoryPlatform
EMDEM.REQ.016	System shall be integrated with ICEGATE and submit the information and documents filled by the user
EMDEM.REQ.017	Information received from ICEGATE shall be captured in the DocumentManagementSystem(SMS)andnotificationshallbesent to the Exporter/ importer and shipper through E-mail andSMS
EMDEM.REQ.018	System shall provide the facility to LSP to uploaded relevant documents using direct upload or selecting the documents from document management system (DMS)
EMDEM.REQ.019	For EXIM trade, relevant documents needs to be shared with the exporter/ importer and shipper
EMDEM.REQ.020	The document exchange should be one-to-one and should not be visible to other LSPs and shall be done in secure environment
EMDEM.REQ.021	Document Exchange shall be carried out in a secure and encrypted session in the NLP MARINE
EMDEM.REQ.022	System shall maintain the detailed audit trails for the document exchange including the date and time

Documents Exchange Module	
Functional Requirements	
EMDEM.REQ.023	System shall perform field validations for the user input information

3.4.1.4 Track and Trace Module

This section presents the key and minimum functional requirements specifications for the National Logistics Portal (NLP MARINE)

Functional Module	Track and Trace Module
Overviewof Module	TrackandTracemoduleprovidesthefacilitytotheusertoviewthe complete tracking details of the order movement. This module captures the tracking details as well as documents from the LSP mobile app, FOIS, PCS, CONCOR and other external agencies involved in order movement through NLP MARINE Exchangeplatform

Track and Trace Module	
Functional Requirements	
General	
EMTT.REQ.001	System shall provide different interface for LSPs and Exporters/Importers andShipper
EMTT.REQ.002	System shall provide facility/forms/tools for document exchange
EMTT.REQ.003	System shall be integrated with the LSP mobile app, FOIS, PCS and other departments which are involved in order movement

Track and Trace Module	
Functional Requirements	
EMTT.REQ.004	System shall interact with the Document Management System (DMS) in NLP MARINE
EMTT.REQ.005	System shall provide notifications over E-mail and SMS
EMTT.REQ.006	System shall use Google Maps or any other map framework to display the live tracking details to the exporter or shipper
Exporter Interface	
EMTT.REQ.007	System shall provide track and trace module from the order details module
EMTT.REQ.010	System shall provide the status update from FOIS, PCS and other departments which are involved in order movement
EMTT.REQ.011	Systemshallprovidetheconsolidatedordertrackingdetails(timeline) through progress chart and shall facilitate to drill down for more information (such as: viewing live location tracking through google map, tracking ID generated from external agencies etc.). Systemshall provide the details of the scope of the tracking/status update information
EMTT.REQ.012	System shall allow the exporter/shipper to view the documents in documents management system
EMTT.REQ.013	System shall provide the update to the exporter/shipper whenever the cargo change hands between the different LSPs and/or different movement methods
EMTT.REQ.014	System shall activate Ratings module when the order gets delivered
EMTT.REQ.015	System shall provide the Emergency Response mechanism in case of any break down or crisis
Information/Documents gathering	

Track and Trace Module	
Functional Requirements	
EMTT.REQ.017	System shall capture the status information from the external agencies such as FOIS, PCS etc. through NLP MARINE Exchange platform
EMTT.REQ.018	System shall be integrated with the LSP mobile app, FOIS, PCS and other agencies which are involved in order movement
EMTT.REQ.019	System shall also capture tracking id from the above external agencies
EMTT.REQ.020	ThedocumentexchangebetweentheLSPandWarehouseand/orany generateddocumentduringthecargomovementshallbeprovidedto the exporter/shipper through NLP MARINE Exchange platform and Document Management System(DMS)
EMTT.REQ.021	The NLP MARINE Exchange platform shall consolidate all the tracking details and status update and present it to the exporter interface of this module
Security Management and Validation Controls	
EMTT.REQ.022	System shall maintain the detailed audit trails for the track and trace module
EMTT.REQ.023	The interaction with external agencies shall be carried out in a secure and encrypted session in the NLP MARINE
EMTT.REQ.024	All the documents in the document management system (DMS) shall be scanned for virus/adware/spyware and shall be immediately deleted in case of any infected document found. The uploader and the receiver of the document shall be notified about this action
EMTT.REQ.025	System shall always use the up-to-date APIs of integration with external agencies (FOIS etc.) and services (Google Map API etc.)
EMTT.REQ.026	The system should be adequate security features built in the architecture of the system to prevent any cyber attack
Help/Grievances	

Track and Trace Module	
Functional Requirements	
EMTT.REQ.027	SystemshallsupportprovisionforIVR/CallCentre/SMS/onlineoption for checking of statusupdate
EMTT.REQ.028	System shall allow the applicant to print/e-mail the status update informationiftheapplicantisretrievingthestatusthroughtheportal.
EMTT.REQ.029	System shall allow the grievance mechanism in case of any false deliveryupdateoranyotherissuesrelatedtothedeliveryoftheorder
Mobile Application	
EMTT.REQ.030	There shall be also hybrid mobile app for exporter/importer for this module

3.4.1.5 Document Management System Module

This section presents the key and minimum functional requirements specifications for the National Logistics Portal (NLP MARINE)

Functional Module	Document Management System (DMS) module
Overview of Module	Document management system (DMS) modules facilitates documents storage and retrieval. The documents retrieved from external agencies through NLP MARINE Exchange platform and the documents uploaded manually shall be stored in the documents management system

Document Management System Module

Functional Requirements	
EMDMS.REQ.001	System shall have document management system which should have a functionality to store and archive the document in the system. The system should have the modules of having following features in the suite: Document Management, Record Management, Archival, Imaging & Information Rights Management
EMDMS.REQ.002	System must be scalable and follow the e-Gov standards as formulated by MeitY, GoI
EMDMS.REQ.003	Provide out-of-the-box integration with leading application servers
EMDMS.REQ.004	Systemshallprovidewebinterfacealongwiththefacilityofdragand drop. Web interface should support popular browsers such as Microsoft Explorer, Firefox, Netscape, Google and any other proposed browseretc.
EMDMS.REQ.005	Systemallowdocument/imagecapturingandshouldbeabletosend to a centralizedrepository
EMDMS.REQ.006	The system shall provide the standard file hierarchy structure of foldersandsub-folderstoallowusersandgroupsofuserstomanage and organize their documents. State any limitations to the number of folders, subfolderlevels.
EMDMS.REQ.007	Theinterfaceshallallowuserscreation,editingandmanagementof documents. The system shall provide the to update the version of the linked document whenever the original isupdated
EMDMS.REQ.008	The web interface shall provide multiple views of the content and allowuserstoaccess/modifyfoldersbasedontheiraccessrightsand permissions. The proposed system should be able to restrict the userstoaccessdocuments/imagesbasedontheirpre-definedrights &privileges
EMDMS.REQ.009	System must provide web-based administration tool and provide a single point of access for managing and administering all repositories, servers, users and groups regardless of their location
EMDMS.REQ.010	System allow the users to add attributes/metadata to the documents and classify the documents based on their Type
EMDMS.REQ.011	System shall have simple search & advanced search facility
EMDMS.REQ.012	System shall provide a policy engine that can execute storage placement and migration policies to optimize storage, while reducing the content storage cost to the business and maintain accessibility and compliance needs as its value changes over time

Document Management System Module	
Functional Requirements	
EMDMS.REQ.013	System shall provide migration logs and audit trails so that operations on content is traceable. Audit trail must contain information such as event performed on document, user who performed the action, and date time stamp
EMDMS.REQ.014	Documents received from external agencies through NLP MARINE Exchange Platform shall be stored in Document Management System
EMDMS.REQ.015	System shall be able to store images/documents in various formats suchjpeg,gif,bmp,worddoc,excel,powerpoint,pdfetc.Thesame infrastructure should be able to support other content types in the future like audio, video filesetc.
EMDMS.REQ.016	System shall not require any additional license to communicate / exchange data between client / host machine and server
EMDMS.REQ.017	System shall support application of metadata taxonomy based on key words within the document.
EMDMS.REQ.018	System shall enable cross-reference of documents
EMDMS.REQ.019	System shall have search capabilities that supports powerful and comprehensive full-text searching, metadata searching or a combination of the two.
EMDMS.REQ.020	System shall provide ability for the user to search and find documents based on any of the associated metadata, such as document type, author, title, location, active/inactive status, date created etc.
EMDMS.REQ.021	System shall provide capability to search within so that users can narrow down the search
EMDMS.REQ.022	Interface for managing the entire lifecycle of Document management, starting from its creation to itsdisposition

3.4.1.6 Payment Module

This section presents the key and minimum functional requirements specifications for the National Logistics Portal (NLP MARINE)

Functional Module	**Payment module**
Overviewof Module	Payment module facilitate the LSP to submit their invoice and also facilitates the exporter/importer/domestic trader and shipper to make payments w.r.t the invoice submitted

Payments Module	
Functional Requirements	
PM.REQ.001	System shall provide separate interface for the exporter/importer and for the LSP
PM.REQ.002	System shall provide facility/forms/tools for invoice submission
PM.REQ.003	System shall implement the validation controls to ensure that all the mandatory fields are filled by the user
PM.REQ.004	System shall capture following minimum information from the LSP: • OrderNumber • Name and Address of the client(pre-filled) • Date • Amount • Amount inwords • Currency • Taxdetails • Description ofServices • Payment DueDate • Any otherdetails
PM.REQ.005	System shall generate invoice from the information captured by the LSP. The generate invoice shall be in pdf or jpeg format
PM.REQ.006	System shall provide the facility to the LSP to either submit the system generated invoice to the exporter/importer or upload the scanned copy of their own invoice and submit against the order number

Payments Module	
Functional Requirements	
PM.REQ.007	System shall allow the exporter/importer to view the invoice submitted in order details
PM.REQ.008	System shall send email notification/alerts about the receiving of the invoice submitted by LSP
PM.REQ.009	System shall provide and allow financial transaction functions
PM.REQ.010	System shall check for all details of the application form before initiating the payment
PM.REQ.011	System shall record and maintain all details of payment against a unique service file number generated for the applicant
PM.REQ.012	System shall be able to maintain all the payment records in a database and retrieve the same as and when required
PM.REQ.013	System shall be integrated to payment gateway and shall provide multiple modes of payment such as Internet Banking, Credit Card, Debit Card and UPI
PM.REQ.014	System shall provide proper error handling payment mechanism
PM.REQ.015	In case of payment issues such as failure in reaching the payment gateway, system shall try for either reconciliation mechanism or re-try mechanism
PM.REQ.016	System shall provide and allow PD Top-up by other stakeholders to terminal operators.

3.4.1.7 Business Transaction Support Module

This section presents the key and minimum functional requirements specifications for the National Logistics Portal (NLP MARINE)

Functional Module	Business Transaction Support Module
Overview of Module	Business Transaction Support module shall facilitate the exporter/importer/LSPs to submit the grievances online. The request shall be forwarded to the NLP MARINE facilitation cell for processing. The response to the grievance query shall be sent through E-mail and SMS

Grievances Module	
Functional Requirements	
Grievances Interface	
EMGRV.REQ.001	System shall provide single interface for exporters/ importers and LSPs to register grievances
EMGRV.REQ.002	System shall provide facility/forms/tools for grievances form
EMGRV.REQ.003	System shall provide the facility to capture grievance related information from the user
EMGRV.REQ.004	System shall allow uploading of supporting documents along with the grievances information
EMGRV.REQ.005	System shall allow only PDF or JPG type of supporting documents and maximum upload size of 4 MegaBytes (MB)
EMGRV.REQ.006	System shall implement the validation controls to ensure that all the mandatory fields are filled by the user
EMGRV.REQ.007	System shall check for spywares/adware/viruses on the uploaded document

Grievances Module	
Functional Requirements	
EMGRV.REQ.008	System shall send E-mail and SMS notification to the user providing the acknowledgement of the grievance submission
EMGRV.REQ.009	System shall maintain the detailed audit trails for the grievances submission
EMGRV.REQ.010	System shall record the date and timestamp of grievances submission
EMGRV.REQ.011	System shall allow NLP MARINE facilitation cell to submit the query response
EMGRV.REQ.012	System shall send grievances query response to the complainant through e-mail and SMS

3.4.1.8 Content Management Module

This section presents the key and minimum functional requirements specifications for the National Logistics Portal (NLP MARINE)

Functional Module	Content Management Module
Overview of Module	The Content Management Module (CMS) shall help/guide/navigate all the users of the NLP MARINE about the various operations. The CMS shall provide FAQs, Video Tutorials, User Manuals and other guiding materials in the NLP MARINE

Content Management Module	
Functional Requirements	
EMCM.REQ.001	System shall provide FAQs on all the modules which provides interface from the user. FAQs shall be made available for public view

EMCM.REQ.002	System shall provide web-based training videos (WBT) demonstrating all the user interaction related modules in detail. Such videos shall explain each phase of the registration process, contents and documents to be attached during registration etc. Online training programmes shall be in both English and local language (Hindi).
EMCM.REQ.003	System shall provide a 'Help/Guidance' page which includes the video tutorials for end-to-end process for each type of stakeholder
EMCM.REQ.004	System shall provide User Manual for each type of stakeholder. The user manual shall be in English and Hindi
EMCM.REQ.005	System shall provide up-to-date content and the content shall be ease in understanding and engaging for the viewer
EMCM.REQ.006	System shall also capture the feedbacks/suggestions from the user of the NLP MARINE
EMCM.REQ.007	There shall be also hybrid mobile app for exporter/importer for this module

3.4.1.9 Mobile App Login Module

This section presents the key and minimum functional requirements specifications for the National Logistics Portal (NLP MARINE)

Functional Module	Mobile App Login Module
Overviewof Module	Mobile application login module shall enable the LSP and exporter/importer to login into the mobile app. The users shall be registered with the NLP MARINE system

Mobile App Login Module	
Functional Requirements	
General	
MALOG.REQ.001	System shall interface for login to both LSP and exporter/importers
MALOG.REQ.002	System shall provide facility/forms/tools for online user login
MALOG.REQ.003	System shall implement the validation controls to ensure that all the mandatory fields are filled by the user
MALOG.REQ.004	System shall provide the facility to reset password through ‘Forgot Password’ option, in case the user forgets the password
Login in Mobile App	
MALOG.REQ.005	System shall facilitate three types of login: a) Login using mobile number and OTP b) Login using Aadhaar number and OTP c) Login using registered username and password
MALOG.REQ.006	In ‘Login using Aadhaar’, the system shall request for OTP generated on mobile/e-mail after entering Aadhaar number as User ID

Mobile App Login Module	
Functional Requirements	
MALOG.REQ.007	In ‘Login using mobile number’, the system shall request for OTP generated on mobile after entering mobile number as User ID
MALOG.REQ.008	System shall validate the user ID: username/mobile/Aadhaar number and password/OTP entered for successful login
MALOG.REQ.009	System shall auto-detect OTP received on the mobile device
Validation & Controls	
MALOG.REQ.010	System shall perform field validations for the login information (For example: mobile number, password etc.)
MALOG.REQ.011	System shall use masking for password/ OTP input in login form
MALOG.REQ.012	System shall inform user of a failure in case the wrong login credentials, inform the user of the failure through an appropriate message
MALOG.REQ.013	In case of Login through mobile and through Aadhaar, the maximum time allowed to enter OTP should not be more than 180 seconds
Security Management	
MALOG.REQ.014	System shall maintain the detailed audit trails for the user login in the system including the date and time of login
MALOG.REQ.015	System shall be highly secure and the security measures should be up- to-date to prevent existing/new cyber attacks
MALOG.REQ.016	User credentials (e.g.: passwords, Aadhaar number) must be validated in an encrypted/hashed format (secured mechanism)

3.4.1.10 Mobile App Track and Trace Module

This section presents the key and minimum functional requirements specifications for the National Logistics Portal (NLP MARINE) Mobile Application

Functional Module	Mobile App Track and Trace Module
Overviewof Module	Track and Trace Module shall enable shipper and LSPs to share live location and status of shipment.

Mobile App Track and Trace Module	
Functional Requirements	
General	
MATT.REQ.001	System shall display order details such as order number, name and contact details of shipper, pickup location, destination location, commodities and capacity, expected date of delivery, etc.
MATT.REQ.002	System shall display important contact details of LSP and shipper
MATT.REQ.003	System shall request Global Positioning System (GPS) permissions of mobile devices to access location information
MATT.REQ.004	System shall use a suitable API to convert the location coordinates into address: Area, City, State, Pin Code
MATT.REQ.005	System shall transmit location information to the NLP MARINE over mobile internet
MATT.REQ.006	System shall enable viewing real-time positioning of the shipment on map
MATT.REQ.007	System shall allow LSPs to manually update the status of shipment with respect to checkpoints (e.g.: arrived at ICD, left from port)

Mobile App Track and Trace Module	
Functional Requirements	
MATT.REQ.008	System shall validate the status of shipment updated by LSP with location information available via the API
MATT.REQ.009	System shall enable alerts via notifications in case of an emergency or delay during transit
MATT.REQ.010	System shall display the time taken by shipment to move between checkpoints
MATT.REQ.011	Systemshallretrievethelistofdocumentstobeexchanged(atorigin and destination) from the Document Management Systemmodule
MATT.REQ.012	System shall display list of documents to be exchanged at the particular origin/destination upon arrival
MATT.REQ.013	System shall provide facility to capture documents digitally
MATT.REQ.014	System shall provide facility to upload documents exchanged to the Document Management System
Security	
MATT.REQ.015	The real-time location and status of the shipment should only be visible to the involved LSP and the shipper
MATT.REQ.016	The documents should be uploaded via a secure, encrypted channel
MATT.REQ.017	Systemshallperformvalidationstoensureallthe requireddocuments areuploaded
MATT.REQ.018	System shall keep a local store of required data on the mobile device in case of loss of network connectivity
MATT.REQ.019	The location transmission should support one or several encryption modes, e.g., static wired equivalent privacy (WEP) encryption

3.4.2 PGA and Regulatory Platform

3.4.2.1 Single Window Certification System

1) ListingModule

This section presents the key and minimum functional requirements specifications for the National Logistics Portal (NLP MARINE) Mobile Application

Functional Module	Listing Module
Overview of Module	Listing module shall enable the user to view the required certifications/NOCs or any other type of document from Export Promotion Councils (EPC) / Participative Government Agencies (PGAs) on the basis of input information such as commodity name and HS codes, source, destination etc.

Listing Module	
Functional Requirements	
SWL.REQ.001	Systemshallmaintainthemasterdatabaseofcommodities,agencies, documents required, application form details and list of certifications/NOCs/other documentsgenerated
SWL.REQ.002	The master database shall contain following minimum information: ▪ Commodityname ▪ Commodity HScodes ▪ List of EPC involved in respectivecommodity ▪ List of PGA involved in respectivecommodity ▪ Listofcertificates/NOCs/otherdocumentsgeneratedfortrade of respectivecommodities ▪ List of fields of applicationform ▪ List of documents required to submit along with the application form to each relevant EPC andPGA ▪ Processing time for each certificate/ NOCs or any other type of document fromEPC/PGA ▪ Location specificdetails ▪ Feesforeachcertificate/NOCsoranyothertypeofdocument fromEPC/PGA ▪ Bank details of EPCs andPGAs

Listing Module	
Functional Requirements	
SWL.REQ.003	Systemshallprovidethelistofrelevantcertificate/NOCsoranyother type of document from EPC/PGA on the based on the input of commodity name, source anddestination
SWL.REQ.004	System shall be able to capture the input details from the Logistics e- market place component (Order Submission)
SWL.REQ.005	System shall provide following minimum information from the master database to the user: • List of EPC/PGAsinvolved • List of certificates/NOCs/otherdocuments • List of documentsrequired • Estimated processingtime • Fees for each certificates/NOCs/otherdocument • List of RCMC required for EPC/PGAsinvolved
SWL.REQ.006	Systemshallbeabletoprovideeasyandquickuserinterfaceanduser experience

3.4.2.2 Common Application Form (CAF) module

This section presents the key and minimum functional requirements specifications for the National Logistics Portal (NLP MARINE) Mobile Application

Functional Module	Common Application Form (CAF) module
Overview of Module	CAF module shall enable the user to submit the single application form and all the required documents to obtain certificated/NOCs/other documents from relevant Export Promotion Council (EPC) and Participative Government Agencies (PGAs)

CAF Module

Functional Requirements	
SWCAF.REQ.001	System shall provide facility/forms/tools for online order submission
SWCAF.REQ.002	System shall implement the validation controls to ensure that all the mandatory fields are filled by the user
SWCAF.REQ.003	Facilitate the user to save a partly filled order form in ‘Save Draft’ mode for a period of 7 days. Further, once the basic information is entered, the System shall also have ‘Auto- Save’ functionality to ensure that additional information already entered by the user does not have to be re-entered in case of any outages/ navigation errors.
SWCAF.REQ.004	System shall facilitate simple user interface and fast user experience for easy submission of orders
SWCAF.REQ.005	System shall be integrated with Document management system (DMS) in NLP MARINE and also with the NLP MARINE Exchange platform
SWCAF.REQ.006	System shall be integrated with the online system of each PGA and EPC
SWCAF.REQ.007	System shall retrieve application form fields from the master database and shall provide the consolidated application form (Common Application form) to the user
SWCAF.REQ.008	System shall provide the single input field to enter, in case of the overlapping of field names
SWCAF.REQ.009	System shall provide standard template for common application
SWCAF.REQ.010	System shall provide the interface to upload all the required documents in documents management system (DMS)
SWCAF.REQ.011	System shall track and maintain the checklist of the required documents to be uploaded and shall display the status of the documents pending and/or uploaded
SWCAF.REQ.012	Upon completion of the information entry, system shall display the data entered by the user in a consolidated view for verification and confirmation by the user.

CAF Module	
Functional Requirements	
SWCAF.REQ.013	System shall maintain the detailed audit trails for the registration application submitted in the system including the date and time of receipt of the application form
SWCAF.REQ.014	System shall check for virus/spyware/adware in the documents uploaded by the user in DMS
SWCAF.REQ.015	System shall delete and publish notifications/alerts to the user, in case of infected document in found
SWCAF.REQ.016	System shall allow the drag and drop interface for the documents upload. User can drag/drop more than one document at a time.
SWCAF.REQ.017	Once the common application form (CAF) has been submitted by the user, system shall move to the payments module
SWCAF.REQ.018	System shall enable the payment option only when all the fields of service request forms are filled and no errors received
SWCAF.REQ.018	System shall have track and trace facility to enable the exporter/importer to view the status of the application, estimated time from each relevant EPC/PGA, status update of the application, etc.

3.4.2.3 Payments Module

This section presents the key and minimum functional requirements specifications for the National Logistics Portal (NLP MARINE) Mobile Application

Functional Module	Payments module
Overviewof Module	Payments module shall facilitate the user to perform online payments for the certificate/NOCs/other documents

Payments Module	
Functional Requirements	
PAY.REQ.001	System shall provide and allow financial transaction functions
PAY.REQ.002	Systemshallcheckforalldetailsoftheapplicationformbeforeinitiating thepayment
PAY.REQ.003	Systemshallrecordandmaintainalldetailsofpaymentagainstaunique service file number generated for theapplicant
PAY.REQ.004	System shall be able to maintain all the payment records in a database and retrieve the same as and when required
PAY.REQ.005	System shall be integrated to payment gateway and shall provide multiplemodesofpaymentsuchasInternetBanking,CreditCard,Debit Card andUPI
PAY.REQ.006	Systemshallconsiderthetotalamountofthefeesforthepayment.For example: If the fees for the certificate to be obtain from one EPC is INR 100 and the fees for the certificate to obtain from another EPC is INR 50,thenthesystemshallconsidertheamountINR150forthepayment
PAY.REQ.007	System shall provide proper error handling payment mechanism
PAY.REQ.008	In case of payment issues such as failure in reaching the payment gateway, system shall try for either reconciliation mechanism or re-try mechanism

Payments Module	
Functional Requirements	
PAY.REQ.009	In case of successful payment, system shall perform following actions:
PAY.REQ.010	Submitting respective payments to each relevant EPC/PGAs bank account
PAY.REQ.011	Receiving acknowledgment for successful credit of amount in bank account from each EPC and PGAs. The minimum information that acknowledgement shall contain are date and time, transaction ID and amount
PAY.REQ.012	Providing consolidated payment acknowledgment to the user. The minimum information in the user acknowledgement shall contain: • Date andtime • Name ofEPC/PGA • TransactionID • Amount • Certificate/NOC/Other documentname
PAY.REQ.013	Submitting filled respective application form details and documents to each EPC/PGA
PAY.REQ.014	The information submission to EPC/PGA shall be done through NLP MARINE Exchange platform
PAY.REQ.015	Receive acknowledgment of the information submission to EPC/PGA and provide it to the user. The acknowledgment shall contain the application ID and other required acknowledgement details
PAY.REQ.016	In case of failed payment, system shall perform following actions:
PAY.REQ.017	Alerts/Notifications to the user about the failed payment
PAY.REQ.018	Providing option of re-try of payment to the user

Payments Module	
Functional Requirements	
PAY.REQ.019	Providing other modes of payment to the user
PAY.REQ.020	Store the CAF information and documents information in the system and provide the facility to the user to make payment at any point of time
PAY.REQ.021	System shall provide end-to-end secure encryption and use secure framework
PAY.REQ.022	System security shall be up-to-date to prevent cyber attacks

EPC/PGA InterfaceModule

This section presents the key and minimum functional requirements specifications for the National Logistics Portal (NLP MARINE) Mobile Application

Functional Module	EPC/PGA Interface Module
Overview	EPC/PGA interface module shall provide the facility to Export Promotion Council (EPC) and Participative Government Agencies (PGAs), which have completely or partial online process and generate certificates/NOCs/other documents through physical copies only. This module shall enable the EPC/PGA to view application information and provide scanned copy of the certificate/NOC/other documents

EPC/PGA Interface Module	
Functional Requirements	
General	
EPCI.REQ.001	Systemshallprovidesingleinterfaceforlogintoallregisteredexporters/ importers andLSPs

EPC/PGA Interface Module	
Functional Requirements	
EPCI.REQ.002	System shall provide facility/forms/tools for online user login
EPCI.REQ.003	System shall implement the validation controls to ensure that all the mandatory fields are filled by the user
EPCI.REQ.004	The login credentials for EPCs and PGAs shall be pre-defined and be shared with the respective EPC and PGAs
EPCI.REQ.005	ThepasswordforEPC/PGAslogincredentialshallbeof12charactersand contain mix of alphabets, numbers and specialcharacters
EPCI.REQ.006	System shall be integrated with NLP MARINE Exchange Platform
Login	
EPCI.REQ.007	System shall allow provide field names: username and password to enable EPC/PGA to login in to the system
EPCI.REQ.008	System shall perform field validations for the login information (For example: mobile number, password etc.)
EPCI.REQ.009	System shall use masking for password/ OTP input in login form
EPCI.REQ.010	System shall inform user of a failure in case the wrong login credentials, inform the user of the failure through an appropriate message
EPCI.REQ.011	User credentials (e.g.: passwords, Aadhaar number) must be validated in an encrypted/hashed format (secured mechanism)
EPCI.REQ.012	Login shall be carried out in a secure and encrypted session in the NLP MARINE
EPCI.REQ.013	System shall maintain the detailed audit trails for the user login in the system including the date and time of login
EPCI.REQ.014	System shall be highly secure and the security measures should be up- to-date to prevent existing/new cyber attacks

EPC/PGA Interface Module	
Functional Requirements	
Application Details Interface	
EPCI.REQ.015	System shall provide list of information about the application submitted and supporting documents for certificate/ NOC/ other documents
EPCI.REQ.016	System shall capture the application submitted through NLP MARINE exchange platform
EPCI.REQ.017	The application submitted shall be for the respective EPC/PGA only
EPCI.REQ.018	System shall provide a facility to export the information in PDF or XLS
EPCI.REQ.019	System shall provide a facility to take action on each application submitted. The action shall open a new interface to upload document
EPCI.REQ.020	The uploaded document (scanned copy of the certificate/NOC/other document) shall be stored in Document Management System
EPCI.REQ.021	System shall send alerts/notification to the applicant about the certificate/ NOC/ other document upload on E-mail and SMS
EPCI.REQ.022	System shall scan the uploaded document for virus/ spyware/ adware and take proper action accordingly
Other	
EPCI.REQ.023	System shall provide the facility to the NLP MARINE Administrator to change/reset the login credentials of EPC/PGA
EPCI.REQ.024	System shall send the new login credentials to EPC/PGA through E-mail and SMS
EPCI.REQ.025	System shall provide workflow mechanism for each EPC and PGA. The workflow mechanism shall be flexible and each EPC and PGA can define their workflow
EPCI.REQ.026	EachEPCandPGAshallbegivenoneseparateadministratorlogintoonly define their workflowmechanism

EPC/PGA Interface Module	
Functional Requirements	
EPCI.REQ.027	System shall provide the facility to the EPC/PGA to view application details and documents and provide the comments. The comments shall be viewed by the next level as defined in the workflow
EPCI.REQ.028	System shall have separate database and separate process flow. System shallalsoprovidethefacilitytotheEPC/PGAadministratortocustomize the look and feel of their departmentinterface

Generated CertificatesModule

This section presents the key and minimum functional requirements specifications for the National Logistics Portal (NLP MARINE) Mobile Application

Functional Module	Generated Certificates Module
Overviewof Module	Generated certificates module shall provide the facility to retrieve the generated certificates/ NOC/ other documents from the EPCs/ PGAs who have their own online system and generate certificates online. This module shall be integrated with the EPC/PGAs online system through NLP MARINE Exchange Platform

Generated Certificates Module	
Functional Requirements	
GC.REQ.001	System shall be integrated with the external online systems of EPCs and PGAs through NLP MARINE Exchange platform
GC.REQ.002	System shall keep track of application id as an identifier for each certificate/ NOC/ other documents to be generated by EPC/ PGA
GC.REQ.003	Oncethecertificate/NOC/otherdocumentisgeneratedintheEPC/PGA online system, system shall be able to fetch the require certificate through the NLP MARINE ExchangePlatform

Generated Certificates Module	
Functional Requirements	
GC.REQ.004	The captured certificate/ NOC/ other document shall in in jpeg or pdf file format
GC.REQ.005	System shall store the captured certificate/ NOC/ other document from each EPC and PGA in Document Management System (DMS)
GC.REQ.006	System shall provide alerts and notifications to the applicant about the generated certificate/ NOC/ other document

3.4.2.4 Integrated Regulatory Platform

1. Integrated Regulatory PlatformModule

Functional Module	Integrated Regulatory Platformmodule
Overviewof Module	Integrated regulatory module shall facilitate the regulatory informationexchangesbetweenICEGATEandExporters/Importers and LSP through NLP MARINE ExchangePlatform

Integrated Regulatory module	
Functional Requirements	
IR.REQ.001	SystemshallbeintegratedwithICEGATEplatformthroughNLP MARINEExchange platform
IR.REQ.002	System shall allow the user to select ‘Customs’ option wherever the interaction with ICEGATE is required
IR.REQ.003	System shall integrate ‘Integrated Regulatory Platform’ module with e- Logistics marketplace module

Integrated Regulatory module	
Functional Requirements	
IR.REQ.004	System shall provide facility/forms/tools for online submission of application to ICEGATE
IR.REQ.005	System shall provide necessary validation controls to the application form
IR.REQ.006	System shall provide the facility to the user to provide supporting documents along with the application form
IR.REQ.007	System shall allow the user to either upload the document directly or drag/drop existing document through document management system
IR.REQ.008	System shall allow the submission of application to the ICEGATE through NLP MARINE Exchange platform
IR.REQ.009	NLP MARINEExchangeplatformshalltranslatethemessageaspertheintegration format and forward toICEGATE
IR.REQ.010	System shall provide the acknowledgement received from the ICEGATE to the user through NLP MARINE Exchange platform
IR.REQ.011	Once the information/document generated by the ICEGATE system, system shall translate and forward it to the user through NLP MARINE Exchange Platform
IR.REQ.012	The information/documents received from the ICEGATE shall be stored in the Document Management System in the pre-defined folder
IR.REQ.013	System shall generate notifications/alerts to the user about the new information/document received from ICEGATE
IR.REQ.014	System shall provide the estimated turnaround time of the information/document generation by thecustoms

3.4.3 Finance and Insurance Platform

3.4.3.1 Trade Finance Platform

Trade FinanceModule

This section presents the key and minimum functional requirements specifications for the National Logistics Portal (NLP MARINE) Mobile Application

Functional Module	Trade Finance module
Overviewof Module	This module shall help exporter/importer to find a suitable service provider for obtaining the Letter of Credit and/or other relevant documents

Trade Finance Module	
Functional Requirements	
TF.REQ.001	The system shall have a master database storing details of banks offering trade finance services
TF.REQ.002	Thesystemshallstoredetailsofthebanksincludingi)Nameofbank,ii) Branch name, iii) Name of contact person, iv) Designation of contact person, v) Contact details of contact person and of branch, v) Branch address, vi) IFSC code, vii) Other relevant information anddocuments
TF. REQ.003	The user shall be able to search for available banking options based on filters on the columns specified above
TF. REQ.004	The system shall display relevant details of a particular bank (retrieved from the database) while a user is viewing the banking options
TF. REQ.005	The system shall be regularly updated to ensure correctness of bank information and add/delete/modify banks offering the L/C service
TF. REQ.006	The system shall inform the user if there are special terms offered by certain banks
TF. REQ.007	The system shall provide an option to confirm bank selection and subsequently display to the user that the particular bank has been selected
TF. REQ.008	The system shall provide the facility to the user to apply for Letter of Credit. The link shall be redirected to the respective bank application page

3.4.3.2 Document Sharing System

This section presents the key and minimum functional requirements specifications for the National Logistics Portal (NLP MARINE)

Functional Module	Document Sharing Module
Overviewof Module	Thismodulefacilitatestheeasysharingofdocumentsobtainedfrom various PGAs/EPCs/regulatory authorities with the bank and vice versa.

Document Sharing Module	
Functional Requirements	
DS. REQ.001	System shall link this module with the Document Management System module to fetch existing available documents
DS. REQ.002	System shall ensure that the drag and drop/movement of documents is seamless
DS. REQ.003	System shall ensure complete end-to-end encryption of documents while transferring
DS. REQ.004	System shall prevent transfer of unnecessary documents to the bank.
DS. REQ.005	System shall display list of required documents which need to be exchanged with the bank
DS. REQ.006	System shall ensure that all required documents have been sent
DS. REQ.007	The documents shall remain in PDF or JPG format and editing should not be allowed in any case.
DS. REQ.008	System shall have simple search & advanced search facility

3.4.3.3 e-BG

This section presents the key and minimum functional requirements specifications for the National Logistics Portal (NLP MARINE)

Functional Module	E-BG Module
Overviewof Module	E-BG Module shall facilitate the exporter/importer for obtaining Performance Bank Guarantee from LSP online

E-PBG Module	
Functional Requirements	
BG.REQ.001	Bankers server will be integrated with NLP MARINE for information interchange related with e-BG through NLP MARINE Exchange Platform
BG.REQ.002	Nearest Branch of bankers will act as advising branch for E-BG related transaction
BG.REQ.003	If needed, exporter/importer may opt for bank guarantee & indicate advising Banker of his choice at time of bidding process in e-Logistics Marketplaceandaccordinglysystemwillalertprospectivebidderabout the requirement of bank guarantee in electronic form from the successful supplier after completion of biddingcycle.
BG.REQ.004	After successful bidding process, System will provide standard BG format complete with all the necessary field such as value of contract, validity of the BG, beneficiary detail, BIC Code of advising bank chosen by the buyer and vital information related with the contract populated from NLP MARINE data base in automated manner
BG.REQ.005	Simultaneously, an advisory containing field value of critical SFMS attribute consisting of beneficiary details, validity of BG, value of BG, contract number & BIC code etc will also be made available by the system to issuing Bank trough supplier to avoid mistake during StructuralFinancialMessagingSystem(SFMS)process.Thesevalueswill alsobetransmittedtoadvisingbankconcurrentlyforvalidationofe-BG
	received from issuing bank of supplier. Responsibility of correctness of BG content will rest with issuing bank and LSP itself.

E-PBG Module	
Functional Requirements	
BG.REQ.006	Paper BG of issuing bank will not be operational unless same is transmitted to advising bank through SFMS message COV 760. There is provisionforSuppliertouploadpaperBGinPDFformatbeforesending the same to buyer for their reference andscrutiny.
BG.REQ.007	Advisingbank,onreceiptoftheSFMSmessage(760COV),willcompare & validate the e_BG from the validation data base created on basis of advance information received from NLP MARINE portal. On positive validation, banker server will update the NLP MARINE server by flag “Y” and thus enabling thebuyertoplaceformalcontractonsupplier.Unlessflagis“Y”,formal contract cannot beplaced
BG.REQ.008	In case validation failed, error message will be generated with the reason of failure. Accordingly NLP MARINE portal will advise supplier for amendmentthroughCOV767messagefromissuingbank.Onreceiptof amendment through SFMS, advising bank will process the input as per above step and update the flag of NLP MARINE portalsuitably
BG.REQ.009	Advising bank will keep on alerting the buyer about the e-BG such asits expiryetc.&ifnothingreceivedadversely,capitalblockedinformofBG willbereleasedwithintimeframewhichwillultimatelyreducethecost ofprocurement.

3. Project Implementation

4.1 Project Implementation Approach

PROJECT PLANNING

Within 21 calendar days of effective date of the contract/ Issuance of LOI, BIDDER shall submit to the Department for its approval a detailed Project Plan with details of the project showing the sequence, procedure and method in which he proposes to carryouttheworks.ThePlansosubmittedbyManagedServiceProvidershallconformtothe requirements and timelines specified in the Contract. The Department and Managed Service Provider shall discuss and agree upon the work procedures to be followed for effective executionoftheworks,whichManagedServiceProviderintendstodeployandshallbeclearly specified. The Project Plan shall include but not limited to project organization, communication structure, proposed staffing, roles and responsibilities, processes and tool setstobeusedforqualityassurance,securityandconfidentialitypracticesinaccordancewith industry best practices, project plan and delivery schedule in accordance with the Contract. Approval by the Department's Representative of the Project Plan shall not relieve Bidder of any of his duties or responsibilities under theContract.

PROGRESS REPORTING

1) BIDDER shall monitor progress of all the activities related to the execution of this contract and shall submit to IPA, progress reports with reference to all related work, milestones and their progress during the implementationphase.

2) Formats for all above mentioned reports and their dissemination mechanism shall be discussed and finalized along with project plan. IPA on mutual agreement betweenbothpartiesmaychangetheformats,periodicityanddisseminationmechanismfor suchreports.

3) PeriodicmeetingsshallbeheldbetweentherepresentativesofIPAandBIDDER once in every 15 days during the implementation phase to discuss the progress of implementation. After the implementation phase is over, the meeting shall be held as an ongoing basis, as desired by IPA to discuss the performance of the contract.

4) BIDDER shall ensure that the respective solution teams involved in the execution of work are part of suchmeetings.

5) Review committees involving representative of Governance Board of NLP Marine under IPA and senior officials of BIDDER shall be formed for the purpose of this project. These committees shall meet at intervals, as decided by IPA later, to oversee the progress of the implementation.

6) At any time during the course of the Contract, IPA shall also have the right to conduct, either itself or through another agency as it may deem fit, an audit to monitor the performance by BIDDER of its obligations/ functions in accordance with the standards committed to or required by IPA and BIDDER undertakes to cooperate with and provide to IPA/ any other agency appointed by IPA, all Documents and other details as may be required by them for this purpose. Such audit shall not include BIDDER's books ofaccounts.

7) Should the rate of progress of the works or any part of them at any time fall behind the stipulated time for completion or is found to be too slow to ensure completion of the works bythestipulatedtime,orisindeviationtoTenderrequirements/standards,IPA representative shall so notify BIDDER inwriting.

8) BIDDER shall reply to the written notice giving details of the measures he proposestotaketoexpeditetheprogresssoastocompletetheworksbytheprescribedtime ortoensurecompliancetoRFPrequirements.

9) In case during execution of works, the progress falls behind schedule or does not meet the Tender

requirements, BIDDER shall deploy extra manpower/ resources to make up the progress or to meet the RFP requirements.

IMPLEMENTATION CHANGE

The bidder is expected to:

1. Conduct change management workshops (including presentation materials and related documents) before the Go Live of Pilot and before the Go Live out of RollOut.
2. Monitoring and reporting on IPA preparedness to adopt planned changes and identifying corrective actions to achieve the desired goals at alltimes.
3. BIDDER needs to submit the training and change management report after successful completion of each training session, including user feedback and duly filled in User Feedback form.
4. In addition to above, BIDDER needs to submit the consolidated training and change management report after successful completion of training(s) for eachphase
5. Rollout inPhases

Phase I	Requirement gathering and submission of SRS document
	Design and development, Cargo and Carrier Services
	Launch of Cargo and Carrier Services
Phase II	Integrated Regulatory Platform:
	Certification Module • Certification: Modules for commodity-destination pair certificationcatalogue • Certification: Integration with 30PGAs/EPCs
	Launch of Logistics National Single Window Certification System and Integrated Regulatory Platform
Phase III	**Certification Additional Modules:** Integration with remaining PGAs/EPCs Trade Finance Module
	Delivery of Complete NLP Marine

4.2 Project Milestone Plan

The project is divided into following three phases:

Phase I – Implementation: This phase would start from project initiation and would be completed once the system has been implemented. The various activities would include freezing of specifications for various components of envisaged system and data migration, application software development, testing, conference room demo of functionality, procurement & installation of hardware and required system software, network creation, and deployment of support staff for pilot.

Phase II – Stabilization and baseline: This phase would have the complete rollout of the envisaged system and all its components as defined. It would end when all transactions and the operations have stabilized for a period of 3 months. The closure includes completion of Phase II.

Phase III – Operations and Maintenance: This phase would continue till the termination of the contract. The SI would be responsible for the functioning of the system for a period of 2years and would also maintain the entire system for the same duration.

No	Milestones	Timeline T=0 at Kick-off
1	Submission and Acceptance of Detailed Business Requirement Specifications (BRS) and Software Requirement Specifications- NLP Marine	T+2 month
2	Solution Architecture and Design, including Logical and Functional Architecture of the NLP Marine System	T+3 months
3	Prototype of the design of the proposed NLP Marine – acceptance of the design by the stakeholders for the additional functionalities proposed in NLP - Marine	T+4 months
4	Development, integration and implementation of NLP Marine Module as per SRS	T+ 6 months
5	Finalization and on-boarding of all the Latch-on applications as per the agreement signed with IPA	T+8 months
6	UATs	T+10 months
7	Training & Pilot implementation	T+11 months
8	Go Live	T+12 months
9	Stabilization & fine tuning	3 months from Go Live (final)
10	O&M	2 years after Stabilization and fine tuning

4.3 Project deliverables

Deliverable No.	Deliverable Description
D1	Kick-off presentation and/or Duly signed agreement
D2	Project charter should cover the following: - Study of scope of work & functionalcoverage - Governance Structure for ProjectImplementation - Project implementationapproach - Resourcedeployment - Change & communication management plan - Change controlprocedure -Contract managementplan - Risk management and information securitypolicy - Business continuity and disaster recoveryplan - Exit managementplan - Milestone completion certificate along with documents to support milestone completionclaim
D3	Detailed Project Plan shall cover the following: - Detailed projectplan - Work breakdownstructure - Deliveryschedule - Keymilestones - Milestone completion certificate along with documents to support milestone completionclaim
D4	Master Design Document shall cover the following: - Requirements Addressed at a broader level for the project - Security andAuthentication - APIs, ExternalInterfaces - DesignConsiderations - System StructureFlows - Milestone completion certificate along with documents to support milestone completionclaim
D5- 1	Software Requirements Specifications (SRS) should cover the following: - Detailed requirement captureandanalysis - Softwarerequirement - Interfacespecifications

Deliverable No.	Deliverable Description
	- Application securityrequirements -Performance requirements - Mapping of FRS &SRS - Requirementssign-off - Identify third party interfaces required along with thetype/specifications - Milestone completion certificate along with documents to support milestone completionclaim
D6-1	System Design & Configuration report should cover the following: - System Configuration and module wise configuration needs as per the design envisaged - Legacy and Third-partySystem Integration/interface Report and integration of same with the envisagedsolutions - Customization Development Plan and Design/development plan ofcomponents of functionalities that are not available - High Level Software Design document including Software Architecture design, Logical and Physical DatabaseDesign - Low Level Software Design document including Programming Logic, Workflows and integration points andmechanisms - Milestone completion certificate along with documents to support milestone completionclaim - Low Level Software Design document including Programming Logic, Workflows and integration points andmechanisms - Milestone completion certificate along with documents to support milestone completionclaim
D7-1	Conference Room Pilot Report shall contain the following: - Pilot demonstration scripts and associated testdata - fault reports for any package errorsencountered, - Issues related to policies, procedures, package configuration values, new or modified business scenarios orscripts Milestone completion certificate along with documents to support milestone completionclaim
D8-1	Software Deployment report should cover the following: - Complete Source Code withdocumentation - Test Plans and Test cases (including Unit Test Plan, System/Integration Test Plan, User Acceptance Test Plan, Security Test Plan, Load TestPlan) - Software Testing Documentation (including details of defects/bugs/errorsand their resolution) - User Acceptance Test Cases, Test Data and Test Results, User Acceptance Test Scripts, Unit Test Cases, Integration Test Results/Cases - System Integration Tests (SIT) including Performance Tests(PT) - Challan of license procurement or verification through online portalof OEM - Periodic data backup and archival post Go-Live. Backup data should be tested for

Deliverable No.	Deliverable Description
	restorability on a quarterlybasis. -Milestone completion certificate along with documents to support milestone completion claim
D8	Overall System Deployment report should cover the following: - Deployment sign-off from IPA/portofficials - User Manuals and SystemManuals - Go-Live Certificate indicating readiness for roll-out with trainings - Pending Issues in the system,Dependencies - Updated System Design documents, specifications for every changerequest - Updated user Manuals, administration manuals, trainingmanuals System stabilization report should cover the following: - Report indicating results, observations and actionitems - UATSign-off - Latest source code, application deployment files, configuration files for entire solution - Detailed changesdescription -Details on the overall applications deployed in respective ports -Submission of all scanned files as per requirements of ports -Exit Management Plan of the BIDDER in case of termination of the project/ expiring of the tenure of the project Milestone completion certificate along with documents to support milestone completionclaim
D9	Submission of Master Data migration design report should cover the following: - Data migrationassessment - Migration & transitioningapproach Milestone completion certificate along with documents to support milestone completionclaim
D10	Cloud enabled Data centres establishment report should cover the following: - Specifications & Design of DC&DRC - Installation&CommissioningofDC&DRCdetailedplan

Deliverable No.	Deliverable Description
D11	SLA Compliance Reports (Monthly) should cover the following: - Performance Monitoring reports forsystem - SLA ComplianceReports - Patches/ Upgrades of allcomponents - Incremental updates tosolution - Change RequestsManaged - Issue/ Problem/ Bugs/DefectTracker - IT facility management services reviewreport - Scanning & digitization completion &review - On-Going ProjectUpdates - Audit/ Standard ComplianceReports Milestone completion certificate along with documents to support milestone completionclaim
D12	The report for BCP-DR Drill for two days should include: -The duration taken for DR migration - The list of functionalities successfully working throughDR. -The health reports of infrastructure and applications. Milestone completion certificate along with documents to support milestone completionclaim
D13	Master Design Document covering integration and interfacing requirements for all functionalities as envisaged in the project - Milestone completion certificate along with documents to support milestone completion claim
D14	Submission of application for UAT report should include: - Development and integration of application code of all functionalities; -sign off of Unit, Integration and system testing completion. -Test execution actuals reports with expected output.
D16	Go-live of user training mobile app should include: -Sign off from IPA/port users on UI design including the various screen -Beta version -Acceptance testing sign from IPA/port users - Milestone completion certificate along with documents to support milestone completion claim

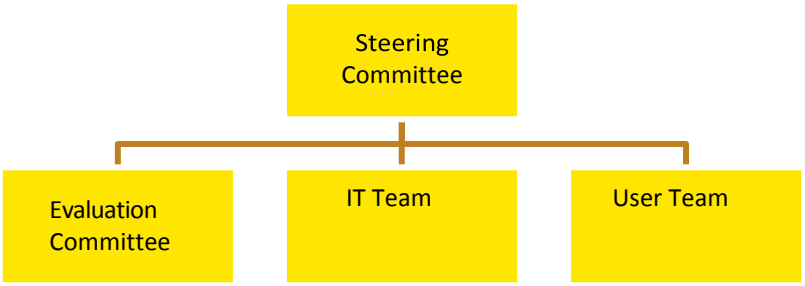
Deliverable No.	Deliverable Description
D17	Initiation of exit management plan as per plan should include Milestone completion certificate along with documents to support milestone completion claim

4. Governance

5.1 Governance Structure

Putting a governance structure around future IT potential (surrounding this solution or any other envisaged solution)isessentialtoensurethatprojectimplementationstaysontrackandachievesitsstrategiesandgoals. It acts as a mechanism to measure the progress of the implementation. Also, the port solutions today are subject to many regulations. An IT governance framework is an efficient system to ensure compliance. As part of the project governance, each Port shall appoint threecommittees:

- AnEvaluation Committee, which shall evaluate the business solutions proposed by the BIDDERs as well as the projecttimelines
- IT team, which will interact with the BIDDER and steeringcommittee.
- A User Team, along with member of IT team will evaluate the fit of the workflows as proposed by the BIDDER. In addition, this team will be involved in the UAT during the implementationphase.



5.1.1 Project Steering Committee

TheSCplaysakeyroleinguidingandadvisingontheprojectimplementationandthesystemictransformation that the project aims at. The SC shall monitor project implementation at a broader level by coordinating with other committees. Primary responsibility of Steering Committee would be to provide project oversight and monitoring work of implemented and operationcommittee.

Responsibilities of the user committee shall be:

- Vetting of all deliverables at all locations on clearance ofsites
- Monitoring installation, implementation, operations and monthlybilling
- Liaising with other committees to provide directions andguidance
- Resolve issues arising during implementation andoperations

5.1.2 IT Team

The responsibilities of the IT team shallbe:

- Providing support during contract finalization with final selectedBIDDER
- Support during project implementation including thefollowing
- Project management, monitoring and evaluation during the project development phase after selection of BIDDER to ensure adherence to the project timelines andrequirements
- Review the project plan submitted byBIDDER
- Assist in reviewing the periodic reports and deliverables submitted by BIDDER. Highlight deviations/issues in deliverables of BIDDER and assist in itsresolution
- Provide assistancein preparing guidelines to conduct testing and acceptance of the solution developed by the BIDDER including hardware, software and ITinfrastructure
- Monitorandmaintainissuetrackerandkeeponupdatingthestatusofalltheissues fromtime to time
- Define escalation mechanism for timely resolution of issues andrisks

5.1.3 GOVERNANCE SCHEDULE

- The BIDDER shall document the agreed structures in a procedural manual under the guidance and supervision of the NodelOffice of eachport.
- The agenda for each meeting of the Steering Committee and other committees shall be set to reflect the discussion items related to the scope of work and additional items may be added either with the agreement of the Parties or at the request of eitherParty.
- Copies of the agenda for meetings along with relevant pre-reading material, shall bedistributed.
- All meetings and proceedings will be documented; such documents to be distributed to both Parties andcopiesshallbekeptasarecord.Allactions,responsibilitiesandaccountabilitiesarisingout ofany meeting shall be tracked andmanaged.
- The Parties shall ensure as far as reasonably practicable that the above formed committees shall resolve the issues and resolve the objectives placed before them and members representing thatParty are empowered to make relevant decisions or have easy access to empowered individuals for decisions to be made to achievethis.
- The Parties will proceed in good faith so that the Steering Committee shall resolve the issues and smoothen the performance of theProject.
- The partiesagreetoattempttoresolvealldisputesarisingundertheAgreement,equitablyandingood faith. To this end, the parties agree to provide frank, candid and timely disclosure of all relevant facts, information and documents to facilitate discussions between them/their representatives or senior officers.

5.1.4 Key Personnel

Sr. No.	Level	Min. No. of People	Minimum Onsite Deployment	
			Phase I & II	During Phase III
1.	Project Director	1	10%	10%
2.	Project Manager	1	100%	100% for first 6 months after Go-Live, 25% afterwards
3.	Project Leads at each Port location (Haldia is considered as sixth location)	6	100%	
4.	Functional Leads	10	100%	100% for first 6 months after Go-Live, 25% afterwards
5.	Network Architect	1	100%	100% for first 6 months after Go-Live,

Sr. No.	Level	Min. No. of People	Minimum Onsite Deployment	
			Phase I & II	During Phase III
				25% afterwards
6.	Solution Architect	1	100%	100% for first 6 months after Go-Live, 25% afterwards
7.	Data Centre Specialist	1	100%	100% for first 6 months after Go-Live, 25% afterwards
8.	Database Administrators	2	100%	100% for first 6 months after Go-Live, 25% afterwards
9.	Trainers/ Change Management Specialists	12	100%	100% for first 6 months after Go-Live, 25% afterwards
10.	Technical Support Team at each Port	12	100%	100% for first 6 months after Go-Live, 25% afterwards
11	IT Helpdesk executives at centre	5	As required	100%
12	IT Helpdesk executives at ports (Minimum 3 per port)	18	As required	100%

5.2 Acceptance Procedure of Deliverables

SI is responsible for providing all the deliverable's to IPA as defined in project deliverables. All the project deliverables shall be submitted by SI for approval through Project Management Information system (PMIS) only. This system will be developed by SI as a part of system development.

#	Sequence of Activities	Medium	Actor
1	Deliverable acceptance	PMIS	
1.1	SI shall upload the deliverables in the system for approval by respective authorities (IPA and port). And also send an email to designated email addresses along with the deliverable. Soft copy (by e-mail) and two (2) printed drafts of all deliverables shall be submitted to IPA / Port (one for IPA and one for port). Source code however need not be submitted in hard copy		SI
1.2	IPA / Port will review the deliverables and either accept the deliverable or provide feedback on changes to be done in writing within a reasonable period of time The SI shall make the appropriate revisions and shall resubmit the updated final version to IPA / Port or their verification and feedback/acceptance The SI should strive to submit the deliverables in parts for getting continuous feedback on the deliverables. The SI should also engage with IPA / Port on a		SI / IPA / Port

#	Sequence of Activities	Medium	Actor
	continuous basis through meetings (weekly till 6 months after Go-live and fortnightly after this period) and periodic workshops to ensure that progress may be reviewed and feedback provided from time-to-time. Please note that the timelines indicated above are timelines for submission of final deliverables. SI should plan to submit the draft versions of deliverables before the timelines indicated above to allow reasonable time for review and acceptance by the time indicated above.		
1.3	Based on an mutually agreed workflow enabled through PMIS, IPA & Port user will approve the deliverables		IPA & Port
2	Payment authorization	PMIS	
2.1	Only when the deliverables are approved within the PMIS, SI shall raise payment request		SI
2.2	Port user shall authorize the payment request within PMIS		IPA & Port
3	Payment release from funds	Offline	
3.2	Once the payment request is authorized, IPA shall release the payment and shall intimate the port user		IPA
4	Status update of payment	PMIS	
4.1	Once the payment release intimation is received from IPA, port user will update the Payment release status in the system		IPA/port user

5.3 Service Level Agreement

The bidder 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 100 or above. The bidder will get lesser payment in case of a lower performance exhibited by a SLA score of less than 100. The maximum penalty to be levied is 10% of Quarterly Payout. The payments will be as per terms defined under Schedule VI of Volume III of this tender.

The payment will be made by IPA to the bidder on quarterly basis. The quarterly invoice will be submitted by the bidder to the IPA, 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 payments will be released subject to acceptance procedure.

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, until and unless decided or agreed with IPA. The SLA holiday period is for streamlining the SLA measurement and monitoring process of the project.

The payment and SLA penalty applicability will be depending on the impact.

The SLA has been divided into two Parts

A. During implementation till Go-live
   Milestone pay-out: Here the penalty will be applicable separately against the payment being made as per payment schedule defined under payment schedule of Volume 1

B. After Go-live (2 years during Phase III)
On-actual pay-out: The total Quarterly Payment will be derived after SLA applicability as per payment schedule defined under volume I

IPA 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. IPA and bidder.

The Penalties will be calculated based on the following table:

S. No.	SLA Score Range	Deductions (Penalties)
Deductions		
1	<=100 &>=95	0.25 % penalty for every point < 100
2	<95 &>=90	0.5 % penalty for every point < 100
3	<90	0.75 % penalty for every point < 100
Note: The percentage penalty would be calculated on the bill raised by the SI for the concerned quarter.		
Example: • SLA Score of 98 will lead to a Penalty of 0.5% (i.e. 2 x 0.25 = 0.5%) • SLA Score of 93 will lead to a Penalty of 3.5% (i.e. 7 x 0.5 = 3.5%) • SLA Score of 88 will lead to a Penalty of 9% (i.e. 12 x 0.75 = 9%)		

Note

1 Annual review SLA shall be done by IPA 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 SLA monitoring tool providing reports against the parameters mentioned below will be used for measurement. IPA and port 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 Data other than EMS or modification to EMS data for SLA monitoring has to be preapproved.
5 Implementation of a Web-based Project progress and SLA monitoring has to be carried out by before Go-live I in order to receive any payment for the project

SLA During Phase I and II: Implementation and Stabilization				
#	**Parameter**	**Metric**	**Penalty**	**Measurement**
1	Adherence to timeline for Go-live	Up to 4 calendar weeks delay from the timelines as mentioned Volume II	No Penalty	Go-live certificate
		Delay beyond 4 week up to 8 calendar weeks	INR XXXXX per week delay per port milestone	
		Any delay beyond 8 calendar weeks	INR XXXXX per week delay per port milestone ,	

SLA During Phase I and II: Implementation and Stabilization				
#	**Parameter**	**Metric**	**Penalty**	**Measurement**
2	Substitution of resources from those CVs provided during the technical evaluation	No substitution of resources will be allowed whose CVs have been provided along with the technical bid for the period XX months from the commencement of Project (other than unavoidable reasons e.g. death, disability, departure from the firm, etc.)	Penalty of INR XXXXX per substitution of resources whose CVs have been provided along with the technical bid	Request submitted for substitution along with project plan or thereafter

SLA Parameters during Operations and Maintenance Period							
Parameter	**Baseline**		**Lower Performance**		**Breach**		**Measurement**
	Metric	**Score**	**Metric**	**Score**	**Metric**	**Score**	
Application							
Availability for applications							
Availability (uptime) of applications for doing business activities, except during scheduled down time as agreed with the department Uptime = {1 - [(Application downtime – maintenance Downtime) / (Total Time – Maintenance Downtime)]}	>=99.5%	5	<99.5% to>= 99%	3	<99%	-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.

SLA Parameters during Operations and Maintenance Period							
Parameter	**Baseline**		**Lower Performance**		**Breach**		**Measurement**
	Metric	**Score**	**Metric**	**Score**	**Metric**	**Score**	
Time for opening of Home Page of portal Average must be achieved with maximum homepage opening time till success for 90% or more of the sample cases being within the stipulated time Web-to-web response time. Time for Home page opening, time for online submission of electronic documents, time for uploading and etc from <= operator to >= operator	<=3 seconds	3	> 3 seconds and <=5 seconds	1	>5 seconds	-1	Automated measurement tool to be developed as part of SLA monitoring tool to provide metric values against this parameter.
Time for on-line submission of the electronic forms 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	<=5 seconds	3	>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.
Time for uploading data file including xml, txt, etc. (other than images and pdf) on various portals Average must be achieved with maximum time till success for 90% or more of the total uploads within the stipulated time Web-to-web response time	<=20 seconds	3	> 20 seconds and <=30 seconds	2	> 30 seconds	-1	Automated measurement tool to be developed as part of SLA monitoring tool to provide metric values against this parameter.
Time for re-sending of the intimation/alerts through email or mobile app from the date of receipt of information of non-delivery.	<= 30 mins	3	>30 mins to <= 4 hours	0.5	>4 hrs	-1	Automated measurement tool to be developed as part of SLA monitoring tool to provide

SLA Parameters during Operations and Maintenance Period							
Parameter	**Baseline**		**Lower Performance**		**Breach**		**Measurement**
	Metric	**Score**	**Metric**	**Score**	**Metric**	**Score**	
							metric values against this parameter.
Application							
Availability (uptime) of applications for doing business activities, except during scheduled down time as agreed with the department Uptime = {1 - [(Application downtime – maintenance Downtime) / (Total Time – Maintenance Downtime)]}	>=99.5%	5	<99.5% to>= 99%	3	<99%	-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.
Time for on-line submission of the electronic forms 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	<=5 seconds	3	> 5 seconds and > =7 seconds	1	>7 seconds	-2	Automated measurement tool to be developed as part of SLA monitoring tool to provide metric values against this parameter.
Time for uploading data file including xml, txt, etc. (other than images and pdf) on various portals Average must be achieved with maximum time till success for 90% or more of the total uploads within the stipulated time Web-to-web response time Time for re-sending of the intimation/alerts	<=20 seconds	3	>20 seconds to < =30 seconds	2	>30 seconds	-2	Automated measurement tool to be developed as part of SLA monitoring tool to provide metric values against this parameter.
	<= 30 mins	3	>30 mins to <= 4 hours	0.5	>4 hours	-2	Automated measurement tool to be developed as part of SLA monitoring tool

SLA Parameters during Operations and Maintenance Period							
Parameter	**Baseline**		**Lower Performance**		**Breach**		**Measurement**
	Metric	**Score**	**Metric**	**Score**	**Metric**	**Score**	
through email or mobile app from the date of receipt of information of non-delivery.							to provide metric values against this parameter.
API service availability							
Availability of API services for mobile, portal and other third party applications	>=99.5%	5	<99.5% and >=99%	3	<99%	-2	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	3	> 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							
Time to deliver the application changes as per desired functionality.	Within Agreed timeline	3	NA	NA	Beyond Agreed timeline	-1	Reports regarding the same to be captured

SLA Parameters during Operations and Maintenance Period							
Parameter	**Baseline**		**Lower Performance**		**Breach**		**Measurement**
	Metric	**Score**	**Metric**	**Score**	**Metric**	**Score**	
							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 (FRS, SRS, User, Training Manual etc.), application version control,	at the end of every quarter	3	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 IPA/ports) and emails to provide these details
Integration and interfacing							
Data exchange with defined system							
Time to post information in form of messages after the transaction carried out within defined system	<=10 seconds	3	>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 after receipt of same from system in form of messages	<=5 seconds	3	>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.
Time to reconcile all messages exchanged (received and posted with the defined system)	<=24 hours	3	NA	NA	Beyond 24 hours	-1	Automated measurement tool to be developed as part of SLA

SLA Parameters during Operations and Maintenance Period							
Parameter	**Baseline**		**Lower Performance**		**Breach**		**Measurement**
	Metric	**Score**	**Metric**	**Score**	**Metric**	**Score**	
							monitoring tool to provide metric values against this parameter.
Data exchange with other systems							
Time to post information to other system in form of messages after the transaction carried out within the defined system	as agreed at the time of design	3	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 other system after receipt of same from the defined system in form of messages	as agreed at the time of design	3	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							

SLA Parameters during Operations and Maintenance Period							
Parameter	**Baseline**		**Lower Performance**		**Breach**		**Measurement**
	Metric	**Score**	**Metric**	**Score**	**Metric**	**Score**	
Uptime of all components at DC, (Network infrastructure related) & DR including but not limited to: · Servers · Storage · Tape Library · SAN · Switches · Routers Any downtime for maintenance shall be with prior written intimation and approval of IPA . Uptime = {1 - [(Component downtime – maintenance Downtime) / (Total Time – Maintenance Downtime)]}	>=99.5%	5	<99.5% and >=99%	3	<99%	-3	Automated measurement tool (EMS) 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.
Security Components Availability							

SLA Parameters during Operations and Maintenance Period							
Parameter	**Baseline**		**Lower Performance**		**Breach**		**Measurement**
	Metric	**Score**	**Metric**	**Score**	**Metric**	**Score**	
Uptime of all security components for DC and BCP/DR site including but not limited to: · Perimeter Security · Firewall etc. Any downtime for maintenance shall be with prior written intimation and approval of IPA. Uptime = {1 - [(Component downtime – maintenance Downtime) / (Total Time – Maintenance Downtime)]}	>99%	5	< 99% to >= 98%	3	<98%	-3	Automated measurement tool (EMS) 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.
IT Infrastructure Monitoring Availability							
Availability of IT Infrastructure Monitoring Tools (IT Infrastructure Monitoring Tools) at the active site.	>99%	5	< 99% to >= 98%	2	<98%	-2	Automated measurement tool (EMS) 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	3	NA	NA	CPU utilization is more than 80% for a sustained period of more than 4 hours	equal to n Where n is number of such instances in the reporting period	Automated measurement tool (EMS) 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.
*Helpdesk 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 quarter.	<=2 hrs	5	>2 hrs and<=8 hrs	1	> 8 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	3	> 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 medium level incident	<=4 hours	3	> 4 hours to < = 8 hrs	1	> 8 Hours	-1	Automated measurement tool (reports

SLA Parameters during Operations and Maintenance Period							
Parameter	**Baseline**		**Lower Performance**		**Breach**		**Measurement**
	Metric	**Score**	**Metric**	**Score**	**Metric**	**Score**	
							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	3	>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%	3	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							

SLA Parameters during Operations and Maintenance Period							
Parameter	**Baseline**		**Lower Performance**		**Breach**		**Measurement**
	Metric	**Score**	**Metric**	**Score**	**Metric**	**Score**	
Update of training materials on portals within 1 week from date of release of modification to software into production environment	Within 1 Week	2	upto 2 weeks	1	more than 2 weeks	-1	Automated measurement tool (reports from PMIS) to be developed as part of SLA monitoring tool to provide metric values against this parameter.
Other Parameters							
Manpower availability							
Manpower availability measures the availability of the required skill sets as proposed by the Si 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: • Key Personnel as per Volume I of RFP • Team Leads for each of the tracks/areas • Team members for various skills required for carrying out the activities of the project • Minimum committed resources for helpdesk • Production Support Team	No Deviation	3	NA	NA	In case of deviations	-1	All deviations would be recorded and report shall be made available to the IPA

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: - 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	Within 2 days from month end	3	NA	NA	Greater than 2 days	-1	reports to provide metric values against this parameter.

* Classification for Helpdesk services

Severity level	Severity Particulars	Service window
Critical	Outage that does not impact PORT SERVICES	24*7
Medium	Outage that does not impact PORT SERVICES but affects department services	24*7
Low	Upgrade, shifting and preventive maintenance	7am to 7pm (Monday to Saturday)

* Classification for Helpdesk services

Severity level	Severity Particulars	Service window
Critical	Outage that does not impact PORT SERVICES	24*7
Medium	Outage that does not impact PORT SERVICES but affects department services	24*7
Low	Upgrade, shifting and preventive maintenance	7am to 7pm (Monday to Saturday)

5. Bill of Material

Indicative information for DC and DR cloud infrastructure environment. The figures provided within the Bill of material are indicative for estimation purpose only. Bidder has to perform an independent assessment of the Infrastructure requirements for the 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.

6.1 Data Centre Infrastructure – Production

S. No	Server / Device name	Min. Indicative Quantity	Server Model	Server Role
1	Application Server	02	Virtual	Application
2	Web Server	02	Virtual	Application - Content
3	Database Server	02	Virtual	Database
4	FTP Server	02	Virtual	SFTP
5	NFS Server	02	Virtual	NFS
6	Web Application Firewall (WAF) Server	02	Virtual	GATEWAY, WAF
7	API Manager &Analytics Server	02	Virtual	API Connect
8	API Portal Server	02	Virtual	API Portal
9	ESB / Integration Server	02	Virtual	App Connect
10	Log / SIEM Server	02	Virtual	SIME Collector
11	Privileged Identity Management (PIM) Server	02	Virtual	PIM Server
12	Active Directory (AD) Server	02	Virtual	Domain Controller
13	Helpdesk Server	02	Virtual	Support Tool
14	Reporting Server	02	Virtual	
15	Security / HSM Server	As required	Virtual	Security
16	Encryption Server	02	Virtual	File Encryption
17	Backup and Archival Server	02	Virtual	Data Backup
18	Other Servers	As required	Virtual	

6.2 Data Centre Infrastructure – UAT / QA

S. No	Server / Device name	Min. Indicative Quantity	Server Model	Server Role
1	Application Server	01	Virtual	Application
2	Web Server	01	Virtual	Application - Content
3	Database Server	01	Virtual	Database
4	FTP Server	01	Virtual	SFTP
5	NFS Server	01	Virtual	NFS
6	Web Application Firewall (WAF) Server	01	Virtual	GATEWAY, WAF
7	API Manager &Analytics Server	01	Virtual	API Connect
8	API Portal Server	01	Virtual	API Portal
9	ESB / Integration Server	01	Virtual	App Connect
10	Helpdesk Server	02	Virtual	Support Tool
11	Reporting Server	02	Virtual	
12	Security / HSM Server	01	Virtual	Security
13	Encryption Server	01	Virtual	File Encryption
14	Other Servers	As required	Virtual	

6.3 Data Centre Infrastructure - Staging

S. No	Server / Device name	Min. Indicative Quantity	Server Model	Server Role
1	Application Server	02	Virtual	Application
2	Web Server	02	Virtual	Application - Content
3	Database Server	02	Virtual	Database
4	FTP Server	01	Virtual	SFTP
5	NFS Server	01	Virtual	NFS
6	Web Application Firewall (WAF) Server	01	Virtual	GATEWAY, WAF
7	API Manager &Analytics Server	01	Virtual	API Connect
8	API Portal Server	01	Virtual	API Portal
9	ESB / Integration Server	01	Virtual	App Connect
10	Security / HSM Server	01	Virtual	Security
11	Encryption Server	01	Virtual	File Encryption
12	Other Servers	As required	Virtual	

6.4 Disaster Recovery Infrastructure

Functional DR with at least 50% compute capacity and 100% storage as that of Primary site.

S. No	Server / Device name	Min. Indicative Quantity	Server Model	Server Role
1	Application Server	01	Virtual	Application
2	Web Server	01	Virtual	Application - Content
3	Database Server	01	Virtual	Database
4	FTP Server	01	Virtual	SFTP
5	NFS Server	01	Virtual	NFS
6	Web Application Firewall (WAF) Server	01	Virtual	GATEWAY, WAF
7	API Manager &Analytics Server	01	Virtual	API Connect
8	API Portal Server	01	Virtual	API Portal
9	ESB / Integration Server	01	Virtual	App Connect
10	Log / SIEM Server	01	Virtual	SIME Collector
11	Privileged Identity Management (PIM) Server	01	Virtual	PIM Server
12	Active Directory (AD) Server	01	Virtual	Domain Controller
13	Helpdesk Server	01	Virtual	Support Tool
14	Reporting Server	01	Virtual	
15	Security / HSM Server	As required	Virtual	Security
16	Encryption Server	01	Virtual	File Encryption
17	Backup and Archival Server	01	Virtual	Data Backup
18	Other Servers	As required	Virtual	

6. Operation and Maintenance

The BIDDER shall be responsible for the overall management of NLP MARINE assistance for a period of 5 years (from the effective date of implementation) including the NLP MARINE software and entire related ICT Infrastructure. The operation and maintenance phase shall commence after Go-Live of the NLP MARINE.

BIDDER shall provide automated tool-based monitoring of all performance indices and online reporting system for SLAs defined in this document. The tools must have the capability for the IPA to log in anytime to see the status.

Additionally, BIDDER must also prepare and submit the, Monthly and Quarterly SLA report during Operation and Maintenance phase based on the SLAs provided in the document.

Besides the SLA reports BIDDER also need to annually submit the following:

- Certification stating all patches/ upgrades/ service releases has been properly installed
- Asset Information Register
- Standard operating procedure
- Updated Project Exit Management Plan

Further, at the last quarter of Operation and Management phase BIDDER needs to submit the Project Exit report.

The broad activities to be undertaken by the BIDDER during the operation and maintenance phase are discussed in subsequent paragraphs.

7.1 Providing applications, support and Maintenance

1. During the contract period, the BIDDER shall be completely responsible for defect free functioning of the application software and shall resolve any issues that include bug fixing, improvements in presentation and/or functionality and others at no additional cost during the operations & maintenance period, within a duration specified in SLA.
2. The BIDDER shall be responsible including but not limitedto:
    a. Providing for warranty/support for the software (Application/system/support) Developed/Customized
    b. Ensuring compliance to uptime and performance requirements of NLP MARINE as indicated in the SLA
    c. Management of Integration Component including the Component for integrating with PCS 1x and external agencies, payment gateway and any third-party component used in the application software
    d. Providing and installing patches and upgrades without any additional cost for contract period for the quoted hardware, software, etc. In case the software patches are not available free of charge, the cost of the same must be included in the contract price
    e. Ensuring timely resolution and fixing of bug/defects reported
    f. Undertaking performance tuning of the System (application and database) to enhance System's performance and comply with SLA requirements on a continuous basis
    g. Version management, License Management and software documentation management, reflecting current features and functionality of the solution
3. AllplannedchangestotheapplicationsystemsshallbecoordinatedwithintheestablishedChange Control processes to ensurethat:
    a. Appropriate communication on change required has takenplace
    b. Proper approvals have beenreceived
    c. Schedules have been adjusted to minimize impact on the productionenvironment.
4. TheBIDDERshalldefinetheSoftwareChangeManagement&Versioncontrolprocessandobtain approval for the same from the IPA. For any changes to the software, the BIDDER has to prepare detailed documentation including proposed changes, impact to the System in terms of functional outcomes/additional features added to the Systemetc.
5. TheBIDDERisrequiredtoobtainapprovalfromtheIPAforalltheproposedchangesbefore implementation of the same into production environment and such documentation is subject to review at the end of each quarter of operations & maintenancesupport.
6. Any changes/upgrades to the software performed during the operations & maintenance phase shall be

subjected to comprehensive & integrated testing by the BIDDER to ensure that the changes implemented in the system meets the desired and specified requirements of the IPA and doesn't impact any other function of theSystem.

7.2 Infrastructure Maintenance

1. The BIDDER shall be responsible for the overall administration and management of the NLP MARINE including the related ICT Infrastructure. The BIDDER shall be responsible includes but not limited to:
    a. Maintenance of Hardware and Server System at Cloud DC and DR
    b. Undertaking of performance tuning of the Hardware System to enhance Systems performance and comply with SLA requirements on a continuous basis.
    c. 24x7 monitoring & management of availability & security of the infrastructure & assets (including data, servers, systems etc.)
    d. Monitoring and recording ICT infrastructure performance at all locations and taking corrective actions to ensure performance optimization on a daily basis
7. The BIDDER shall escalate and co-ordinate with SDC and IPA for problem resolution wherever required.
8. In case of any confusion of the genesis of a problem between the BIDDER, DC and DR and the problem getting traced to the BIDDER, the entire delay in resolving the problem shall be attributed to the BIDDER and shall be used in measuring the Service Levels. An appropriate mechanism has to be suggested by the BIDDER, as part of the SRS, for clearly identifying the source of various types of problems.
9. The BIDDER shall enable audit logs for the Servers, System activities and such audit logs shall be analyzed at regular intervals to identify and address security and performance issues. The BIDDER shall also produce and maintain system audit logs on the System for a period agreed to with the IPA. On expiry of the said period the audit logs must be archived and stored off-site at a location agreed to with the IPA.

    a. The BIDDER shall co-ordinate with all external agencies/vendors during this period for addressing any issues arising out of the project.

    b. calamities and proven mishandling of the equipment by the operators of the IPA.

    c. The BIDDER shall provide comprehensive AMC for the entire hardware infrastructure at the client DC and DR locationsfor the entire contractperiod.

7.3 Providing Information Security Services

a) The BIDDER shall be responsible for ensuring overall information security of the NLP MARINE, including but not limitedto:

    1) WebPortal
    2) Applicationsoftware
    3) SystemSoftware
    4) SupportSoftware
    5) Data,
    6) Information, etc.

b) TheBIDDERshallberesponsiblefortheregularupdateofthesecuritypolicyasformulatedduring project development/ customizationphase.

c) The BIDDER is responsible for implementing measures to ensure complete security of the NLP MARINE (including its entire environment) and confidentiality of the related data, in conformity with the security policy of the NLP MARINE (framed by the BIDDER in consultation with the IPA).

d) The BIDDER shall be responsible for guarding the Systems against virus, malware, spyware and spam infections using the latest Antivirus corporate/Enterprise edition suites which include anti- malware, anti-spyware and anti-spam solution for the entire NLP MARINE solutiondeployment.

e) The BIDDER shall monitor security and intrusions, which mandatorily shall include taking necessary preventive and correctiveactions.

f) The BIDDER, with appropriate co-operation of the IPA shall manage the response to security incidents. The incident response process shall seek to limit damage and shall include the investigation of the incident and notification to the appropriate authorities. A summary of all security incidents must be made available to the IPA on a weekly basis; however the significant security incidents must be reported immediately on occurrence of theincident.

g) The BIDDER shall have to maintain strict privacy and confidentiality of all the data it gets access to and adequate provisions shall be made not to allow unrestricted access to the data. The BIDDER cannot sell or part with any data in anyform.

h) The above security services are subject to guidelines/ procedures of hosting server and other ICT equipment at DC/DRfacility.

7.4 Setting Up and Management of Helpdesk

This will include providing manpower & other field support staff.

a) The BIDDER shall be required to provide Helpdesk services (Technical and Operational Helpdesk) to enable effective support to the users for technical issues regarding the NLP MARINE.

b) BIDDER shall ensure helpdesk facility shall havefollowing:
- Call logging mechanism throughPhone
- Call logging mechanism throughe-mail
- Call logging mechanism throughportal

c) The BIDDER shall provide at least the following services:
- Provision and supervision of personnel for the help-desk. Minimum qualification requirements for personnel for this process are stated in the document.
- All grievances shall be assigned a ticket number and the number shall be made available to the user along with the identification of the agent, without the user having to make a request in this regard, at the beginning of the interaction.
- Helpdesk shall provide support for technical queries and other software related issues arising during day to day operations
- The Physical space for the helpdesk and any other required infrastructure shall be provided by the BIDDER
- The BIDDER shall adhere to the service level agreement with respect to the resolution of issues at various levels.
- The interactions shall also be recorded, and the records maintained for reference for a period of 1 month from the date of resolution of the problem.
- All complaints/ grievances of users shall be recorded and followed up for resolution and an escalation matrix to be developed for any delay in resolution.
- The Technical team must register the complaints to the Helpdesk for the server/network/Application related problems. It shall be ensured that the complaints lodged by the technical team must be on High Priority Basis.
- There shall be multi-lingual helpdesk support. The multi-lingual helpdesk support shall be in Hindi, English, and shall include more languages over period of time as per the requirement

d) The BIDDER shall provide the following helpdesk performance monitoring reports–
Calls per week, month or otherperiod;

- Numeric and graphical representation of callvolume
- Calls for each interaction tracked by type (calls for information on specific service, calls for specificenquiries)
- Number of dropped calls after answering,including:
  - Calls that ended while on hold, indicating that the caller hungup;
  - Call that ended due to entry errors using the automated system, indicating difficulty in using thesystem

Helpdesk:

ThescopeofworkfortheHelpdeskforNLP MARINEcanbebroadlycategorizedunderthefollowingareas:

- Business Services – Technical Helpdesk and OperationalHelpdesk
- Call Centre infrastructure andtechnology
- Resources onboarding andtraining
- Monitoring andReporting

Below table provides a broad overview of the scope of work:

Category	Scope of Work
A. Business Services	Technical helpdesk
	Operational helpdesk
B.Resources on-boarding and training	Selection of manpower
	Decide help desk model
	Provide required training
C.Monitoring and Reporting	Maintain unique call ID
	Generate regular reports of calls
	Respond to statutory bodies and law enforcement agencies

7.5 Training and Capacity Building

1. BIDDER needs to execute the Change management and capacity building activity as per the approved Change Management and Capacity Building Plan prepared by the BIDDER and approved by the IPA at the software Solution Analysis & DesignStage.
2. The BIDDER should prepare required training material and manuals
3. The BIDDER shall conduct the training at IPA office in New Delhi and/or online using tools like Zoom, TEAMS or equivalent
4. The BIDDER is required to impart the following types of training to ensure smooth implementation ofNLP MARINE.

- **Functional user training –** Providing on-the-job training on the specific modules, sub modules being implemented related application system underNLP MARINE.
- **Applicationadministrationtraining-**Applicationadministrationtrainingshallbeprovidedto keyadministratorswhoshallbedesignatedassuperusershavingadministrativerightsofthe application.ThebasictrainingtotheseadministratorsshallbeprovidedbytheBIDDERinthe areasof:
    - Management of accessrights
    - Recoveries and Backupsmanagement
    - Database administration,etc.

a) A detailed calendar of training, with the exact trainings shall be finalized after detailed discussions with all the key stakeholders of the NLP MARINE project. The date schedule shall be prepared for each section as per the availability of the concernedofficials.

b) The duration of the training shall be jointly decided by IPA and BIDDER, however, the duration shall be sufficient to meet the training requirements of the user and facilitate userincarryingouttheroutineactivitiesonsystem.

c) BIDDER shall also develop an e-training module to facilitate online training by the user by downloading it andpractice.

d) The Training sessions must be participative in nature and BIDDER must respond to the queries/ doubts of theuser.

e) BIDDER shall also adopt the train the trainer approach and create champions amongst the user offices, so that the training usage on the job becomes moresustainable.

7. Annexures

8.1 Annexure - I

8.1.1 Major Ports on PCS 1x

- Deendayal Port Trust, Kandla
- Mumbai Port Trust
- Jawaharlal Nehru Port Trust
- Mormugao Port Trust
- New Mangalore Port Trust
- Cochin Port Trust
- V.O Chidambaranar Port Trust, Tuticorin
- Chennai Port Trust
- Kamarajar Port Ltd, Ennore
- Visakhapatnam Port Trust
- Paradip Port Trust
- Syama Prasad Mukherjee Port Trust, Kolkata Including Haldia Dock Complex)

8.1.2 Non-Major Ports on PCS 1x

- Mundra Port
- Pipavav Port
- Hazira Port
- Dahej Port
- Konkan LNG Pvt Ltd
- PNP Port, Dharamtar
- Angre Port Pvt. Ltd.
- Kakinada Sea Port
- Redi Port Ltd.
- Finolex Terminals
- Indo Energy International Ltd
- Sikka Port

This section contains the CFS and ICD onboarded on PCS Ver 1x. These have to be taken up under the scope of this RFP.

8.1.3 Container Freight Station on PCS 1x

- A.L. LOGISTICS PVT LTD
- CENTURY PLYBOARDS (I) LTD.
- CENTURY PLYBOARDS (I) LTD.
- CONTAINER CORPORATION OF INDIA LIMI
- CENTRAL WAREHOUSING CORPORATION 3 CENTRAL WAREHOUSING CORPORATION
- RALSON PETROCHEMICALS LIMITED
- SEAWAYS LINER AGENCIES PVT.LTD.
- BALMER LAWRIE & CO LTD
- PLPL1
- APEEJAY LOGISTICS PARK PVT.LTD.
- NEPAL TRANSIT AND WAREHOUSING CO LTD
- TRANSWORLD TERMINALS PVT LTD
- All cargo Logistics Limited
- KERN ENTERPRISES PVT LTD
- KSWC CONTAINER FREIGHT STATION
- GATEWAY DISTRIPARKS KERALA LTD
- MIV Logistics Pvt. Ltd.

- Triway Container Freight Station Private Limited
- APM
- APEEJAY INFRALOGISTICS PVT.LTD
- LCL LOGISTIX (INDIA) PVT. LTD.
- A.L. LOGISTICS PVT.LTD.
- RALSON PETROCHEMICALS LIMITED
- UNITED LINER AGENCIES OF INDIA (PVT.) LTD.,
- PENNON SHIPPING PVT.LTD.
- CENTURY PLYBOARD (I) LIMITED
- APOLLO LOGISOLUTIONS LTD
- AMEYA LOGISTICS PVT LTD
- ARSHIYA INTERNATIONAL LIMITED
- ASHTE LOGISTICS PVT. LTD.
- APM Terminals Pvt. Ltd.(NEW Maersk)
- APM TERMINALS
- CONTAINER CORPORATION OF INDIA LIMI
- A SINGH
- CONTINENTAL WAREHOUSING CORPORATION
- CWC, KALAMBOLI CENTRAL WAREHOUSING CORPORTION
- CWC, DRONAGIRI NODE CENTRAL WAREHOUSING CORPORTION
- CWC IMPEX PARK CFS
- CWC, DISTRIPARK CENTRAL WAREHOUSING CORPORATION CFS
- CWC, IMPEX PARK CENTRAL WAREHOUSING CORPORTION
- FORBES GOKAK LTD
- PUNJAB STATE CONTAINER AND WAREHOUS
- GATEWAY DISTRIPARKS LTD
- CWC LOGISTICS PARK
- JWR LOGISTICS PVT LTD
- KRIBHCO INFRASTRUCTURE LTD
- KSH DISTRIPARKS PVT LTD
- MAERSK INDIA PVT LTD
- MAHARASHTRA STATE WAREHOUSING CORPO
- NAVKAR CORPORATION LTD
- NAVKAR CORPORATION LTD. - 3 NAVKAR CORPORATION LTD. -3
- PUNJAB STATE CONTAINER AND WAREHOUS
- PUNJAB STATE CONTAINER AND WAREHOUS
- SBW LOGISTICS PVT LTD
- SEABIRD MARINE SERVICE PVT LTD.
- SPEEDY MULTIMODES LIMITED
- TRANSINDIA LOGISTICS PARK P. LTD
- UNITED LINER AGENCIES OF INDIA PVT.
- VAISHNO LOGISTICS YARD CFS
- AMEYA LOGISTICS PVT. LTD.
- BALMER LAWRIE & CO LTD
- CWC, DISTRIPARK CENTRAL WAREHOUSING CORPORATION
- CWC, DISTRIPARK CENTRAL WAREHOUSING CORPORTION
- INTERNATIONAL CARGO TERMINAL PRIVAT
- JWC LOGISTICS PARK PVT. LTD.
- NAVKAR CORPORATION LIMITED1
- ASHOK PATIL
- PREETI LOGISTICS LTD
- PUNJAB STATE CONTAINER AND WAREHOU

- MUMBAI INTERNATIONAL CARGO TERMINAL
- APOLLO LOGISOLUTIONS LIMITED
- TAKE CARE LOGISTICS PARK INDIA PRIVATE LIMITED
- ALLCARGO LOGISTICS LTD.
- SARVESHWAR LOGISTICS SERVICES PRIVATE LIMITED
- TG TERMINALS PRIVATE LIMITED
- EFC LOGISTICS INDIA PVT LTD
- KERRY INDEV LOGISTICS PRIVATE LIMITED
- MAHARASHTRA STATE WAREHOUSING CORPORATION
- APM Terminals Pvt. Ltd. (OLD Maersk)
- ALLCARGO LOGISTICS LIMITED
- APM TERMINALS INDIA PVT LTD
- A S SHIPPING AGENCIES P LTD
- BALMER LAWRIE & CO. LTD
- CONTAINER CORPORATION OF INDIA LTD
- CHANDRA CFS AND TERMINAL OPERATORS
- GLOVIS INDIA PVT LTD
- GATEWAY DISTRIPARKS LTD
- GERMAN EXPRESS SHIPPING AGENCY (I)
- KAILASH SHIPPING SERVICES PVT LTD
- KENCES CONTAINER TERMINAL LIMITED
- KERN ENTERPRISES PVT LTD
- SATTVA HITECH AND CONWARE PVT LTD
- SANCO TRANS LIMITED
- SUN GLOBAL LOGISTICS PRIVATE LIMITE
- SICAL MULTIMODAL AND RAIL t
- SICAL SATTVA RAIL TERMINAL PVT LTD
- STP SERVICES PVT LTD
- VIKING WAREHOUSING
- WESTERN GATEWAY CARGO SERVICES PRIV
- ENNORE CARGO CONTAINER TERMINAL PVT
- HIND TERMINALS CHENNAI PVT LTD
- NDR INFRASTRUCTURE PRIVATE LIMITED
- SATTVA CFS AND LOGISTICS PVT LTD
- SUDHARSAN LOGISTICS PVT LTD
- THIRURANI LOGISTIC PRIVATE LIMITED
- TRIWAY CONTAINER FREIGHT STATION P
- SUN GLOBAL LOGISTICS PVT LTD
- ALLCARGO LOGISTICS LTD
- INDIAN CORPORATE BUSINESS CENTRE LTD
- CONTINENTAL WAREHOUSING CORPORATION NS LTD
- CALYX CONTAINER TERMINALS PRIVATE LIMITED
- MARINE LINKS SHIPPING AGENCIES
- MSC AGENCY (INDIA) PRIVATE LIMITED
- ALLCARGO LOGISTICS PVT LTD
- ASHUTOSH CONTAINER SERVICES PVT LTD
- EMPEZAR LOGISTICS PVT LTD
- HIND TERMINALS PVT LTD
- LANDMARK CFS PVT LTD
- MERIDIAN SHIPPING AGENCY PVT. LTD
- MUNDHRA CONTAINER FREIGHT STATION P
- SAURASHTRA FREIGHT PVT LTD

- SEABIRD MARINE SERVICES PVT LTD
- TG TERMINALS PVT LTD
- TRANSWORLD TERMINALS PVT LTD
- HONEYCOMB LOGISTICS PVT. LTD.
- MUNDRA INTERNATIONAL CONTAINER TERM
- Adani EXIM Yard
- ACT SHIPPING LTD
- NITYANAND ACHARYA
- KSPS NATARAJAN CFS PARK
- DIAMOND CFS PARK
- HARI and CO CFS
- S SHIPPING AGENCIES PVT LTD
- A L S Tuticorin Terminal Pvt Ltd
- CONTINENTAL WAREHOUSING CORPORATION Nhava seva Ltd
- VILSONS SHIPPING PVT LTD
- SICAL MULTIMODAL AND RAIL TRANPORT LTD
- PROMPT TERMINALS P LTD
- SEC Services Ltd
- TRANSWORLD TERMINALS PVT LTD
- RAJA AGENCIES
- CHOLA LOGISTIKS PRIVATE LIMITED
- Kerry Indev Logistics Pvt Ltd
- CONTAINER CORPORATION OF INDIA LIMI VPT
- THE COMMISSIONER OF CUSTOMS
- GATEWAY EAST INDIA PVT LTD.
- SICAL LOGISTICS LIMITED
- SRAVAN SHIPPING SERVICES
- VPL INTEGRAL CFS PVT LTD
- VISAKHA CONTAINER TERMINAL PVT LTD
- GATEWAY EAST INDIA PRIVATE LIMITED
- SICAL DISTRIPARKS LTD
- VISAKHA CFS & LOGISTICS PVT LTD
- SRAVAN SHIPPING SERVICES

8.1.4 Inland Container Depots on PCS 1x

- ICD Patli
- ICD Garhi
- ICD Loni
- ICD APM PUNE
- ICD DLI NAGPUR
- ICD WWI WARDHA
- ICD APMT DADRI
- ICD CMA DADRI
- ICD DPW HARYANA
- ICD B2B LUDHIANA
- ICD KI UTTARAKHAND
- ICD PL SAMRALA
- ICD PL KANPUR
- ICD ADANI LUDHIANA
- ICD HP AHMEDABAD
- ICD KRIBHCO GUJRAT
- ICD GRFL LUDHIANA
- ICD HT HARYANA

- ICD ILP KARUR
- ICD SAT PONDICHERRY
- ICD SICAL KAINOOR-3
- ICD GRFL FARIDABAD
- ICD DLI KARNATAKA
- ICD STW HARYANA
- ICD HP JODHPUR
- ICD Kribhco HARYANA
- ICD DPW THIMMAPUR
- ICD TKD
- ICD Dadri
- ICD DDL
- DELHI INTERNATION CARGO TERMINAL
- KribhcoModinagar
- ICD Durgapur
- ICDADMAPL006
- KSH Distriparks PVT LTD
- ICD Vaishno Container Terminal

8.2 Annexure - II

8.2.1 Functional Requirement of Cloud

Compute, Network and Storage

Overall Cloud Requirement:

- CSP should be empanelled under MeitY's "Provisional Empanelment of Cloud Service Offerings of Cloud Service providers (CSPs)"
- 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
- Meet the ever-evolving security requirements as specified by CERT-In (http://www.cert-in.org.in/)
- The Data Center should conform to at least Tier III standard (preferably certified under TIA 942 or Uptime Institute certifications by a 3rd party) and implement tool-based processes based on ITIL standards
- The primary DC and the disaster recovery site should be in different seismic zones within India
- The Data Center should be certified for the latest version of ISO 27001 and provide service assurance and effectiveness of Management compliant with SSAE 16 / ISAE 3402 standards

Cloud Service Requirement:

- The cloud services should provide scalable, redundant, dynamic compute and storage
- Cloud service must offer self-service provisioning of multiple instances concurrently either through an interface (API/CLI) or through a management console.
- Provide the capability to dynamically allocate instances based on load, with no service during demand spikes to maintain performance and decrease capacity during lulls to reduce costs.
- Cloud services shall be provided minimum on a 10GB network connectivity between the server, Storage and Network.
- Cloud service shall be able to support multiple (primary and additional) network interfaces
- Cloud service shall support the ability to create a network interface, attach it to an instance, detach it from an instance, and attach it to another instance.
- Cloud service shall support capabilities such as single root I/O virtualization for higher performance (packets per second), lower latency, and lower jitter
- Cloud service shall support Load balancing of instances across multiple host servers
- Cloud service shall support multiple routing mechanism including round-robin, failover, sticky session etc
- Cloud service shall support a front-end load balancer that takes requests from clients over the Internet and distributes them across the instances that are registered with the load balancer.
- Cloud provider shall offer block storage volumes greater than 1 TB in size.
- Cloud service shall use solid state drive (SSD) backed storage media with minimum latencies.
- Cloud services shall support the needs of I/O-intensive workloads, particularly database workloads that are sensitive to storage performance and consistency in random access I/O throughput.
- Cloud service shall offer SSD backed storage media and shall support High IOPS Storage.
- Cloud provider shall offer a simple scalable file storage service to use with compute instances in the cloud.
- Monitor VM up/down status and resource utilization such as RAM, CPU, Disk, IOPS and network

Cloud operational requirements:

- Manage the network, storage, server and virtualization layers, to include performance of internal technology refresh cycles applicable to meet the SLAs
- Upgrade and periodically replace hardware without financial impact to the purchaser. All the data within it shall be immediately deleted/destroyed and certify the VM and data destruction to the purchaser as per stipulations and shall ensure that the data cannot be forensically recovered.
- SI / CSP should undertake OS level vulnerability management – all OS images created within the cloud platform are regularly patched with the latest security updates

- CSP should manage CSP provisioned infrastructure including VMs as per the ITIL or equivalent industry standards.
- Comply with technology refresh requirements as mandated by CERT-IN and MeitY
- Software within the CSP's scope will never be more than two versions behind unless deferred or rejected by MeitY / Purchaser / Purchaser's authorized agency

Cloud management reporting requirements:

- Provide service level management reports (as per the service levels agreed in the Service Level Agreement between the purchaser and the CSP)
- Monthly and quarterly utilization reports (peak and average volumetric details)
- 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)
    - SLA reports
    - Cloud service usage
    - Helpdesk and tickets
    - User profile management

Database and Allied Services:

- Cloud services provider shall provide services like Database as a service (both RDBMS and No SQL), SMTP and SMS, DNS, Data warehouse, Storage, Analytics, Message queuing etc.
- Cloud provider shall offer a service with ability to take regular and scheduled backup.
- Cloud services shall provide Audit Trail of the account activity to enable security analysis, resource change tracking, and compliance auditing

Cloud Security

Cloud provider shall offer fine-grained access controls including, conditions like time of the day, originating IP address, use of SSL certificates, and multi-factor authentication. The policies for NLP Marine shall comply with international security standards like ISO 27001/27017.

- Cloud services shall support reporting a user's access and last use details.
- Cloud service shall have access control policies that are attached to users, groups. Cloud service shall integrate with LDAP / Active Directory.
- Cloud provider shall support setting up a stand-alone directory in the cloud or connecting cloud resources with LDAP / Microsoft Active Directory.
- Cloud service shall support features such as user and group management.
- Cloud service shall support audit 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.
- Audit plans must be developed and maintained for NLP Marine to address business process disruptions. Audit shall focus on reviewing the effectiveness of the implementation of cyber security. Any/all audit activities must be agreed upon prior to executing.
- Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic Surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems. Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the NLP Marine landscape. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full overwrite of the drive to ensure that the erased drive is released to inventory for reuse and deployment, or securely stored until it can be destroyed.
- User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management.
- Access to data and organizationally owned or managed (physical and virtual) application interfaces and infrastructure network and systems components
- Policies and procedures shall be established to store and manage identity information about every user who accesses IT infrastructure and to determine their level of access
- Policies based controlled access to network resources based on user identity

- The security architecture should be a Multi-layer security model that must be employed starting with networks, perimeter, DMZ, Cloud enabled Data Centre, applications, databases, End user machines and mobile computing devices, which uses above mentioned tools to secure the overall Infrastructure.
- Threat and its mitigation for cloud application which include spoofing, tempering, repudiation, information disclosure, denied of service and elevation of privilege along with OWASP (Open web application security project) testing guidelines should be undertaken to effectively manage the risk and help management take informed decisions.
- The cloud security architecture model should encompass the mentioned security technologies, and work together to effectively improve the process such as incident response resolution, forensic investigation during incident analysis with best practices like real time internal network defence, etc.
- Hypervisor architecture security concern like virtual machine guest hardening, Hypervisor security, inter VM attack blind spot, operation complexity from VM, virtual machine encryption, data communication, VM data destruction, VM image tampering.
- All sensitive data must be secured using encryption with the encryption keys generated, escrowed synchronized and under control of IPA and not by the cloud service provider. Encryption solutions used must have industry standard certifications and accreditations like FIPS, Common Criteria etc.
- Native or default encryption options available at different layers such as storage, database, application etc. are only to be used when it is possible to provide centralized key management for the options. All encryption keys at every part of the infrastructure should be auditable and accessible to IPA through a centralized key manager.

Incident Response

For the proposed NLP Marine, Service Provider shall plan for policies and procedures to ensure timely and thorough incident management, as per established IT service management policies and procedures. Service Provider shall have proper forensic procedures defined and implemented, including chain of custody, required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident

Disaster Recovery and Continuity Planning

NLPNLP Marine shall be designed to run on cloud services offered from multiple Data Centre facilities to provide business continuity with no interruptions in case of any disruptions /disaster to one of the Data Centre facility. In case of failure, automated processes shall move customer data traffic away from the affected area. The Cloud Service Provider shall provide adequate bandwidth between the Data Centre Facilities to provide business continuity.

- Cloud Service Provider shall propose a framework for disaster recovery planning and the plan consistent in addressing priorities for IPA
- Cloud Service Provider shall plan for Disaster recovery drills and testing at planned intervals or upon significant organizational or environmental changes
- Encryption of backup data
- Continuous file integrity health check and automatic repair
- Secure management of critical backup data with enhanced authentication
- Ensure the services offers 24×7 support, this is essential in case an incident occurs outside of normal business hours.
- The SI should provide tools and mechanism to the purchaser or its appointed agency for defining their backup requirements & policy.
- The SI should provide tools and mechanism to the purchaser or its appointed agency for configuring, scheduling, performing and managing back-ups 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

Refer **Annexure II** for further information's

Sizing Considerations for NLP Marine

Service Provider shall submit the details of methodology used by them for sizing of Cloud including capacity of storage, compute, backup, and network & security components.

Service Provider shall be responsible for adequately sizing the necessary compute, memory, and storage required, building the redundancy into the architecture (including storage) and load balancing to meet the service levels as agreed upon by IP.

8.2.2 Technical Requirements of Cloud

There shall be logical separation (of space, servers, storage, network infrastructure and networks) to protect data, applications and servers, in the cloud proposed by Service provider.

Cloud proposal by Service Provider

- DC-DR shall be Tier-3 or higher
- In case of the any disaster at DC site, DRshall act as primary disaster recover site for DC for the entire system.
- DC and DR shall be provided by the same service provider. DR should be more than 100 Km away from DC
- The Disaster Recovery Site should host all the critical production Landscape
- IPA may at any point of time do physical audit of the DC and DR facilities and the service provider shall facilitate such timely physical audits as decided by IPA
- If required Cloud provider shall support multipleISP's leased line connections between cloud provider and Stakeholder locations
- Data shall not leave the boundaries of the country and data residing within Cloud shall not be accessed by any entity outside the control of IPA/authorized representative of Ministry.
- In the event of a Primary site failover or switchover, DR site will take over the active role, and all requests will be routed through that site
- Cloud services shall be accessible via internet or MPLS
- Cloud Service provider shall configure, schedule and manage backups of all the data including but not limited to files, folders, images, system state, databases and NLP Marine applications. There shall be sufficient capacity (compute, network and storage capacity offered) available for near real-time provisioning (as per the SLA requirement of IPA) during any unanticipated spikes in the user load.
- Cloud Service provider shall be responsible for adequately sizing the necessary compute, memory, and storage required, building the redundancy into the architecture (including storage) and load balancing to meet the service levels as specified by IPA
- Cloud Service provider shall perform and store data and file backups consisting of an initial full back with daily incremental backups for files
- Cloud Service provider shall Perform weekly backups for the files
- For the databases, perform minimum twice weekly full database backup, with a three times daily backup of database log files
- Retain the backups for entire project period on system and thereafter on disk which can to be restored when required.
- Cloud Service provider shall not delete any data at the end of the agreement (for a maximum of 90 days beyond the expiry of the Agreement) without the express approval of
- Pre-Production environment for all modules going to be developed and tested for the complete data cycle before releasing in production.
- Providing a staging environment or Pre-Production environment will be having everything as closely replicated to the production environment as possible to maximize the chances of finding any bugs before any release of the software in production. Even the hardware that is used for the staging environment is often the same as the hardware used in the production environment. It would be required to deploy a separate set of VM on separate VLAN for staging environment.

- Provide the Audit artefacts, security policies and procedures demonstrating its compliance with the Security Assessment and Authorization requirements as described in Security Requirements in this RFP.
- IPA will also involve third party auditors to perform the audit/review/monitor the security testing carried out by SI. Cost for such auditors to be paid by IPA.
- SI shall get the Vulnerability Assessment (VA) and Penetration Testing (PT) and Application Security Audit conducted by CERT-In empanelled agency before deployment/ Go-Live of each project phase. SI shall be responsible for all payments to engage such agencies. SI shall be required to make necessary changes in the SRS as well as other documents based on the changes made during testing and UAT.
- Security Audit shall include penetration testing, vulnerability assessment, application security assessment, web security testing and implementation of information security controls.
- The SI is required to configure the solution to allow audit logging of transactions.
- The security Audit logs should capture at least the following information:
    - ✓ Credentials
    - ✓ Transactional logs
    - ✓ IP address and date / time stamp
    - ✓ Session details (time, id, key)
    - ✓ License key

Cloud Service provider shall ensure redundancy at each level and shall provide interoperability support with regards to available API's, data portability etc. for IPA to utilize in case of

- Change of Cloud Service Provider,
- Integration with Utilities backend systems,
- Burst to a different cloud service provider for a short duration, or
- Availing backup or DR services from a different service provider

Cloud Service provider shall provide required support to IPA in migration of the Virtual Machines (VMs), data, content and any other assets to the new environment created by IPA to enable successful deployment and running of NLP Marine on the new infrastructure

- Cloud Hosting Model to provide Virtual Servers, Firewalls, Data Base & Load balancer
- Security Services for the infrastructure SIEM (Security information and event management, DDoS protection, PIM (Privileged identity Management) & MFA (Multi Factor Authentication).
- Multi-layer security infrastructure to prevent unauthorized access to the Data Centre.
- Networking and other associated IT Components in the Data Centre of Cloud Service provider.
- Storage requirements as per server specifications.
- 24 * 7 monitoring and management services.

Refer **Annexure IV** for further information's

8.3 Annexure – III

8.3.1 Message on PCS 1x

Sr.No.	EDI	Document Name
1	VESPRO	Vessel Profile
2	CALINF	Voyage Registration
3	CALINV	Allotment of VCN
4	BERMAN	Berth Management
5	BERALT	Berth Allotment
6	ETAETD	Expected time of Arrival
7	ACKTAD	Expected time of Arrival Acknowledgment

8	PLTMEM	Pilot Memo Application
9	ACKPLM	Pilot Memo Acknowledgment
10	PAISPS	Pre-arrival notification
11	TPFREP	Terminal Performance Report
12	VESDEP	Vessel Movement
13	PAXLST	Passengers/Crew List
14	UNBERT	Re-Berthing
15	ACKMSG	Acknowledgment Message
16	REQVAC	Request for Assessment of Charges-Vessel
17	REQCAC	Request for Assessment of Charges-Cargo
18	REQSAC	Request for Assessment of Charges- Stevedoring
19	CNFASC	Confirmation Advance Assessment of charges
20	PAYSTS	Payment Status
21	PDABAL	PD Account Balance details
22	DLYSUM	Daily Transaction Summary
23	INVOIC	Invoice
24	COPRAR	Container Loading and discharge Order / Adv. Container List
25	COARRI	Container Loading
26	CODECO	Container/Cargo Gate-in Gate-Out Report
27	COEDOR	Container Stock Report
28	GOCOFR	Gate Open Cut off time
29	CARREQ	Request for Carting Permission
30	CARCFN	Confirmation of Carting
31	COSTCO	Container Stuffing / De-stuffing report
32	EICREP	Equipment Interchange Report
33	AGDORD	Agent Delivery Order
34	CONTPE	Pendency of Containers
35	CHPOE05	Shipping Bill Details
36	CHPOE07	LEO
37	CHPOI03	IGM On Submission/Inward Entry
38	CHPOI09	Bill of Entry on submission
39	CHPOI10	Out of charge
40	CHPOI13	Transshipment Permit Approval
41	CHSAE02	Allotment of Rotation number
42	CHSAI15	Cargo Movement Approval
43	POCHE14	Vessel Sailing Report
44	POCHI08	Location of Cargo
45	IFTDGN	Dangerous Goods Notification
46	DGNACK	Dangerous Goods Notification Acknowledgement
47	AGNCHG	Agency Change
48	CLPMSG	Container Load Plan
49	RAILSC	Train Schedule
50	POCHI07	Excess Landed Cargo
51	COSTOR	Container Stuffing

52	COHAOR	Container Special handling order
53	REQCTC	Request for Assessment of Charges- Container
54	STOPLN	Stowage Plan
55	BAPLIE	Bay Plan
56	MOVINS	Stowage Instruction
57	RESREQ	Requisition of Resources
58	ALORES	Allotment of resources
59	MMDINP	MMD Inspection Report
60	MMDVDO	MMD Vessel Detention Order
61	MMDVRO	MMD Vessel Release Order
62	HLTDLR	Health Declaration for sail out
63	INSCER	Inspection Certificate
64	REQFPQ	Request for free Pratique
65	FREPRQ	Request for permission
66	RLOENT	Application for Log Entry
67	GLOENT	Grant of Log Entry
68	COPARN	Empty Container Release Order
69	JOBORD	Job Order
70	COPINO	In land Way bill
71	RAILRE	Rail Receipt
72	RMLMEM	Removal Memo from Rake
73	REQCOC	Request for Assessment of Charges- Containerized Cargo
74	REFORD	Refund Order
75	PAYORD	Pay Order
76	POCHE06	Goods Arrival at Port
77	POCHI06	Landing/ Tally Report
78	CHSAE04	Cancellation of Rotation No.
79	CHSAI02	Grant of Entry Inward
80	CHSAE13	Grant of Port Clearance
81	CHPOE09	Details of Shutout Cargo
82	CHPOE08	Stuffing Report
83	CHPOE11	Grant of Entry Outward
84	GTINAP	Gate-In Appointment Booking
85	DGTSCH	Delivery Gate Schedule
86	TPRORD	Transport Order
87	PRGMSG	Pre-Gate
88	STPCGO	Stowage plan for Cargo
89	POCHE17	Consignment Arrival at Port
90	EIRMSG	Equipment Interchange Report
91	CHSAI01A	IGM Acknowledgement
92	CHPOI05	Cancellation of IGM No.
93	CHPOI33	Disposal Order
94	CHCMI02	Console Manifest
95	CHSAE01A	Application for Rotation No. Acknowledgement
96	CHPOE06A	Entry of Goods Acknowledgement

97	CHSAE15A	EGM Acknowledgement
98	AGDORD	Delivery Order

Apart of above, API integration between PCS 1x andICEGate is also being done/in progress in respect of following 11 payloads:

	Total Messages		Messages Mapped to	
S.No	Message ID	Message Description	Messages ID (Payload)	Message Description
1	PCCHCO1	Communication of conveyance call number (VCN)	PCCHCO1	Communication of Conveyance call number (VCN)
2	CHSAE02	Allotment of rotation number		
3	CHSAI01A	IGM acknowledgement		
4	CHSAE01A	application for rotation number acknowledgement		
5	CHSAE15A/CHSAE18A	EGM Acknowledgement		
6	CHSAE04	Cancellation of Rotation Number		
7	CHPOI05	Cancellation of IGM number		
8	CHSAI02	Grant of Entry Inward	CHTOI04N	Customs Control Message
9	CHSAE13	Grant of Port clearance		
10	CHPOE11	Grant of Entry Outwards		
11	CHPOI09	Bill of entry submission	CHPOI09	Bill of Entry Submission
12	CHPOI10	Out of charge Details		
13	CHPOI13	Transhipment Permit	CHPOEO8	Communication of goods intended for arrival
14	CHSA15	Cargo Movement approval		
15	CHPOE08	stuffing report		
16	CHPOEO5	Shipping bill details	CHPOE05	Shipping bill details
17	CHPOE07	let export order		
18	TOCHI02	Intimation of Actual time of Arrival/Departure of Conveyance	TOCHI02	Intimation of Actual time of Arrival/Departure of Conveyance
19	TOCHI03	Intimation of transport equipment's landed/loaded in the conveyance	TOCHI03	Intimation of transport equipment's landed/loaded in the conveyance
20	CMCHI21	CONSOL Manifest	CMCHI21	CONSOL Manifest
21	VESPRO	Vessel Profile	VESPRO	Vessel Profile
22	CHPOI03	IGM on INW/Vessel details,Cargo,container	CHPOI03	IGM on INW/Vessel details,Cargo,container
23	POCHE06	Goods arrival at port	POCHE06	Goods arrival at port

Out of 11 payload, 3 payload have been made LIVE. Once the above11 payload made LIVE, the XML exchange through SFTP with ICEgate will be discontinued .

8.4 Annexure – IV

8.4.1 Software Component Stack for NLPMarine

Sr. No.	Technical Components	Description (Highlighted components of Existing PCS1x are to be used in building NLP Marine)
1	Form Management System	A Forms Framework that governs how forms for a system should be developed.
2	Application Framework	To standardize coding practices MS.Net
3	Database	To store all OLTP data
4	Reporting	To provide Management with reporting information RDLC, MS SQL SSRS, PDF / Excel Export
5	Analytics / BI	To provide Management with strategic information - Application Embedded Charts framework
6	Customer Relationship Management	To Maintain Master data of Stakeholders
7	DMS	Document Management System
8	Messaging System *	To provide message store and forward capabilities IBM IIB framework / Open standards framework
9	Format Translator *	To translate message/content formats from one form to another IBM IIB framework / Open standards framework
10	Message Routing*	To route messages/contents from one endpoint (and technology) to another endpoint (and technology) IBM IIB framework / Open standards framework
11	Authorization & Authentication Component	To authorized and authenticate the user who would be registered on to the portal.
12	Communications *	Email utility to send email or SMS one to one or mass email
13	Events *	To communicate between one end to another end using IBM queue IBM IIB framework / Open standards framework
14	SFTP Server	File transfer Server
15	SFTP Client	File Transfer Client “PMX”
16	Archival	File Storage
17	Data Encryptions	For B2B interaction of financial documents i.e. invoices

8.4.2 Technical Requirements Security

Cloud DC and Server Security

- Designing all the key supply components to be redundant
- Monitor access: access control system, video monitoring systems, movement sensors, security personnel, alarm systems, etc.
- Two-factor authentication for access to the data centre
- Fire protection: fire alarm system, fire early detection system, suitable fire extinguishers, regular fire drills
- Robust infrastructure that provides adequate resistance to damage by the elements and unauthorised entry
- Redundant data centres that are, at least, far enough away from one another that a controllable damage event does not simultaneously affect the data centre originally containing the backup capacities
- Technical measures to protect the host (host firewalls, regular integrity checks, host-based intrusion detection systems)
- A secure basic configuration for the host (e.g. deploying hardened operating systems, disabling unnecessary services, etc.)
- Secure default configuration for the guest operating system using hardened operating systems, disabling unnecessary services, etc. (with PaaS/SaaS only)
- Remote administration via a secure communication channel (e. g. SSH, TLS/SSL, IPsec, VPN)
- Encrypted communication between Cloud Computing provider and Cloud Computing user (e. g. TLS/SSL)
- Encrypted communication with third party providers where these is required for the provider's own offering

Network Security

- Security measures against malware (anti-virus, Trojan detection, anti-spam, etc.)
- Security measures against network-based attacks (IPS/IDS systems, firewall, Application Layer Gateway, etc.)
- DDoS mitigation (protection against DDoS attacks)
- Suitable network segmentation (isolate the management network from the data network)
- Secure configuration of all components in the cloud architecture

8.4.3 Reliability (up time), redundancy, persistency, fall back scenarios

- Built in high availability - SLA from 99.5% to 99.999%.
- We recommend Cloud SLA to be up and above 99.5% to be taken into consideration while selecting CSP.
- The system must have appropriate measures to ensure processing reliability for the data received or accessed through the solution. NLP-Marine is a critical operation and requires reliability to ensure stakeholder confidence.

Reliability SLA:

DataReliability Guarantee	Description	SLA
> 99.99%	Loss of Data due to unavailability / failure of infrastructure	

DR Objectives

- RPO – Recovery Point Objective. Target lag for data at DR site compared to primary site.
- RTO – Recovery Time Objective. Time required to start IT infrastructure at DR site during actual disaster scenario.

Service-Level Objective (SLO)		
1	RPO	30 Mins
2	RTO	4 Hrs.

DR Objective dependencies

- RPO and RTO will be analysed during first DR Drill and if any fine tuning is required, respective owner will take appropriate action as per the inputs shared by Service Provider. No SLOs are applicable till completion of first DR Drill.
- RPO achievement is dependent on provisioning and availability of required Bandwidth by IPA for data replication.
- RTO will be applicable for making the IT Infrastructure, Operating Systems and Database services available. RTO starts post IPA has declared DR invocation and informed all stake holders & will exclude third party application, IPA network team dependencies and other third-party services which are not under Service Provider scope.
- IPA and Service Provider will need to verify the application consistency before releasing it to users.
- Application wise partial recovery DR Drill is not to be performed. During DR Drill or actual disaster recovery complete application Landscape excluding dependent applications to be made available from DR site.

DR Drill Schedule

DR Site Readiness, DR Deliverables (DR Documentation & DR Drill) High Level Roles & Responsibility Table		
Activity Name	**SERVICE Provider**	**IPA**
Replication Link, Bandwidth for Replication	Yes	No
Bandwidth Estimation	No	Yes
End user locations Connectivity to DR Site -Failover/Failback	No	Yes
DR Documentation for services in Service Provider Scope	Yes	Support
DR Drill for services in Service Provider Scope	Yes	Support
Communication enablement for DRM server access. SOP's for technologies scope	Yes	Support

Service Provider will perform two DR drills in the 1st year in form of Admin and User Drill and 1 DR drill annually in subsequent years.

Deliverables

- Service Provider will deliver the following on 7th Business Day of the month:
- Monthly Incident/Change Report
- Monthly Availability report
- Monthly Performance report
- Monthly RTO/RPO report
- Monthly Replication Link utilization report

8.5 Annexure - V

List of documents exchanged in Maritime Logistics

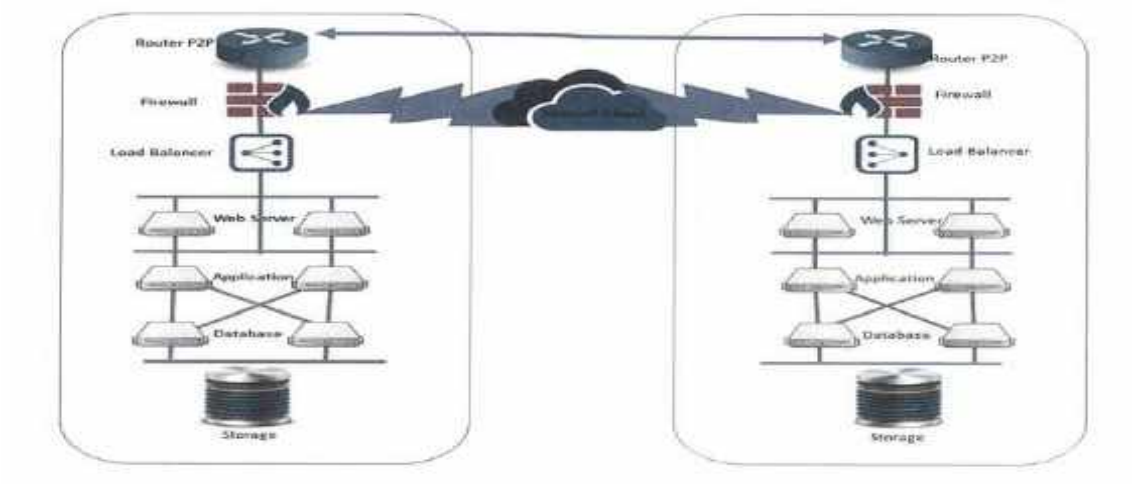
Sr. No.	Document	From	To
1	IEC Number	DGFT	Exporter
2	RCMC Certificate	EPC	Exporter
3	Purchase Order	Importer	Exporter

4	LC Application	Importer	Importer's Bank
5	LC Application	Importer's Bank	Exporter's Bank
6	LC Notification	Exporter's Bank	Exporter
7	Invoice	Exporter	Importer
8	Packing List	Exporter	Importer
9	Letter of Instruction	Exporter	FF cum CB
10	Booking Note	Shipping Line	FF cum CB
11	Shipping Bill	FF cum CB	Customs
12	Shipping Bill Number	Customs	FF cum CB
13	Booking Note Copy	Truck	Empty Container Depot
14	Equipment Interchange Report	Empty Container Depot	Truck
15	Gate Pass	Exporter's Factory	Truck
16	LEO	Customs	ICEGATE
17	Forwarding Note	ICD	Rail Operator
18	List of loaded cargo	ICD	Rail Operator
19	Rail Receipt	Rail Operator	FF cum CB
20	Rail Receipt	FF cum CB	Shipping Line

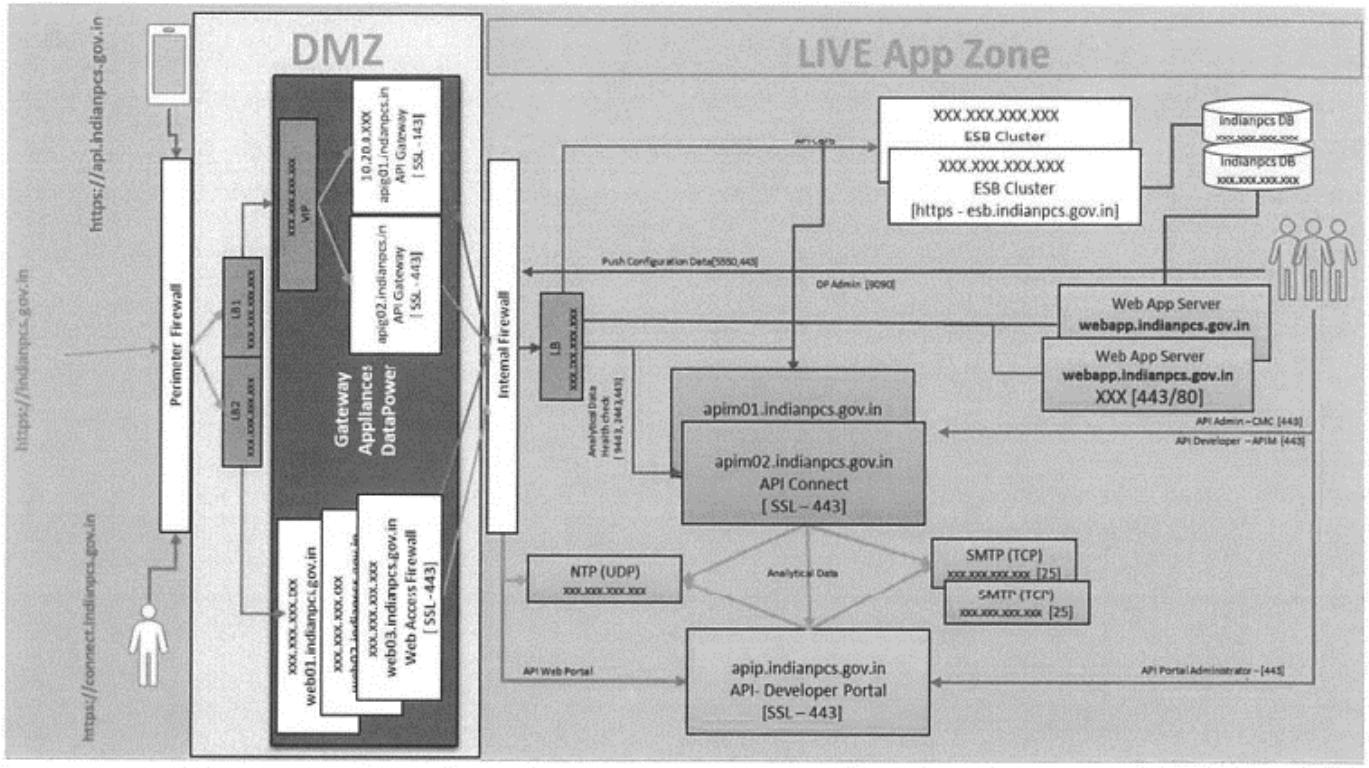
8.6 Annexure VI

8.6.1 Existing Systems Details:

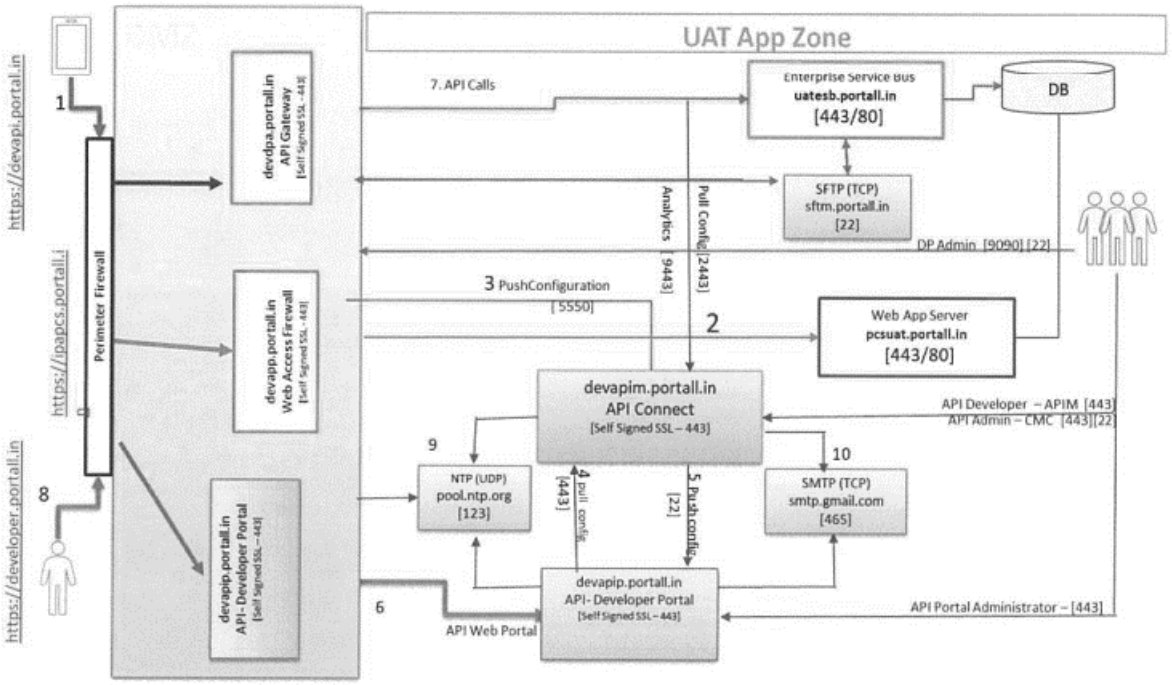
8.6.1.1 IPA PCS Proposed Solution Architecture



8.6.1.2 Deployed Solution Architecture:



8.6.1.3 Deployed UAT Infrastructure Solution:



DC Infrastructure:

Sr. No	Server / Device name	Server Role	Host Name	Operating System	HDD	Processor	Processor Speed	Memory in GB
1	IPAWEB1	Web	IPAWEB1	Windows 2016 STD	200	4	2.20 Ghz	16
2	IPAWEB2	Web	IPAWEB2	Windows 2016 STD	200	4	2.20 Ghz	16
3	IPA-APPSRV1	Application	IPAAPPSRV1	Windows 2016 STD	200	8	2.20 Ghz	64
4	IPA-APPSRV2	Application	IPAAPPSRV2	Windows 2016 STD	200	8	2.20 Ghz	64
5	IPA-DBSRV1	Database	IPADBSRV1	Windows 2016 STD	1024	8	2.20 Ghz	64
6	IPA-DBSRV2	Database	IPADBSRV2	Windows 2016 STD		8	2.20 Ghz	64
7	IPAFTP1	SFTP	IPASFTP1	Oracle Linux 7.4	200	2	2.20 Ghz	16
8	IPAFTP2	SFTP	IPASFTP2	Oracle Linux 7.4	200	2	2.20 Ghz	16
9	IPA-NFS-SRV1	NFS	IPANFSSRV1	Oracle Linux 7.4	2048	2	2.20 Ghz	16
10	IPA-NFS-SRV2	NFS	IPANFSSRV2	Oracle Linux 7.4		2	2.20 Ghz	16
11	SMTP - 1	SMTP	IPASMTP1	Oracle Linux 7.4	200	4	2.20 Ghz	8
12	SMTP - 2	SMTP	IPASMTP2	Oracle Linux 7.4	200	4	2.20 Ghz	8
13	IBM DataPower Gateway Virtual 1	Datapower Gateway	IPADPGW1	OVA	300	4	2.20 Ghz	32
14	IBM DataPower Gateway Virtual 2	Datapower Gateway	IPADPGW2	OVA	300	4	2.20 Ghz	32
15	IBM API Manager & Anylitics 1	API Manager	IPAAPIM1	OVA	350	4	2.20 Ghz	32
16	IBM API Manager & Anylitics 2	API Manager	IPAAPIM2	OVA	350	4	2.20 Ghz	32
17	API Portal	API Portal	IPAAPIP	OVA	300	4	2.20 Ghz	32
18	IBM IIB ESB 1	Enterprise Service Bus	IPAESB1	Redhat Linux 7.4	500	4	2.20 Ghz	32
19	IBM IIB ESB 2	Enterprise Service Bus	IPAESB2	Redhat Linux 7.4	500	4	2.20 Ghz	32
20	IBM Monitoring ESB	ESB - Monitoring	IPAESBMON	Redhat Linux 7.4	300	3	2.20 Ghz	16
21	SIEM Collector	SIMs Collector	IPASIME	Centos 7.4	500	6	2.20 Ghz	8
22	PIM Server	PIM Server	IPAPIM1	Windows 2016 STD	160	4	2.20 Ghz	8
23	PIM Server	PIM Server	IPAPIM2	Windows 2016 STD	160	8	2.20 Ghz	8
24	Portall App Server	Devops	IPADEVOPS1	Windows 2016 STD	200	4	2.20 Ghz	16
25	Portall App Server	Devops	IPADEVOPS2	Windows 2016 STD	200	4	2.20 Ghz	16
26	IPAWEB1	Web		Windows	200	4	2.20 Ghz	8
27	IPA-APPSRV1	Application		Windows	200	4	2.20 Ghz	16
28	IPA-DBSRV1	Database		Windows	500	4	2.20 Ghz	16
29	IPAFTP1	FTP		Oracle Linux	200	2	2.20 Ghz	8
30	IPA-NFSSRV1	NFS		Oracle Linux	200	2	2.20 Ghz	8
31	Datapwr-gw1	Datapower Gateway and WAF		OVA	500	4	2.20 Ghz	32
32	API-Connect-1	API Manager		OVA	300	4	2.20 Ghz	32
33	API-Connect-2	API Developer Portal		OVA	300	2	2.20 Ghz	16
34	APP-Connect	Enterprise Service Bus		Redhat Linux	500	4	2.20 Ghz	32
35	IPA SMTP UAT	SMTP Gateway		Oracle Linux	200	4	2.20 Ghz	8

Sr. No	Category	On-Demand Hosting Code	Description	Qty	Remarks
	PAAS				
1	OS License	PAAS-OS-ENTLNX-VPI-PEROS	Operating system license - OEL Enterprise Linux OS per VPI	8	Oracle Enterprise Linux
2	OS License	PAAS-OS-RHEL-VPI-04vCPU-ABOVE-PEROS	Operating system license - RHEL Linux OS for VPI with 04vCPU & above configuration per guest OS	4	Redhat Linux License
3	OS License	PAAS-OS-MS-WINSTD-VPI-AV-PER-2vCPU	Operating system license - Microsoft Windows Server Standard 2016 /2012 /2008 per 2vCPU VPI, with antivirus	36	Windows OS License for VPI
4	OS License	PAAS-OS-CENTOS-VPI-MDS-VPE-PVT-PEROS	Operating system license- Cent OS per VPI, MDS,VPE or PVT Cloud per host	1	Centos for SIME
5	DB License	PAAS-DB-MS-SQL-ENT-VPI-PER 2vCPU	Database Licenses - Microsoft SQL Enterprise edition 2016 /2014/ 2012 /2008 for VPI per 2vCPU	10	MS SQL Ent Edition
	InfinitNetwork&Security				
1	Firewall	INET-VPDC-FLEX-100Mbps	Virtual Private Datacenter, 1 dedicated vFirewall, 3 LAN, 2 Site Direct Tunnels, 10 SSL VPN user, support for 100 Mbps N-S traffic & 1G E-W	1	Firewall MZ & DMZ
2	FW Virtual + NFV deployment	PAAS-OTHER-SOFTWARE	PAAS-other software-Per BOM specification	1	Firewall Internal
3	Load Balancer	INET-HW-SLB-500Mbps-5VIP-20RIP	Hardware Load balancer context in HA with 500 Mbps throughput, support for 5 VIP,20 RIP, SSL offloading capabilities 20000 concurrent connections per RIP.	2	Load Balancer
4	DDoS Protection	ISEC-DDOS-NM-11-50Mbps	DDOS service Notification & Mitigation, 11-50Mbps Slab-per annum	100	DDoS
5	PIM	PIM	PIM per User	5	PIM for 5 user
6	Virtual Router	INET-CLOUDPORT-100MBPS-PERPOR	Cloud connectpPort with 100 Mbps throughput and 99.95% SLA	1	Virtual router for P2P connectivity
7	Cross Connect	Cross connect	Cross Connect	1	Cross connect
8	Additional IP	INET-EXTIP-1IP	Extra public IP (Per IP)	16	Extra 16 IP's
9	SIEM	ISEC-SIEM-PER-10-LOGSOURCES	SIEM services with security incident response for 10 log source per setup retention up to 30 Days	1	SIEM 10 Log source
10	Addon SIEM	ISEC-SIEM-ADDON-PER-LOGSOURCE-MAX-50LOGSOURCE	SIEM services with security incident response for add-on log source per setup max log sources supported 50 log sources, retention up to 30 Days	31	Addon SIEM

11	MFA	ISEC-MFA-10USER-PACK-PERVPDCFLEX	Multifactor authentication for 10 users per VPDC Flex	1	Multi Factor Authentication 10 User Pack
12	DNS Service	INET-EXDNS-1DOMAIN-UTD RECORDS	Domain Name Service (DNS) Per Domain (URL) with unlimited records on Sify High available (Primary and Secondary) DNS setup	5	DNS As a Service
13	Bandwidth	INET-IBW-1:1 PERMBPS	INET-IBW-1:1-PERMBPS	30	Internet Bandwidth 30 Mbps
	CloudInfinit Managed Services				
1	OS Management	CI-MITS-OS-LNX-PROFICIENT 1 OS	OS Support - Linux, 24x7-PROFICIENT-Management & Monitoring-Per OS	8	OS Management Linux
2	OS Management	CI-MITS-OS-WIN-PROFICIENT-1-OS	OS Support - Windows, 24x7-PROFICIENT-Management & Monitoring-Per OS	13	OS Management Windows
3	OS Management	CI-MITS-OS-LNX-PROFICIENT-1-OS	OS Support - Linux, 24x7-PROFICIENT-Management & Monitoring-Per OS	1	Cent Os manegement SIME Server
4	OS Management	CI-MITS-OS-LNX-PROFICIENT-1-OS	OS Support - Linux, 24x7-PROFICIENT-Management & Monitoring-Per OS	4	OS Management RedHat Server
5	DB Management	CI-MITS-DB-MSSQL-PROFICIENT-1-DB	Database Support - MSSQL, 24x7-PROFICIENT-Management & Monitoring-Per DB	3	MS SQL Management
6	Other Application & Web Management	CI-MITS-EMAIL-POSTFIX-PROFICIENT-1-ESRV	Messaging Support - POSTFIX, 24x7-PROFICIENT-Management & Monitoring-Per Email Server	2	FTP, NFS, Web Application & IIS Management
7		CI-MITS-AM-WEBSERVER-PROFICIENT-1-APP	Application Support - WEBSERVER, 24x7-PROFICIENT-Management & Monitoring-Per Application	9	
8	FW Mgt	CI-MITS-SEC-LE-FIREWALL-PROFICIENT-1-FIREWALL	Security Support - LOW END Firewall-24x7- PROFICIENT-Management & Monitoring-Per Firewall	1	Firewall
9	Backup	GI-BKP-FE-PERGB	GoInfinit-Backup-Data protection-file, folder, VM, Apps-Front End capacity, per GB	6,000	Backup License
10		GI-BACKUPSTOR-PERGB	GoInfinit-BackupStore, per GB	6,000	Backup Storage within the DC
11		GI-2ndCOPYSTOR-PERGB	GoInfinit 2ndCopy store per GB in a different seismic zone inclusive of replication cost	6,000	2nd Copy at a different Sesmic Zone

DR Infrastructure:

S.No	Server / Device name	Server Role	Operating System	LUN Allocated in GB	Processor in vCPU	Memory in GB	ROLE
1	IPAWEB1	Web	Windows	200	4	16	PRODUCTION DR
2	IPA-APPSRV1	Application	Windows	200	8	64	PRODUCTION DR
3	IPA-DBSRV1	Database	Windows	1024	8	64	PRODUCTION DR
4	IPAFTP1	FTP	Linux	200	2	16	PRODUCTION DR
5	IPA-NFS-SRV1	NFS	Linux	2048	2	16	PRODUCTION DR
6	SMTP - 1	SMTP	Linux	200	4	8	PRODUCTION DR
7	IBM DataPower Gateway	IBM ESB	OVA	250	4	32	PRODUCTION DR
8	IBM API Connect Enterprise	IBM ESB	OVA	300	4	32	PRODUCTION DR
9	IBM API Connect Enterprise	IBM ESB	OVA	300	4	32	PRODUCTION DR
10	IBM APP CONNECT ENTERPRISE	IBM ESB	Redhat	500	4	32	PRODUCTION DR
11	Portall - App Server	Gateway	Windows	200	4	16	PRODUCTION DR

Sr. No	Category	On-Demand Hosting Code	Description	Qty	Remarks
	PAAS				
15a	OS License	PAAS-OS-ENTLNX-VPI-PEROS	Operating system license - OEL Enterprise Linux OS per VPI	3	Oracle Enterprise Linux
15a	OS License	PAAS-OS-RHEL-VPI-04vCPU-ABOVE-PEROS	Operating system license - RHEL Linux OS for VPI with 04vCPU & above configuration per guest OS	1	Redhat Linux License
18a	OS License	PAAS-OS-MS-WINSTD-VPI-AV-PER-2vCPU	Operating system license - Microsoft Windows Server Standard 2016 /2012 /2008 per 2vCPU VPI, with antivirus	12	Windows OS License
19a	DB License	PAAS-DB-MS-SQL-ENT-VPI-PER 2vCPU	Database Licenses - Microsoft SQL Enterprise edition 2016 /2014/ 2012 /2008 for VPI per 2vCPU	0	MS SQL Ent Edition not required as this is passive instance
	Infinit Network & Security				
20a	Firewall	INET-VPDC-FLEX-100Mbps	Virtual Private Datacenter, 1 dedicated vFirewall, 3 LAN, 2 Site Direct Tunnels, 10 SSL VPN user, support for 100 Mbps N-S traffic & 1G E-W	2	External facing single Firewall
21a	Virtual Router	INET-CLOUDPORT-100MBPS-PERPOR	Cloud connectpPort with 100 Mbps throughput and 99.95% SLA	1	Virtual router for P2P connectivity
22a	DDoS Protection	ISEC-DDOS-NM-11-50Mbps	DDOS service Notification & Mitigation, 11-50Mbps Slab-per annum	100	DDoS
22a	Load Balancer	INET-HW-SLB-500Mbps-5VIP-20RIP	Hardware Load balancer context in HA with 500 Mbps throughput, support for 5 VIP,20 RIP, SSL offloading capabilities, 20000 concurrent connections per RIP.	1	Load Balancer
23a	P2P Connectivity	P2P Connectivity	P2P 20 Mbps - From Mumbai Sify DC to Bangalore Sify DC	1	Extra 16 IP's
24a	Cross Connect	Cross connect	Cross Connect	1	Cross connect
25a	Additional IP	INET-EXTIP-1IP	Extra public IP (Per IP)	16	Extra 16 IP's
26a	SIEM	ISEC-SIEM-PER-10-LOGSOURCES	SIEM services with security incident response for 10 log source per setup retention up to 30 Days	1	SIEM 10 Log source

	Addon SIEM	ISEC-SIEM-ADDON-PER-LOGSOURCE-MAX-50LOGSOURCE	SIEM services with security - incident response for add-on log source per setup. max log sources supported 50 log sources, retention up to 30 Days	7	Addon SIEM
28a	DNS Service	INET-EXDNS-1DOMAIN- UTD RECORDS	Domain Name Service (DNS) Per Domain (URL) with unlimited records on Sify High available (Primary and Secondary) DNS setup	5	DNS As a Service
29a	Bandwidth	INET-IDT-PER-GB	Internet data transfer per GB per month - Internet data transfer overage per GB per month @ 7 Per GB Per Month	500	Internet Data Transfer for 500GB Per Month
	Replication				
30a	Replication tool	IPTC-DRAAS-SRM-V2V-PER INSTANCE-PERANNUM	DRaaS License per protected Virtual instance-X-86, Online Dashboard, Per Year	11	Host Based replication tool
31a	**Replication & Monitoring Server**	ICOM-VPI-1vCPU-1GBRAM-50GB BSAN-SHM-99.5%	Virtual private instance, 01vCPU (2 GHz & above),1GB RAM, 50GB boot SAN, 99.5% SLA, server health monitoring & management	2	(4 vCPU, 16 GB RAM)x2 - No OS Required & No Management Requried
32a		ICOM-VPI-ADD-1vCPU-99.5%	Virtual private instance, add on 01vCPU (2 GHz & above), 99.5% SLA. Max vCPU per VPI =32 vCPU	6	
33a		ICOM-VPI-ADD-1GBvRAM-99.5%	Virtual private instance, additional 01 GB vRAM. Max RAM per 01vCPU = 8GB & multiples thereof	30	
34a	**Replication Management**	Replication Management	Replication management Per Server	11	Replication Management
35a	Replication Link	IPSEC tunnel replication link between Customer DC and Sify DR	IPSec Tunnel Configuration	1	Client to validate
	CloudInfinit Managed Services				
36a	OS Management	CI-MITS-OS-LNX-PROFICIENT-1-OS	OS Support - Linux, 24x7-PROFICIENT-Management & Monitoring-Per OS	3	OS Management Linux
37a	DB Management	CI-MITS-DB-MSSQL-PROFICIENT-1-DB	Database Support - MSSQL, 24x7-PROFICIENT-Management & Monitoring-Per DB	1	MS SQL Management
38a	OS Management	CI-MITS-OS-WIN-PROFICIENT-1-OS	OS Support - Windows, 24x7-PROFICIENT-Management & Monitoring-Per OS	4	OS Management Windows
39a	Application Management	CI-MITS-EMAIL-POSTFIX-PROFICIENT-1-ESRV	Messaging Support - POSTFIX, 24x7-PROFICIENT-Management & Monitoring-Per Email Server	1	FTP, NFS, Web Application & IIS Management
		CI-MITS-AM-WEBSERVER-PROFICIENT-1-APP	Application Support - WEBSERVER, 24x7- PROFICIENT-Management & Monitoring-Per Application	3	
40a	DR Management	DR Mngt	DR Mngt -DR Drill 02 & BCP mngt	2	DR Drill and Management

Infrastructure and Application Security:

1. **Infrastructure:**
    a. Security of Facilities, Physical security of hardware, Network infrastructure and Virtualization infrastructure.
    b. Security of the Virtual Machine Images, Operating systems.
    c. Applications, Data in transit, Data at rest, Data stores, Credentials and Policies and configuration. Encryption of data at rest, and HTTPS encapsulation for the payloads for protecting the data in transit to and from the service.
    d. Operating system will be hardened.

2. **Platform services:**
    a. Firewall in HA will protect our application access.
        - Built-in Firewalls – to control accessibility the instances are by configuring firewall rules
    b. Data backup and recovery tools will be configured.
    c. Business continuity and disaster recovery (BC/DR) policy will be implemented.

3. **Security tools Implemented in IPAPCS1.x Application**:

    a. **Identity and Access Management (IAM)** - allows controlling the level of access to the users to the CSPs infrastructure services. With IAM, each user can have unique security credentials, eliminating the need for shared passwords or keys and allowing the security best practices of role separation and least privilege.

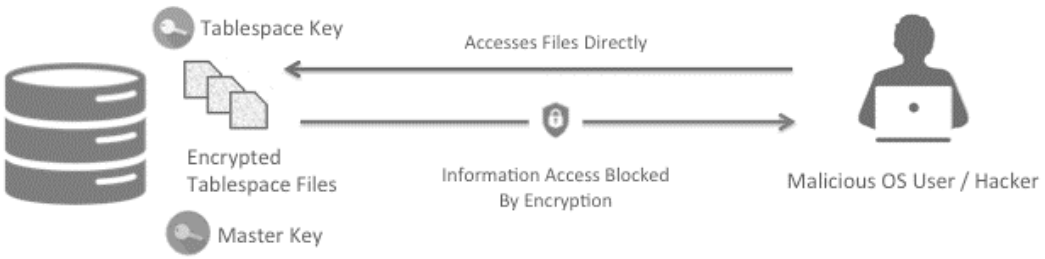
    b. **Two Factor Authentication –** Our application will have 2FA, Two Factor Authentication, also known as 2FA, two step verifications, is an extra layer of security that is known as "multi factor authentication" that requires not only a password and username but also something that only, and only, that user has on them, i.e. a piece of information only they should know or have immediately to hand - such as a physical token.

    c. **Secure Access –** IPAPCS 1.X application will use Hypertext Transfer Protocol Secure (HTTPS), or "HTTP Secure," which is an application-specific implementation and is a combination of the Hypertext Transfer Protocol (HTTP) with the SSL/TLS. HTTPS is used to provide encrypted communication with and secure identification of a Web server.

    d. **SIEM**- security information and event management (SIEM) software and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by applications and network hardware.
    e. **PIM** - Privileged identity management (PIM) will be used for monitoring and protection of superuser accounts in IT environments.
    f. **DDoS Prevention -** In a distributed denial-of-service attack (DDoS attack), the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source. A DoS or DDoS attack is analogous to a group of people crowding the entry door of a shop, making it hard for legitimate customers to enter, disrupting trade. Our Infra will have protection against the same attack.
    g. **Anti-virus programs** – All IPAPCS1.x Applications servers will be protected with Antivirus.
    h. **Encryption** – Encryption protects our critical data by enabling data-at-rest encryption in the database. It protects the privacy of your information, prevents data breaches and helps meet regulatory requirements including the Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA) and numerous others. The User profile and access management data will be in separate encrypted Database to avoid hacking.

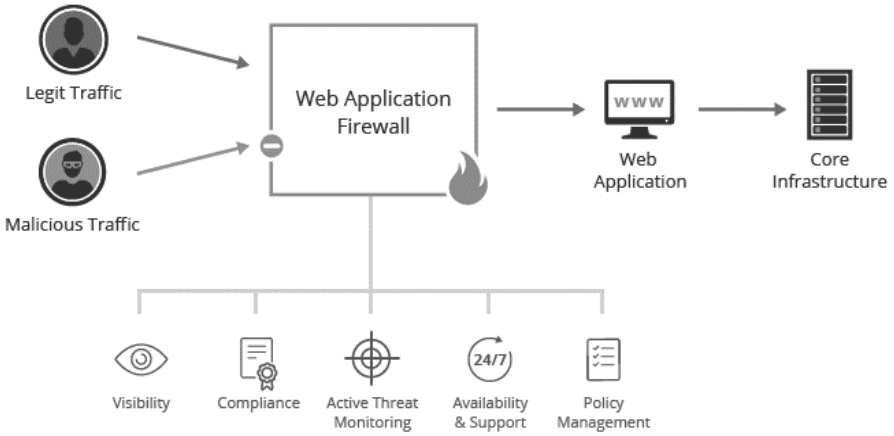
    IPAPCS 1.x will have data-at-rest encryption by encrypting the physical files of the database. Data is encrypted automatically, in real time, prior to writing to storage and decrypted when read from storage. As a result, hackers and malicious users are unable to read sensitive data from tablespace files, database backups or disks. We will use industry standard AES algorithms.

Pic:1 Encryption



i. **WAF -** A web application firewall (WAF) is an application firewall for IPAPCS1.x applications. It applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection.

Pic:1 Encryption



j. **Load balancer –** IPAPCS1.x will have load balancer whichprovide the bedrock for building flexible networks that meet evolving demands by improving performance and security for many types of traffic and services, including applications.

k. **VAPT -**Additional we will implement third-party security products for network security, server and vulnerability management as per the security requirements of the IPAPCS. Vulnerability Assessment and Penetration Testing (VAPT) are two types of vulnerability testing. The tests have different strengths and are often combined to achieve a more complete vulnerability analysis. In short, Penetration Testing and Vulnerability Assessments perform two different tasks, usually with different results, within the same area of focus. Vulnerability assessment tools discover which vulnerabilities are present in the application code and where they are located.

l. IPS /IDS - Intrusion detection is the process of monitoring the events occurring in your network and analyzing them for signs of possible incidents, violations, or imminent threats to our security policies. Intrusion prevention is the process of performing intrusion detection and then stopping the detected incidents. These security measures are available as intrusion detection systems (IDS) and intrusion prevention systems (IPS), which is part of our network to detect and stop potential incidents.

Data Backup Policy

M/s Portall Infosystems Pvt Ltd. will perform backup and restore management in accordance with mutually agreed to backup and restore policies and procedures, including performance of daily, weekly, monthly quarterly and annual backup functions (full volume and incremental) for data and software maintained on Servers and storage systems including interfacing with customer's specified backup media storage facilities;

1. Backup and restore of data in accordance to defined process / procedure.

2. 24 x 7 support for file & volume restoration requests

4. Performance analysis of infrastructure and rework of backup schedule for optimum utilization.

5. Generation and publishing of backup reports periodically.

6. Maintaining inventory of onsite tapes.

7. Forecasting tape requirements for backup.

8. Ensuring failed backups are restarted and completed successfully within the backup cycle.

10. Real-time monitoring, log maintenance and reporting of backup status on a regular basis.

11. Management of storage environment to maintain performance at optimum levels.

12. Periodic Restoration Testing of the Backup once a quarter.

13. Periodic Browsing of the Backup Media.

14. Interacting with Process Owners in maintaining Backup & Restoration Policies / Procedures.

15. To provide MIS reports as per agreement

Application Back Up:

- Files, applications including databases to be backed up (SECRET, CRITICAL and CONFIDENTIAL)
- Apart from the above-mentioned point, information assets in hard format such as, but not restricted to vendor agreements, paper licenses and any other documents not necessarily in CRITICAL or SECRET or CONFIDENTIAL category, but which are required from an availability perspective; shall be digitized with smart search for ease of reference and retrieval of information, and stored on either a portal with restricted access or a server with folder level protection.
- IT (backup) Administrator assigned and authentication details.
- Inventory of backup media including the location of their storage and contents.
- Record of blank (unused), discarded and destroyed media in a manner that complete history of media usage is available.
- The request shall be sent to the HOD who shall assign the backup activity to the IT Team member.
- Any changes done to system, which affects regular backup, shall be intimated to IT team backup initiator.
- A suitable platform shall be deployed for backing up application configuration, OS, databases which also offers DR in the box capability.

Server Backups:

- A tool-based approach shall be deployed while backing up data from servers. This shall be scheduled based on the work schedule.
- Backup Scheduling shall be related to business risk, frequency with which data and software is changed and the criticality of the system to business operations.
- Based on criticality a full image back up shall also be taken using tools which provide DR in a Box features.
- Systems software, application software, data, different logs and documentation shall be backed up on a regular basis, in accordance with back-up schedule as defined below.
- As a minimum standard for SECRET or CRITICAL or CONFIDENTIAL Servers:
    - Full daily back-up of data will be done as per business requirement.
    - Full weekly back-ups of all application data including its configuration are taken.
    - Full monthly back-ups of all data, including operating system configuration files.
    - Consolidated backup shall be taken monthly for archival. Such archives shall be stored for a year or as per business need.
    - Yearly backup of all consolidated monthly tapes/media shall be taken and archived.
    - Time frame for the archival will be as per the regulatory and business requirements.
- As a minimum standard for rest of the servers:
    - Full monthly back-ups of all data, including operating system configuration files and applications.
    - Quarterly full backup, six monthly full backup and yearly full backup shall be done.
- Configuration back-up of Routers, Switch, and Firewalls to be taken on monthly basis, the configuration details history to be maintained and stored on a storage system with restricted access.

Ad-hoc Backups:

- Backup of the complete operating system, including all applications and data shall be taken before and after any significant changes that may affect the operating system, system or application software. The changes may be the result of a system upgrade, a planned power outage or any other event that may put the system and data at risk.
- All ad-hoc backup shall be initiated by the data owner, who shall send a formal request for backup of the same.
- Based on the retention period specified in the backup request form and the classification level, the media shall be stored, erased or destroyed.

Event or Calendar-based backup procedure:

- Applications may require a backup based on occurrence of an event or a quarterly, end-of-month or end-of-year backup
    - Asset Owners with specific backup requirements driven by either events or the calendar shall provide written instructions to the IT team detailing those requirements with the associated retention requirements for the backup media.
    - IT team performs backup according to the written instructions from the Asset Owner.
    - Media produced, as a result of an Asset Owner request, shall be placed in secure on-site/off-site storage.

Backup Register and Logs:

- A register of the backups, including the verification of their success and failures shall be maintained at the location where restoration activity was carried out with the details as under.
    - Date and time of backup (start time and end time).
    - Type of backup (Incremental / Full/Differential).
    - The label of the tape/CD/DVD/Hard disk used.
    - The details of offsite / on site storage of media.
    - Details of movement of the tape (if stored offsite).
    - Date of movement.
    - Courier Company used.
    - Whether backup completed successfully.
    - Reasons for unsuccessful backup (if any).
- Automatic logs shall be generated which show the status of the backups taken.
    - These status logs shall be sent to the application owners in case of applications and to HODs in case of failure of the identified desktops and laptops by the IT Administrator indicating the success/failure of critical server's (SECRET, CRITICAL, CONFIDENTIAL) backup and failure of GENERAL servers as may be applicable.
    - All the backup logs shall be archived by the IT Administrator on a dedicated system with restricted access.

Selecting an Off-site Storage Facility

- The off-site storage facility shall be at least 15 kilometers (9.32 miles) from the facility and not be located within the same flood plain, tectonically unstable area, or other area of significant shared physical or environmental risk.
- The off-site storage facility shall not be located in an area that would be inaccessible due to blocked streets or damaged bridges in the event of a natural disaster or civil unrest.
- The off-site storage facility shall either have an alternate source of backup power or be on a different power grid than the facility.
- The off-site storage facility shall be accessible by at least three entirely different routes to disaster recovery site and to the facility.

- Off-site storage facilities must provide physical and environmental security that is compliant with the requirements of the companies Physical and Environmental Policy for Information Security.

Contents of Off-site Storage:

- Secure off-site storage shall contain the following:
    - Removable media containing backup data.
    - Copy of the current inventory of the backup media that are both on-site and in off-site storage.
    - Copies of all procedures addressing backup, restoration, and reconstitution of data storage.
    - Copy of log reflecting introduction and removal of contents of off-site storage.

Media Rotation:

- The rotation of the media shall be informed by the respective application owners to the IT (Backup and restoration) Team in writing for every quarter. Any change to this schedule shall also be done in writing and informed to the IT team. The rotation data of media shall also be maintained by the Information Security Team.

Restoration Drills:

- Restoration shall be scheduled monthly basis or atleast once a quarter for CRITICAL/CONFIDENTIAL data by the respective IT Administrators. The result shall be communicated in writing by the IT Head to the respective application owners/HODs. The IT administrator shall select a tape at random basis for restoration drill of or as requested by the concerned application owner and HOD.
- A log of restoration drills shall be maintained by IT Administrator to include the following details:
    - Tape Identification Number.
    - Date and time of drill.
    - Whether restoration completed successfully.
    - Whether the process owner has verified the restored data.
    - Details of review by the IT Team.
    - Reasons for unsuccessful restoration (if applicable).
    - Corrective Actions if any.
- After the restoration drill is completed successfully, the media shall be safely returned to its original location.
- In case of failure in restoration, the IT Administrator shall inform the application owner/Information Security Team citing reasons of failure and the nature of the intervention required. The Infrastructure Head along with the concerned manager with ISO/ HOD oversight and IT Administrators shall decide on the corrective action.
- The IT Administrator shall log the incident and shall update the media issue register (if required) and inform the Information Security Team.
- The restoration drill for backups taken by user on the external media (CDs/DVDs) shall be user's responsibility.

Restoration of Backups in case of data loss:

- Servers:
    - The IT Team shall decide on the tape to be used for restoration. The tape, as far as possible, shall be the most recent successfully backed up tape.
    - Recovery procedures as defined by application owners shall ensure the relevant files are restored in order to ensure full application functionality is restored.
    - Restoration is being done on a standby machine and then transferred to the live machine. Restoration directly on a live machine shall be treated as an exception and a written approval from Head of IT/HOD shall be taken.
    - After successful test restoration, the restoration shall be carried out on the actual server.

    - While restoring the files and directories, it shall be ensured that access permissions are not changed or corrected after restoration is complete.
    - IT Administrator shall maintain a log containing details about the date and time of restoration, label of the backup media, location of storage etc. These details shall be filled in the restoration form and filed in Restoration register.
    - The IT Administrator shall inform the Infrastructure Team about the data loss on the server. The Information Security Team shall also be informed to log the incident.
- Outdated Media Formats:
    - The IT Administrator shall convert the existing backups to the new formats if required. This shall be applicable in case of old floppies and tapes from legacy systems if any.
- Disposal:
    - There shall be a formal mechanism for the execution of the disposal process.
    - With approval from the concerned department/ application owner /information security team/ IT Team, the data on the media shall be erased completely before disposal.
    - It shall be ensured by the IT Administrator that the media is completely unreadable before discarding it.
    - The hard disk media shall be degaussed or physically destroyed, while the tapes shall be crushed/ cut into multiple pieces or degaussed under supervision of the personnel from IT Team.
    - Disposal records shall be maintained for audit purpose by IT Team
    - The Media Issue Register shall be updated accordingly if the tapes are being incinerated/ destroyed through a third party with NDA to protect from violations. A supervisor from the side of PIPL shall be present at the time when PIPLs' media is being destroyed at the external party's premises.

Responsibilities

The responsibility for implementing this policy is with the following personnel:

IT Administrator and Team:

- Label and issue the media.
- Review the status logs of the backup activity.
- Inform the application owners/HOD whenever there is a failure of data backup.
- Ensure proper configuration of the backup system.
- Backup data in accordance with the schedule.
- Maintain / Review restoration drill schedules and execute the same.
- Restore data whenever requested and take a sign off from the requester of successful restoration
- Maintain accounting of issued media.
- Assign the responsibilities of backup to the IT Administrator.
- Review the backup request and assign the task to IT Administrator.
- Random review of the backup/restoration logs and media. Review media issue register.
- Approve direct restoration on live server in case of data loss.
- Approve disposal of media.
- Manage offsite backup process
- Ensure Information Security Team Audits the backup process on-site and offsite.

HOD, application owners and Users as the case may be:

- Give information to IT Team about the data to be backed up, the frequency of backups etc. taking into consideration the criticality of information.
- Ensure backups are taken for their business-critical data.
- Request restoration in case of loss to data.
- Record the incident in case of loss of data on the server and restoration failure.

- Employees and third parties of PIPL are expected to ensure backup of CRITICAL and CONFIDENTIAL business data and adhere to this procedure. Non-compliance to this could result in disciplinary action as per the code of conduct of the organization.
- While restoring the files and directories, it shall be ensured that access permissions are not changed after restoration is complete.

Metrics

Metrics shall be measured by IT Team and shall be reported to respective HoDs every quarter.

The periodicity of reporting shall be once in a quarter and shall include, but not limited to:

- Number of times restoration has failed for Critical and Confidential assets
- Number of times data was lost on account of back up not being taken.
- Number of times media was lost on account of it not being entered into the register before removal.
- Number of times back up media was lost in transit/damaged/stolen.
- Media wise issues during the backup procedure.
- Number of times scheduled back up and restoration has not happened.
- Media destroyed without any record.

Existing modules

1. Vessel Module
2. Cargo (Containerized / Non-Containerized) Module
3. Regulatory Clearance Module
4. Payment Module
5. Latch-on Services

Documents exchanged during import procedure

Sr. No.	Document	From	To
1	IEC Number	DGFT	Importer
2	Import General Manifest	Carrier	Customs
3	Import license	DGFT	Importer
4	Invoice	Exporter/ Seller	Importer
5	Packing List	Exporter/ Seller	Importer
6	Terms of Shipment	Importer	Exporter / Seller
7	Certificate of Insurance	Exporter/ Seller	Importer
8	Certificate of Origin	Exporter/ Seller	Importer
9	Letter of Credit	Bank	Importer
10	Bill of Lading	Shipping Line	Exporter / Seller
11	Arrival Notice	Shipping Line	Importer
12	Bill of Entry	Importer	Customs
13	Duty receipt	Customs	Importer
14	Delivery Order	Shipping Line	Importer
15	Gate Pass	Terminal Operator	Importer
16	Equipment Interchange report	Shipping Line	Terminal operator
17	Equipment Interchange report	Terminal Operator	Importer
18	Endorsed Bill of Lading	Bank	Importer
19	Goods receipt	Truck	Importer

Sr. No.	Document	From	To
21	LEO	FF cum CB	Shipping Line
22	GST RFD 11	Shipping Line	Sea Port
23	Equipment Interchange Report	Sea Port	Rail Operator
24	Export Load Plan	Shipping Line	Sea Port
25	Mate Bill	Shipping Line	Exporter
26	Master Bill of Lading	Shipping Line	Exporter
27	Master Bill of Lading	Exporter	Exporter's Bank
28	Export General Manifest	Shipping Line	Customs

8.7 Annexure VII

Latest developments in PCS1x- New milestones achieved during Covid and recent period- Transformation into NLP including different latch-ons and API integration

A. DIGITALIZATION OF SHIPPING AND TRADE DOCUMENT

For issuance of the Delivery Order for the imported cargo, the Importer/Consignee or nominated Customs Broker / Freight forwarder has to surrender the Original Bill of Lading (OBL) to the Shipping Line along with the other documents such as KYC, Bond etc . On the basis of same Shipping Line generates the Invoice. The requisite payment is made and Shipping Line issues the Delivery Order (DO/eDO).

With the ongoing COVID19 pandemic situation and subsequent lock down/reduced mobility imposed by the Government of India for general public, maritime trade is facing challenge for submission of the OBL with Shipping Line. This is impacting further delay in getting delivery of cargo to the consignee.

To overcome this challenge, had called upon for electronic process of submission of OBL to Shipping Lines. Therefore, Shipping Lines, Trade Associations of the Customs Brokers, Freight Forwarders has come forward with suitable process (Has minute differences in each ones suggestions).

This process will involve with connecting of various stakeholders as per the different scenarios as suggested by trade. Stakeholders involved in this are Shipper of cargo (organisation out of India; not part of PCS1x), Banks (Partially part of PCS1x), Importers, Customs Brokers, Freight Forwarders, Shipping Lines and Custodians. Other than Shippers and Banks all other stakeholders have to be registered users of PCS1x.

B. e-Conveyance of OBL and release of goods on e-DO

The proposed solution enables the stakeholders to submit the requisite documents and eliminate the need to visit the offices of the Shipping Line. Also, system will have track and audit logs of the activities performed on PCS1x. This will boost the Government objectives of ease of doing business and social distancing. This functionality has been deployed on production.

Status:
In this connection, IPA has taken the initiative and started the integration with e-B/L service providers with PCS 1x. The details of which are as follows:

1. CARGOX

   The solution enables the stakeholders to submit the requisite documents and eliminate the need to visit the offices of the Shipping Line. The system will have track and audit logs of the activities performed on PCS1x. This will boost the Government objectives of ease of doing business and social distancing.

   End to end live shipment was conducted on blockchain (1st time in India) during lockdown period.

2. essDOCS

   Integration with essDOCS enables PCS 1x to extend the facility of e-B/L to a larger share of the market. **This is an achievement in itself, by integrating on a single platform, 2 of the 5 service providers in the world in this space**.

3. Tradelens

   Service provider for providing services for the facilitating electronic B/L services was referred by the trade to be integrated with PCS1x. Demo, Dialogue and discussions with Tradelens ongoing. Work is in progress.

4. Bolero

   Service provider for providing services for the facilitating electronic B/L services was referred by the trade to be integrated with PCS1x. Dialogue ongoing, last meeting conducted on 15th July 2020. Work in in progress.

C. Integration with Transportation Service Providers

Thecovid 19 and the subsequent lockdown has had a major impact on trade due to several reasons such as displacement of migrants, shortage of service providers, unavailability of capital, etc.
In order to encounter such issues, IPA took the initiative to onboard below service providers on PCS 1x so as to facilitate the users to book transport for their cargo and container electronically by adhering to social distancing norms and requirements.

1. Return Trucks – Andhra Pradesh, Tamil Nadu and Telangana
2. Gocon– Maharashtra, Gujarat and West Bengal

D. CUSTOMS API INTEGRTION

<u>VCN Standardization initiative –</u>

- For sharing the Vessel Call Number (VCN) with Customs there is requirement of the standardisation as numeric values may get repeated for different ports. Each Port has unique standard for allocating the VCN number.
- IPA has taken initiative and converted the VCN number at PCS 1x level as per requirement of the Customs.
- Three payloads namely VCN ATR(TOCHI02), ELR (TOCHI03) have been made LIVE and is being exchanged with ICEGATE in real time

<u>Others API payload</u>

- Testing for next set of messages is underway

E. EDO IMPLEMENTATION AT MUNDRA PORT

- PCS1x has functionality of electronic delivery order to be submitted by Shipping Line/Agent and PCS1x shares the eDO in consumable format with the Ports/CFS/ICD.
- eDO is being used extensively by Major Ports of India. During COVID 19, Mundra Port officials approached IPA for support for implementing the eDO at PCS 1x level at Mundra Port.

Mundra Port has become the first private port to start sharing the VCN details with the PCS1x and accepting the delivery order via PCS1x.

F. **DGFT INTEGRATION**

- Integration Scope:
  - E-Certificate of Origin (linkage with eInvoice to eDO)
  - IEC Code validation
  - KYC User Registration on PCS 1x.
- Discussion initiated; meeting held with DGFT on 17th July 2020 and agreed to start IEC code validation within 3-4 days

G. NAVY INTEGRATION

- Navy had approached IPA with requirement of PANS (Pre-Arrival Information) from PCS 1x
- UAT for Vessel Profile completed - Production deployment done and made LIVE

H. **DGSHIPPING INTEGRATION**

- IPA had meeting with the Director General of Shipping Shri Amitabh Kumar on 24th June 2020 to demonstrate the functioning of the dashboard developed for DG Shipping. During the meeting, various points were discussed including the need for a 100% digital port call.
- Action points under progress:
  - Integration with LRIT system for live tracking of vessels
  - To make modifications in the dashboard as desired by DG Shipping
  - MMD to start sharing the required information with PCS 1x
  - FAL Convention and HNS Convention requirements to be incorporated onto PCS 1x.

I. LDB INTEGRATION

- LDB (Logistics Data Bank) has been integrated with PCS 1x to facilitate real time tracking of containers
- LDB had conducted open house session on 3rd January 2020 at Hotel Ashok, New Delhi. During the session, it was discussed for the information coverage of the LDB to be enhanced in order to assess the insights and identify bottlenecks in the supply chain.
- Accordingly, National Industrial Corridor Development Corporation Limited approached to IPA for additional integration between PCS 1x and LDB.
- IPA/PCS team thereafter has undertaken multiple discussions with LDB technical team to understand the data requirements and modalities of the integration for which development is currently underway.
- Once completed, this project will help in reducing India's transaction cost by bringing in information available with various stakeholders on a single platform to help the trade in effective planning, coordination and streamlining of business processes. In this connection, agreement has been finalized and signed.

J. ePAYMENT BANKS

A. IDBI Bank
- Additional option for selection of Corporate Banking option to cater to upgrade net banking version of IDBI
- Development for facilitating payment verification on two different services

B. HDFC Bank
- Dialogue started to facilitate integration with upgraded net banking system

- Development required for facilitating payment verification with two different net banking platforms

C. Kotak Mahindra

- integration of Kotak Mahindra payment gateway to facilitate any bank to any bank transactions has been done

K. NATIONAL LOGISTICS PORTAL – MARITIME

PCS 1x provides its robust infrastructure and strong user base of stakeholders from 27 different categories. A natural platform to bootstrap to National Logistics Portal (NLP)

IPA is in process for bootstrapping PCS1x to National Logistics Portal -Marine to act as Unified Digital Platform. Expected timeline for NLP Marine tender to implementation of project is estimated to be around 12 months

8.7.1 List of Stakeholders of PCS 1x:

Sr. No.	Stakeholder	Registered Users
1	Port Authority	158
2	Shipping Lines/ Shipping Agent	3301
3	Customs	2
4	Container Freight Station	158
5	Custom Broker	4898
6	Importer / Exporter	5852
7	Bank	8
8	Container Agent	564
9	Terminal Operator	45
10	Stevedore	236
11	Rail Transport Operator	60
12	Mercantile Marine Department (MMD)	14
13	Navy/Coast Guard	11
14	Ships Chandler	84
15	Port Health Organisation	11
16	Transporter	17
17	Surveyor	11
18	Inland Waterways	3
19	Coastal Shipping Operator	18
20	Empty Yard	219
21	Freight Forwarder	23
22	Barge Owner / Operator	6
23	NVOCC	172
24	DGLL	1

25	Inland Container Depot	104
26	Immigration	0
27	Tank Farm Operator	8
Total		**15976**

8.7.2 Latch on services carried out on PCS 1x

Service Provider	Service	Remarks	Status as on date
JMB Technologies (P-CaSO)	eBL,	Live on production	Latch on agreement signed.
	Transport		Latch on service provided with eBL by Cargox and essDOCS
	eVGM and Booking		Transport – Return Trucks and GOCON
			eVGM- Portall Infosystems
ODEX	eDO	Integrated with PCS 1x via API.	LIVE
Kale Logistics	e-VGM, e-DO and Codex Exports module at Tuticorin location.	Final Agreement forwarded to M/s Kale for signature.	Con call done with Kale Team on 6th March 2020
			IPA has put reminder to Kale Team on 15th March 2020
			Awaiting response
Master Marine	eVGM, Form-13	Products: Integration for e-VGM, Form-13 and Shipping Bill Data	Discussions ongoing for integration of VERMAS
			Awaiting technical documents and agreement
Bolero	Blockchain Platform	Under Discussion	Under Discussion, meeting conducted on 22nd July 2020
			Latch-on agreement to be signed and effort estimate to be prepared
LDB	Container Tracking	Live on Production environment from 16th January 2020.	LIVE
			Further integration taken up as per requirements received from LDB
PortShield (Corsenant)	RFID Tracking	Awaiting Presentation and Requirement Document	Awaiting tri-partite latch-on agreement.
Tradelens	Blockchain Platform for e B/L	Under Discussion	Under Discussion
			Awaiting response from 29th May 2020.
			Awaiting tri-partite latch-on agreement.
Trucksuvidha	Transport	Awaiting Response	API document received on 10th April 2020.
			Awaiting tri-partite latch-on agreement
Shipsy	Cargo Booking	Awaiting Response	Demo conducted on 28th

Service Provider	Service	Remarks	Status as on date
			February 2020
			Awaiting tri-partite latch-on agreement

8.7.3 API Integrationwith Stakeholders

Sr. No.	Category	Name	API On Production	API under testing	Status
1	Port	Mumbai Port Trust	36	0	Live
2	Port	JN Port Trust	14	5	Live
3	Port	New Mangalore Port Trust	0	41	UAT Complete
4	Port	Cochin Port Trust	0	30	UAT Complete
5	Port	EBS Project	0	55	UAT ongoing
6	Shipping Line	ONE	0	1	UAT Complete
7	Shipping Line	Omega	0	1	UAT Complete
8	Shipping Line	Evergreen	0	1	UAT ongoing
9	CFS	Adani Exim yard	8	0	Live
10	CFS	Ashte Logistics Pvt. Ltd.	8	0	Live
11	CFS	International Cargo Terminal Private Limited (Globicon)	8	0	Live
12	CFS	SAURASHTRA FREIGHT PVT LTD	8	0	Live
13	CFS	TG Terminal Kolkata	8	0	Live
14	CFS	TG TERMINALS PVT LTD	8	0	Live
15	CFS	TRANSWORLD TERMINALS PVT LTD	8	0	Live
16	CFS	Vaishno Logistics Yard (Transworld CFS)/ TG Terminal	8	0	Live
17	CFS	Adani CFS	0	8	Under Testing
18	CFS	Continental Warehousing Ltd.	0	8	Under Testing
19	CFS	Hind Terminal CFS	0	8	Under Testing
20	CFS	HONEYCOMB LOGISTICS PVT. LTD.	0	8	Under Testing
21	CFS	JWR Logistic Pvt. Ltd	0	8	Under Testing
22	CFS	MUNDHRA CONTAINER FREIGHT STATION PVT LTD	0	8	Under Testing
23	CFS	MUNDRA INTERNATIONAL CONTAINER TERMINAL	0	8	Under Testing

24	CFS	Navkar Corporation Ltd.-III	0	8	Under Testing
25	CFS	Seabird CFS	0	8	Under Testing
26	CFS	SEABIRD MARINE SERVICES PVT LTD	0	8	Under Testing
27	CFS	Seabird Marine Services Pvt. Ltd.	0	8	Under Testing
28	CFS	Speedy Multimodes Ltd.	0	8	Under Testing
29	CFS	United Liner Agencies of India Pvt. Ltd. (MICT)	0	8	Under Testing

8.7.4 Business transactions per day on PCS 1x

Month-wise EDI Transactions for all Ports

Month	Vessel	Finance	Cargo	Customs	Daily Average
Apr-20	13331	42118	24074	548784	20944
May-20	14736	47179	36933	1179893	42625
Jun-20	17311	48080	39538	1599316	56808
Monthly Average	15126	45792	33515	1109331	---------

Month wise E-Payment

Month	Apr-20	May-20	Jun-20
e- payment	38260.75	36666.55	41857.21

***Amount in INR Lakhs**

8.7.5 Stakeholder wise break-up of per day transactions on PCS 1x

ROLE WISE TRASACTION COUNT (APR 20 to JUN 20)*(QURTERLY)*					
ROLE CODE	**ROLE NAME**	**Apr-20**	**May-20**	**Jun-20**	**Grand Total**
BA	Bank	10	12	20	42
BO	Barge Operator	44	59	14	117
CAGU	Container Agent	922	1381	1783	4086
CDADM	ICD Administrator		2	1	3
CDGU	ICD Shipping Line	1	23	1	25
CFS	Container Freight Station	659	761	869	2289
CHA	Customs Broker	2890	4217	3160	10267
DGS	DG Shipping			13	13
FF	Freight Forwarder	6			6
IE	Importer/Exporter	2561	1963	1915	6439
IW	Inland Waterways	1		32	33
NCG	Coast Gaurd / Indian Navy			12	12

NVOCC	Non Vessel Operating Common Carrier	56	131	88	275
PF	Port Finance	17	12	16	45
PHO	PHO	4			4
PM	Port Marine	120	187	222	529
PO	Port Operations	3418	3623	3755	10796
POADM	Port Admin	300	455	490	1245
PT	Port Traffic	2	7	4	13
RA	Regulatory Authority			2	2
RTGU	Rail Transport	25	32	41	98
SA	Shipping Agent	23247	27277	26781	77305
SAADM	SA Administrator	2			2
SC	Ship Chandlers	94	95	138	327
SL	Shipping Line	110	217	275	602
SM	Shipping Minister			2	2
STV	Stevedore	83	95	93	271
TOADM	TO Administrator	1			1
TOGU	Terminal Operator	137	120	129	386
TR	Transporter			16	16
Grand Total		**34710**	**40669**	**39872**	**115251**

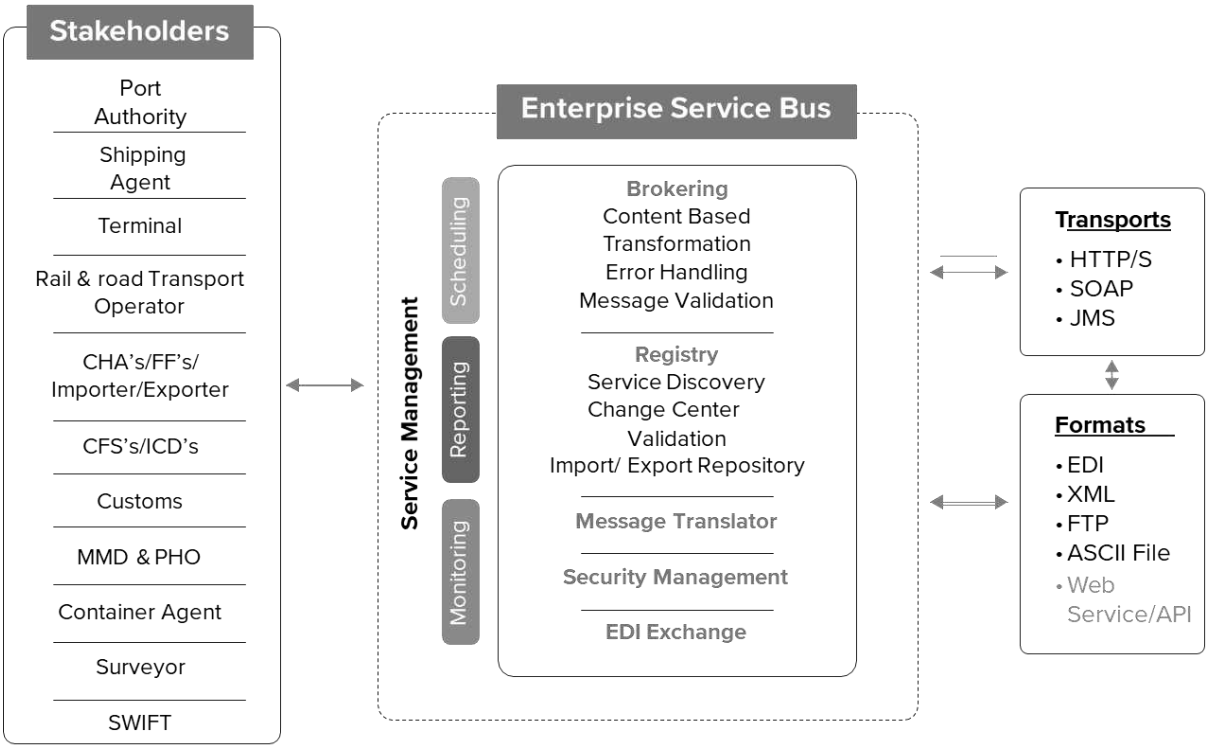
8.7.6 API Integration with existing stakeholder application

PCS 1x is integrated with below stakeholder categories via API for exchange of information

Stakeholder Category	Count
Ports	6
CFS	21
ICD	3
Shipping Lines	3
Customs	-
Banks	11
Payment Gateways	5
Transport Service Providers	2
e-BL	1
DGFT	-
LDB	-

8.7.7 Information on Data exchange with various user (Different Formats such as XML,

PDF, EDI Messages etc.)



8.8 Annexure VII

INFORMATION REQUIRED FOR SIZING NLP MARINE

List of Total Stakeholders to be part of NLP-Marine

In addition to current 27 categories of stakeholders in PCS 1x for performing various activities, below stakeholders will be additional:

1. DG Shipping
2. DGFT
3. Inland Waterways – Terminals
4. Inland Waterways – Vessel Operators
5. Warehouse Provider
6. Insurance Provider
7. *Additional PGAs and EPCs*

Modules proposed in NLP-Marine

Cargo Service Platform	
Module Name	**Mapping with Services**
Registration Module	Stakeholder Registration
	Stakeholder Service Quality Check/Validation
Login Module	Multiple methods of user login
Order Submission Module	Selection of Trade type-Import/Export/Domestic Tools
	Submission of Export/Import/Domestic Trade information – Commodity, Source & Destination, Estimated delivery & pickup date, Packaging details (weight, number, size etc.) Payment terms, Incoterms, pickup address etc.
	Selection of Export/Import/Domestic Trade services from service catalogue
	Listing of available routes – Road, Sea, Rail depending on selection of transport mode type service
	Listing of Export/Import/Domestic Trade service providers depending on the type of service selection
	Selection of Logistics service providers depending on the type of filters applied by the exporter/importer/domestic trader
	Subscription of Value-added Services. Example: Insurance purchase
	Submission of request for bidding based on inputs from exporter/importer/domestic trader
Documents Exchange Module	Submission of request for data exchange with marketplace stakeholders
	Data Exchange with 3rd party & External systems
	Shipping Bill Generation, LEO etc.
Track and Trace Module	Consignment Tracking on Google Map
	Data Exchange with 3rd party & External systems
Document Management System Module	Data Exchange with 3rd party & External systems
	Document storage
	Document submission
Payments Module	Invoice Generation
	Duty Payment
	Online Payment
Ratings Module	Portal User Rating
	Stakeholder Feedback & review
Business Transaction Support Module	Support
MIS Module	Dashboards and Analytics
Content Management Module	Portal Content Generation
	FAQs
Mobile app-Login Module	Multiple methods of user login
Mobile app-Order Module	Listing of all orders received
	Service Consumer Rating
	Grievance Redressal

Mobile app-Track and Trace	Update consignment status and location

Finance and Insurance Platform	
Insurance Module	Price discovery of insurance service from different service provider.
Trade Finance Module	Selection of service provider for obtaining the Letter of Credit and/or other relevant documents
Document Sharing Module	Document exchange through NLP exchange platform

Regulatory Bodies and PGAs Platform	
Listing Module	Information about the list of certificates, supporting documents, estimated time etc. on the basis of commodities, source location, destination location etc.
Payment Module	Payments for certificates
EPC/PGA Interface Module	EPC/PGA simple interface for digital enablement
Integrated Regulatory Module	Integration with customs and services

Certification Platform	
Listing compulsory certification requirement	Compulsory certification requirement for origin/destination and product pair
Online certification system	Common Application Form for all certificates
	Obtaining certificates/ license/ authorization from the concerned PGA/ EPC
Track and Trace	Mobile and web-based notification
	Visibility of ETA for different certifications

Latch on services proposed in NLP-Marine

1. Transport Module
2. Empty Yard Module
3. VGM Module
4. E-SEAL Module
5. Rail Module
6. Terminal Module
7. CFS Module
8. ICD Module
9. Booking Module
10. Liner Solution (booking and route management)
11. Clearance Module

12. Document Manager
13. E-Payments Module
14. E-Berthing Module

List Participating Govt. Agencies

List of PGAs

Sr No	PGA / Commodity Body
1	Food Safety and Standards Authority of India
2	Central Drugs Standard Control Organization
3	Wildlife Crime Control Bureau
4	Directorate of Plant Protection, Quarantine & Storage
5	Animal Quarantine Certification Service
6	Committee for the Purpose of Control And Supervision of Experiments on Animals
7	Hazardous Substances Management Division
8	Central Pollution Control Board
9	Department of Animal Husbandry, Dairying and Fisheries
10	Central Farm Machinery Training and Testing Institute, Budni, Madhya Pradesh
11	Telecommunication Engineering Centre (TEC), Department of Telecommunications
12	Central Bureau of Narcotics
13	Ministry of New and Renewable Energy
14	Textile Committee
15	Bureau of Indian Standards
16	Legal Metrology Unit
17	Directorate General of Civil Aviation
18	Archeological Survey of India
19	Chief Controller of Explosives
20	Director General of Foreign Trade
21	Ministry of Home Affairs
22	Vehicle Research and Development Establishment, Ahmednagar
23	Ministry of Electronics and Information Technology
24	The Export Inspection Council (EIC)
25	The Directorate General of Hydrocarbon
26	Bureau of Energy Efficiency
27	National Authority, Chemical Weapons Convention
28	Central Insecticide Board
29	The Directorate General of Hydrocarbon

List of EPCs

Sr No	EPC / Commodity Body
1	Agriculture & Processed Food Products Export Development Authority
2	(APEDA)

3	Chemical and Allied Export Promotion Council (CAPEXIL)
4	Carpet Exports Promotion council
5	Gem & Jewellery Export Promotion Council
6	Indian Oilseeds & Produce Export Promotion Council (IOPEPC)
7	Apparel Exports Promotion Council
8	Basic Chemicals, Cosmetics and Dyes EPC (CHEMEXCIL)
9	Coffee Board
10	Cotton Textiles Export Promotion Council
11	EEPC INDIA (Formerly Engineering Export Promotion Council)
12	Electronics and Computer Software EPC
13	Export Promotion Council for EOUs & SEZs
14	Federation of Indian Export Organisations
15	EPC for Handicrafts
16	Handloom Export Promotion Council
17	Leather EPC
18	Pharmaceuticals Export Promotion Council
19	Plastics Export Promotion Council - PLEXCONCIL
20	Powerloom Development & Export Promotion Council
21	Projects EPC
22	Rubber Board
23	Services EPC
24	Shellac & Forest Products Export Promotion Council
25	Sports Goods EPC
26	Synthetic & Rayon Textiles Export Promotion Council
27	Tea Board
28	Telecom & Communication EPC
29	Tobacco Board
30	Woolen –WWEPC
31	Wool Industry Export Promotion Council
32	Cashew Export Promotion Council of India
33	Coconut Development Board
34	Coir Board
35	Indian Silk Export Promotion Council
36	Jute Products Development and Export Promotion Council
37	Marine Products Export Development Authority
38	Spices Board

Comprehensive list of services under

Cargo Services & Carrier Services

S. No.	Module Name	Mapping with Services
1	Registration Module	Stakeholder Registration Stakeholder Service Quality Check/Validation
2	Login Module	Multiple methods of user login
3	Documents Exchange Module	Submission of request for data exchange with marketplace stakeholders Data Exchange with 3rd party & External systems Shipping Bill Generation, LEO etc.
4	Track and Trace Module	Vessel Tracking Consignment Tracking on Google Map Data Exchange with 3rd party & External systems
5	Document Management System Module	Data Exchange with 3rd party & External systems Document storage Document submission
6	Payments Module	Invoice Generation Duty Payment Online Payment
7	Ratings Module	Portal User Rating Stakeholder Feedback & review
8	Business Transaction Support Module	Support
9	MIS Module	Dashboards and Analytics
10	Content Management Module	Portal Content Generation FAQs
11	Mobile app-Login Module	Multiple methods of user login
12	Mobile app-Order Module	Listing of all orders received
13	Mobile app-Track and Trace	Visibility of live details with approvals subject to acceptance by stakeholder

Regulatory Bodies & PGA services

S. No.	Module Name	Mapping with Services
1	Listing Module	Information about the list of certificates, supporting documents, estimated time etc. on the basis of commodities, source location, destination location etc.
2	Payment Module	Payments for certificates
3	EPC/PGA Interface Module	EPC/PGA simple interface for digital enablement
4	Integrated Regulatory Module	Integration with customs and services

Finance & Insurance Services

S. No.	Module Name	Mapping with Services
1	Insurance and Trade	Selection of service provider for obtaining the Letter of

	Finance Module	Credit and/or other relevant documents
2	Document Sharing Module	Document exchange through NLP exchange platform

Existing number and expected number of users under each service

Existing Total Number of Users of PCS 1x: 15976

Expected Users

Carrier: 17750

Cargo: 314830

Regulatory Bodies and PGAs: 793

Banking and Insurance: 1400

Anticipated Business transactions per day

Business Transactions per Year : 376618000

Business Transactions per Day: 1031830

Anticipated Total users and concurrent users

Anticipated Total Users: 334777

Anticipated Concurrent Users: 6,709

8.9 Annexure IX

8.9.1 LATCH ON AGREEMENT

This Latch on Agreement ("hereinafter referred as "Agreement") is made and entered into on this _____ day of _____, 2020 ("Effective Date") by and between,

INDIAN PORTS ASSOCIATION, a society registered under The Societies Registration Act,1860 having its office at 1st Floor, South Tower, NBCC Place, Bhisham Pitamah Marg, Lodhi Road, New Delhi, Delhi 110003 (hereinafter referred to as "IPA" which expression shall unless repugnant to the context or meaning thereof be deemed to mean and include its successors, and permitted assigns) of the FIRST PART;

AND

_____, a company incorporated under the provisions of the Companies Act, 1956 and having its Registered Office at_____, as a Latch on service provider (hereinafter

referred to as “LSP” which expression shall unless repugnant to the context or meaning thereof be deemed to mean and include its successors, and permitted assigns) of the SECOND PART;

(IPA and LSP are individually referred to herein as a “Party” and collectively as “Parties”.)

WHEREAS

IPA, under the guidance of Ministry of Shipping has embarked on rolling out the PCS 1x platform connecting Maritime stakeholders in the country. It has been designed as an “Open Platform” which allows coexistence of multiple service providers to provide EXIM related services independently or by using connectivity options and data as authorized by IPA. In order to expand the adoption of the platform, IPA has devised a Latch On program for other platforms/solutions, available in the country for Maritime trade to seamlessly connect with PCS 1.x. IPA is in the process of coming out with a National Logistics Portal (NLP) and the governance for the same will be assigned to a SPV/Joint Stock Co in due course. This agreement will be novated/assigned to the aforementioned agency

LSP is in the business of providing IT Solutions and services to the Logistics Industry and desirous to provide those solutions and services to the Maritime stakeholders through the Platform and IPA has agreed to avail the Latch on services from the LSP on the terms and conditions as described and agreed to between both the parties in this Agreement.

NOW THEREFORE, in consideration of the representations, promises and mutual covenants and agreements set forth herein, and for good and other valuable consideration, the Parties hereby agree as follows:

DEFINITIONS.

When used in this Agreement the following words and expression shall have meanings assigned hereto:

“Account” means the Account of the LSP’s Latch on Modules end users which enables access to and use of the Latch on Modules;

“Affiliates” means any entity controlling or controlled by or under common control with a Party, where “control” is defined as the ownership of more than 50% of the equity or other voting interests of such entity or the power to direct or cause the direction of the management or policies of such entity, whether through ownership, voting securities, contract or otherwise.

“As-Is’’ means the existing and the demonstratable functions and features of the Latch on Module.

“Confidential Information” shall include all information or material that has or could have commercial value or other utility in the business or prospective business of the Disclosing Party or its subsidiaries or affiliates. Confidential Information also includes all information of which unauthorized disclosure could be detrimental to the interests of the Disclosing Party or its subsidiaries or affiliates whether or not such information is identified as Confidential Information. By example and without limitation, Confidential Information includes, but is not limited to, any and all information of the following or similar nature, whether or not reduced to writing: Customer lists, customer and supplier identities and characteristics, Agreements, marketing knowledge and information, sales figures, pricing information, marketing plans and business plans, strategies, forecasts, financial information, budgets, software, research papers, projections, procedures, routines, quality control and manufacturing procedures, patents, patent applications, processes, formulas, trade secrets, innovations, inventions, discoveries, improvements, research or development and test results, data, know-how, formats, plans, sketches, specifications, drawings, models, and any other information or procedures that are treated as or designated secret or confidential by the Disclosing Party or its customers or potential customers.

For purposes of this Agreement, the term “the Disclosing Party” shall be the party that discloses Confidential Information to the Receiving Party.

For purposes of this Agreement, the term “the Receiving Party/Recipient” shall be the party that receives Confidential Information from the Disclosing Party and shall include the Receiving Party, the company he or she represents, and all affiliates, subsidiaries, and related companies of the Receiving Party.

For purposes of this Agreement, the term “Representative” shall include each party’s directors, officers, employees, agents, and financial, legal, and other advisors.

“Data” means any content uploaded and shared on the PCS 1x, regardless of the method of upload or sharing, or whether the Data was the result of an upload, the combination with other Data or enrichment of the Data by IPA or LSP;

“Data Sharing Rules” means the unambiguous and clear sharing rules applicable to the Data.

“Deliverables” shall mean all or part of the software or services to be delivered and/or milestones to be achieved by LSP.

“Force Majeure” means any event or circumstance or combination thereof, which satisfies all of the following (i) materially and adversely affects the performance of an obligation by a party; (ii) are beyond the reasonable control of the affected Party; (iii) are such that the affected party could not have prevented or reasonably overcome with the exercise of reasonable skill, care and diligence; and (iv) do not result from the negligence, misconduct, breach or default on part of the affected Party. Force Majeure includes the following conditions provided they satisfy the foregoing conditions: war (whether declared or undeclared), act of sabotage, revolution, act of terrorism, explosions, radioactive or chemical contamination, strikes or lockouts, fire, floods, earthquake, tidal wave, cyclones, tornado, epidemic, pandemic etc.

“Integration” shall mean the process of coupling the Latch on Module with PCS 1x

“Intellectual Property Rights” means all rights, title or interest conferred under statute, applicable law or equity in relation to, inventions (including patents), copyright (including in relation to software), service marks, trademarks, trade or business names, design rights (whether the above rights are registered, unregistered or are the subject of pending applications), circuit layouts, database rights, know-how (including trade secrets and confidential information), proprietary information, all other rights resulting from intellectual activity in the industrial, scientific, literary or artistic fields and any rights, title or interest similar or analogous to any of the above.

“Latch on Modules” shall mean the software solution (or parts thereof) and services provided by the LSP and made available on PCS 1x in accordance with this Agreement.

“Latch on Service Provider (LSP)” shall mean the government entities or any other Indian or International service provider which includes, but not limited to, Commercial Software service providers ,Logistics entities with in house developed systems, academic/social/not for profit organizations having a software solution or any other provider of software solutions in the field of Maritime Logistics who will provide Latch on Modules in order to avail benefits which may include monetary/non-monetary benefits for the LSP or its users from the Platform..

“PCS Operator” shall mean a service provider who is responsible for the development, integration, implementation, operation and maintenance of PCS 1x for the stakeholder communities of Indian Sea Ports except for the Latch on Modules.

“PCS 1x” shall mean Port Community System of Indian Ports Association.

“Platform” shall mean Port Community System i.e. PCS 1x or any other trade facilitation platform developed by IPA or its assigns or Government of India.

“Service Level Agreements” means the Service Level Agreements provided and amended from time to time by LSP and accepted by the IPA in accordance with this Agreement

"User" means a stakeholder or registered user of the Latch on Modules or Platform.

SCOPE

To serve the different stakeholders of the Platform by providing Latch on Modules and associated services in the EXIM/Shipping Industry/Port community, as detailed in Annexure 1 ("Statement of Work") of this Agreement.

TERM OF AGREEMENT

This Agreement shall have term of Three (3) years ("Initial Term") from the Effective Date unless terminated by either party with Sixty (60) days' notice period. Further, this Agreement may be extended for such period as may be mutually agreed by the parties in writing.

LICENSE BY LSP

Data Provision: - By uploading, routing, creating or otherwise providing information or Latch on Module or *Data* on PCS1x, LSP grants to IPA a non-exclusive, non-transferable and non-sublicensable license which is limited to:

make the Data/information or Latch on Module available to IPA and the users of PCS 1x, in strict compliance with the instructions made available by the LSP, who will, subject to payment of a *Fee*, if any, be granted the right to share within their organization, create derivatives from, make non-commercial use of and display specified *Data*, all in strict accordance with the Data Sharing Rules as per the provisions of this agreement

use, save, store and process any raw Data through the Platform to the extent necessary to provide, maintain use the data/information solely in an aggregated and unidentifiable manner and only for the purpose of creating industry level statistics.

LICENSE BY IPA

Data Provision: - By uploading, routing, creating or otherwise providing information to LSP, IPA grants to LSP a non-exclusive, non-transferable and non-sub licensable license which is limited to:

make the Data/information available to LSP and the users of LSP software solution, in strict compliance with the instructions made available by the IPA, who will, subject to payment of a *Fee*, if any, be granted the right to share within their organization, create derivatives from, make ~~non-~~commercial use of and display specified *Data*, all in strict accordance with the Data Sharing Rules as per the provisions of this agreement

use, save, store and process any raw Data through the Platform to the extent necessary to provide, maintain use the data/information solely in an aggregated and unidentifiable manner.

The license provided by the either party does not allow any of the party from providing such Data to any other third party

No Party is not allowed to use the Data in a manner not authorized by the providing party. Each party shall use the Data solely in full compliance with (i) the Data Sharing Rules and (iii) any applicable legislation, rules or regulations

ROLES AND RESPONSIBILITIES OF IPA

IPA undertakes and agrees that the Services of the LSP are being taken by IPA on "As is basis"IPA shall ensure that it will adhere to the data protection policies as per Government guidelines /rules requirements as amended from time to time as well as those in line with global best practices.IPA shall provide full support to LSP to enable it to provide the services to the extent possible.IPA shall, directly or through its appointed PCS operator, ensure support for integration of the services with the PCS

platform.IPA shall not unnecessarily interfere or disturb the LSP for the services being offered, without any reasonable reason.IPA represents warrants and agrees that it will not use, nor authorize, assist or permit any User or third party to use, the Services:in violation of any applicable laws or in violation with all policies and instructions communicated by LSP.

for any unlawful, fraudulent or immoral purpose, including, without limitation, the transmission of any Content in violation of applicable laws

to tamper with, alter or change the Service or the Facilities, or otherwise abuse the Service in any manner that interferes with LSP's Facilities or the use of Service by any other person.

IPA shall adhere to the following Service levels of complaint resolutions and response:

Category	Definition
Category 1	These are showstoppers that prevent any use of the Platform.
Category 2	These are major defects that cause normal operation in a module to be completely restricted with no work-around or result in significantly wrong data output.
Category 3	These are minor defects that cause normal operation to be partly restricted. A reasonable temporary work-around can however be devised.
Category 4	Trivial defects are those where one or more functions in the Platform are not working as they do, but a workaround is possible

SLA's for Defect Resolution

The SLA's for resolution of the above are as follows. IPA will provide a monthly statement on the status of reported faults.

Category	Service Level
Category 1	IPA will respond to LSP's Account Manager with a plan to resolve the problem within 2 business hours of notification. IPA will make its best efforts to resolve the problem or Provides a workaround as soon as possible. 90% of Category 1 defects would be resolved within 4 business hours

Category 2	IPA will respond to LSP's Project Manager within 6 Business hours of notification to the IPA help desk with a plan to resolve the problem or provide a workaround. 90% of Category 2 defects would be resolved within One (1) business day.
Category 3	IPA will respond to LSP's Project Manager within One (1) Business day of notification to the IPA help desk with a plan to resolve the problem. 90% of Category 3 defects would be resolved within Three (3) business days.
Category 4	IPA will respond to LSP's Project Manager within Four (4) working weeks of notification to the IPA help desk with a plan to resolve the problem.90% of Category 4 defects would be resolved in Ten (10) business days.

ROLES AND RESPONSIBILITIES OF LSP

LSP shall keep a close track of development of the services/solution and be a source of advice and suggestions in the product visualisation and testing.

LSP shall advise IPA in documentation and process.

LSP shall be required to answer questions/queries of stakeholders/users/IPA and provide quick inputs to handle the same.

PROHIBITION OF BRIBERY, CORRUPTION AND ANTI-COMPETITIVE BEHAVIOUR

Both Parties agrees to fully comply at all times with all applicable laws and regulations, including but not limited to prohibition of anticompetitive behaviour as well as any anti-corruption laws, and that they have not, and covenants that they will not, in connection with the performance of the Agreement, directly or indirectly, make, promise, authorise, ratify or offer to make, or take any act in furtherance of any payment or transfer of anything of value for the purpose of influencing, inducing or rewarding any act, omission or decision to secure an improper advantage; or improperly assisting other Party in obtaining or retaining business, or in any way with the purpose or effect of public or commercial bribery, and warrants that they taken reasonable measures to prevent subcontractors, agents or any other third parties, subject to their control or determining influence, from doing so. For the avoidance of doubt this includes facilitating payments, which are unofficial, improper, small payments or gifts offered or made to government officials to secure or expedite a routine or necessary action to which we are legally entitled.

INTEGRATION SERVICES

The LSP, for providing the Latch on Modules, will opt for one of the following modes of coupling with PCS 1x

Type 1: This will be enabled as a uni-directional flow of data/information from LSP to PCS 1x or vice versa.

Type 2: This will be enabled as two- directional flow of data/information from LSP to PCS 1x and vice versa

Type 3: This will enable the LSP to provide its Latch on Module through the PCS1x framework by way of a pseudo module of the PCS 1x platform

The LSP can change from with one type of coupling to another in agreement and with mutual consent of IPA. Bothe the LSP and IPA will ensure that any changes done at their respective end is informed at least 30 days in advance in writing to the other party so that the coupling integrity is maintained.

The integration services will be governed by the Latch on Integration Technical framework as provided in Annexure 3 and as amended from time to time.

CONFIDENTIAL INFORMATION

Each Party (the "Receiving Party" for the purposes of this Section) shall (i) use the Confidential Information of the other Party (the "Disclosing Party" for the purposes of this Section) solely for the purposes of the Agreement and for no other purpose (the "Specified Purpose"); and (ii) hold the Confidential Information at all times in the strictest of confidence and utilize no less than the highest degree of care that it uses to maintain the confidentiality of its own confidential information and shall not disclose the Confidential Information to any person, other than to its personnel, who have a need to know in connection with the Specified Purpose and content of disclosed Confidential Information shall be strictly limited on a need to know basis; and to any other party only with the prior written consent of the Disclosing Party provided in each case that (i) prior to disclosure of the Confidential Information to any such party, Disclosing Party shall have appropriate written agreements with such party, sufficient to require that party to treat the Confidential Information in accordance with the terms of this Section; and (ii) it shall be a breach of these Sections in the event any act by any such party results in the Confidential Information not being treated in accordance with this Section.

The obligations under this Section shall not apply to any information that (i) is or becomes publicly available other than by breach by Recipient of this Agreement; (ii) was already in Recipient's rightful possession prior to its receipt from Disclosing Party; or (iii) is rightfully received by Recipient from an independent source without obligation of confidentiality.

Recipient may disclose any Confidential Information to the extent required to do so under the Applicable Law provided that in such event, Recipient shall (i) promptly notify Disclosing Party and extend reasonable co-operation in any action by Disclosing Party to seek a protective order or take other steps against such requirement; and (ii) use reasonable endeavors to minimize the extent of the information disclosure pursuant to such requirement and obtain confidential treatment for the portion of the information disclosed.

Recipient shall, promptly upon the request by Disclosed Party return or destroy all Confidential Information including without limitation, all originals, copies, reproductions, extracts and summaries and certify to Disclosing Party that it has returned or destroyed such Confidential Information.

Recipient agrees that the use or disclosure of the Confidential Information in breach of this Section will cause irreparable harm or injury to Disclosing Party, which is incapable of recompense by way of damages. Accordingly, Recipient agrees that Disclosing Party is entitled to seek injunctive or other appropriate relief to restrain any breach or threatened breach of this Section. The confidentiality obligations of the Parties hereunder shall survive for three (3) years from the termination and/or expiration of this Agreement.

A separate Non-Disclosure Agreement if signed between the two parties will be considered as part of this Agreement.

INTELLECTUAL PROPERTY RIGHT (IPR)

The IPR of the Parties in this agreement shall remain in their respective names. The use of IPR of LSP and/or IPA during the course or extension of this Agreement shall not constitute transfer or shall not be

transferred to the other party. The use of any IPR of either party, by the other, without the prior consent of the other shall therefore be considered as passing off or infringement and the party at default shall be liable for punitive damages, as agreed under arbitration or as decreed by the court of law.

Any employees, directors, agents, consultants, advisors and other third parties who are informed of the IPR and confidential information on a “need to know basis” shall keep the terms of this Agreement in strict confidence.

FORCE MAJEURE

Neither Party shall be liable to the other for any delay or failure in the performance by it of any obligation under this Agreement, to the extent affected or prevented by an event of Force Majeure, provided that the Party that is affected by the Force Majeure shall provide notice thereof to the other Party as soon as practicable, but in any event but not later than seven (7) days after the date on which the affected Party knew or should reasonably have known of the commencement of the event of Force Majeure. The affected Party shall use its reasonable endeavors to mitigate the adverse effects of the Force Majeure event affecting it and shall seek reasonable alternative means for performance of the Work to the extent not affected by the event of Force Majeure. Neither Party shall be entitled to make any claim for fees, costs or expenses incurred as a result of an event of Force Majeure.

TERMINATION:

Either party can terminate the agreement without cause with an advance written notice of at least 90 days

Either party can terminate the agreement subject to the following

The other party to the Agreement is in material breach of the Agreement and does not remedy the breach within 30 days of notice from the other party so to do (if capable of remedy) the other party may terminate the Agreement immediately by notice to the party in breach. The material breach including but not limited to the following.

Either of the Party is found indulging in any illegal activity/any activity(ies) which are not in the national interest security etc

Either of the Party is not adhering to the terms and conditions of this Agreement.

Either of the Party is unable to resolve its liabilities and claims under this Agreement

Either of the Party has disclosed or provided incorrect or false information pertaining to its products, credentials, relationships etc

Either of the Party is no longer interested in pursuing the line of business/area of operations etc

vi Either of the Party infringes the Intellectual Property Rights (“IPR”) of the other Party.

vii Either of the Party misuses/discloses the Confidential Information of the other Party.

If either party becomes bankrupt, dissolved, wound up, or makes any arrangement with its creditors or has a receiver, administrative receiver, liquidator or provisional liquidator appointed over all or any part of its assets or goes into liquidation (whether voluntary or otherwise) save as part of a bona fide reconstruction not involving insolvency or takes or suffers any similar action as a result of its liability to pay its debts or its insolvency it shall promptly so notify the other party in writing providing particulars of the circumstances whereupon the other party may terminate the Agreement immediately by unilateral notice.

EFFECTS OF TERMINATION

Upon the termination of the Agreement for any reason whatsoever at the moment of effective termination:

The LSP will no longer be authorized to access or use the Platform

Either party will return all the Data associated with Latch On module and will notify the other party;

all rights and obligations of IPA or LSP under this Agreement shall terminate, unless otherwise prescribed in the Agreement.

NOTICES:

Any notices and communication hereunder shall be in writing and may be sent by email, facsimile, courier or by registered mail or served personally; to the representative of the respective party and at the address as specified below. Any notice or communication shall be deemed to be given (i) if delivered in person, at the time of and upon delivery; or (ii) if sent by facsimile or by email upon receiving of delivery receipt or non-receipt of non-delivery message (iii) if sent by fully prepaid and properly addressed registered mail or courier, at the expiration of two days after the day of dispatch. In proving service of a notice or communication it shall be sufficient to prove that delivery was made or that the facsimile, email, registered mail or courier was properly addressed and sent.

For IPA

Attention:

Address:

Tel No.

Email Id

For LSP

Attention:

Address:

Tel No.

Email Id:

Either Party may change its addresses for notices and representatives by written notice to the other Party. Any change of address not notified to the other Party shall not be enforceable and opposable with respect to present Agreement and any notification made to the former address shall be deemed to be made to the right address.

NON-SOLICITATION

During the term of this Agreement and for a period of Twelve (12) months thereafter, LSP, IPA and PCS operator shall not hire/employ or make efforts to hire/employ the employees of the other parties, either directly or indirectly.

PRIVACY AND DATA PROTECTION

The Parties hereto confirms and ensures that all the Data and information shared by the Parties or its end users including but not limited to the location of the end user's device when using the Platform/Interface and services, and information regarding the devices, computers and the end users'

use of the Platform/integration services shall remain confidential and shall not be disclosed to any other third party.

DATA RESIDENCY

Both Parties hereby agrees that the Data in relation to the Latch on Modules hosted on servers shall be physically present in India. Either Party shall not transfer the Data hosted on the servers without the prior consent of the other Party.

LIMITED WARRANTY

Each Party warrants to the other Party that it has the right to enter into this Agreement and fully perform all obligations applicable to it hereunder. Both Parties warrants that the products, services and other assistance to be provided will be in accordance with this Agreement and will be performed in accordance with its specifications.

Disclaimer: EXCEPT AS SET FORTH ABOVE IN THIS CLAUSE 0, EACH PARTY DISCLAIMS ANY AND ALL PROMISES, REPRESENTATIONS AND WARRANTIES WITH RESPECT TO ANY DATA, INFORMATION, SERVICES OR OTHER MATERIAL FURNISHED HEREUNDER OR THEREUNDER, INCLUDING MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR THE SUCCESS OF ANY ACTIVITIES CONTEMPLATED BY THIS AGREEMENT.

INFRINGEMENT AND INDEMNIFICATION

Each Party shall defend indemnify and hold other party and its officers, employees, representatives and agents harmless from and against any and all Liabilities arising or brought against or incurred by the other Party and its officers, employees, representatives and agents for (a) any injury to persons (including physical or mental injury, libel, slander and death) caused by wrongful acts and or omissions(or relating to the strict liability) of the indemnifying Party, or its officers, employees, representatives, personnel or agents (“Indemnifiers”); or (b) loss or damage to property, caused by the Indemnifiers (c) any violation or infringement of Intellectual Property Rights.

LIMITATION OF LIABILITY

In no event shall either Party be liable to each other or any third party for any loss of profits, loss of data, or other incidental, special, exemplary, punitive, or consequential damages arising from any provision of this Agreement even if such Party has been advised in advanced of the possibility of such damages or such damages could have been reasonably foreseen by such Party

ASSIGNMENT SUBPCONTRACTING AND NOVATION

This Agreement or any interest herein shall not be transferred or assigned or novated, in whole or in part, by either Party without the prior written consent of the other. LSP can subcontract the performance of Work or LSP’s obligations under this Agreement in whole or in part and shall be solely responsible for the performance and discharge of obligations under this Agreement.

SEVERABILITY

In the event any portion of this Agreement is deemed invalid or unenforceable for any reason by a court of competent jurisdiction or under an applicable law, the remaining portions of this Agreement shall remain in full force and effect.

CHANGES

No modification or amendment to this Agreement shall be binding upon the Parties unless made in writing and signed by duly authorized officials of both Parties.

INDEPENDENT CONTRACTORS

The Parties agree that no relationship of agency, partnership or joint venture is created by this Agreement, express or implied, and that the Parties will each remain independent contractors. No Party will be considered as principal or agent or hold itself as the legal representative of the other Party. No Party shall have the authority to bind or to make any commitment on behalf of the other Party unless such authority is expressed in writing by the Parties jointly or by a Party individually as the case may be.

WAIVER

No failure or delay on the part of either party in the exercise of any right or privilege hereunder shall operate as a waiver thereof or of the exercise of any right or privilege hereunder, nor shall any single or partial exercise of any such right or privilege other or further exercise thereof of any other right or privilege.

DISPUTE RESOLUTION AND ARBITRATION

Should any kind of dispute arise in relation to this Agreement, then the Parties agree to resolve such issues through amicable discussion and negotiation. In the event that any dispute relating to this Agreement cannot be resolved by amicable discussion and negotiation between the parties, the parties shall attempt to resolve all disputes through informal means.

If the Parties fail to settle any dispute, controversy or claim ("the Dispute"), either Party may serve a formal written notice on the other Party that a Dispute has arisen (the "Notice of Dispute"). The Parties shall use all reasonable efforts for a period of thirty (30) days from the date on which the Notice of Dispute is served by one Party on the other Party (or such longer period as may be agreed in writing between the Parties) to resolve the Dispute on an amicable basis. If the Parties are unable to resolve the Dispute by amicable negotiation within the said time period of thirty (30) days (or such longer period as may be agreed in writing between the Parties), the Dispute shall be resolved by way of arbitration as provided below.

Should the Parties fail to settle the Dispute amicably; they shall submit the same for arbitration. The arbitrator hereunder shall be agreed upon and appointed by the parties or in case of disagreement as to the appointment of a single arbitrator, to the appointment of two arbitrators, one to be appointed by each party and if there are two arbitrators, they shall before taking upon themselves the burden of reference appoint an umpire. The arbitration proceedings shall be conducted in accordance with the International Commercial Arbitration Rules, which rules are deemed to be incorporated by reference into this clause. The language for arbitration shall be English and the juridical seat of the arbitration shall be Delhi. The arbitrators' award shall be substantiated in writing and shall be final and binding on the Parties and appealable to the extent permitted under the applicable laws.

GOVERNING LAW AND JURISDICTION

This Agreement and any non-contractual obligations arising out of or in connection with it shall be governed by and construed in accordance with the laws of India. Any dispute, controversy or claim arising out of or relating to this Agreement, or the breach shall be settled in the Courts of Mumbai, India.

ENTIRE AGREEMENT

This Agreement together with its annexures contains the final agreement between the Parties in respect of the subject matter of the Agreement and supersedes and replaces any and all prior Agreements, understandings or arrangements, whether oral or written heretofore made between the Parties and relating to the subject matter hereof and constitutes the entire understanding of the Parties with respect to the subject matter of the Agreement. This Agreement may not be modified, changed, altered or amended except by an express written Agreement signed by all the Parties hereto.

In Witness Whereof, the parties have caused this Agreement to be duly executed by their respective authorized representatives as of the day and year first above written.

For Indian Ports Association	For LSP
Signature:	Signature:
Name:	Name:
Title:	Title:
Date:	Date:
Place:	Place:

Annexure 1– Statement of Work

Annexure 2 - Registration Process for LSP

Annexure 3 - Latch on Integration Technical Framework

8.10 Annexure X

8.10.1 Memorandum of Understanding

This Memorandum of Understanding (MoU) is drawn on the ……day of 2020,

between:

Ministry of Commerce, Government of India, (hereinafter referred to as **"MOC"),** of the **FIRST PART will be acting as 'Nodal Department'** for logistics related aspects **represented by**;

AND

Indian Ports Association , a society registered under the Society Registration Act 1860 having its office at 1st Floor, South Tower, NBCC Place, B P Marg, Lodi Road, New Delhi (hereinafter referred to as "IPA") of the SECONDPART, will be acting project management body, represented by Chairman, IPA/MD, IPA

AND

Ministry of Shipping, Government of India, (herein after referred to as "MOS"), of the THIRDPART will be acting as 'confirming party' represented by …… Ministry of Shipping has entrusted the task of development and implementation of National Logistics Portal – Marine (hereinafter referred to as NLP) to Indian Ports Association.

MOC, MOS and IPA are individually referred to as "**Party**" and collectively as the **"Parties".**

OBJECTIVE

The overall objective of this MoU is to have an understanding between MOC, IPA and MOS to provide service of National Logistics Portal - Marine for a period of five years.

WHEREAS:

IPA has been entrusted by the MOS for setting up a National Logistics Portal - Marine(NLP-M) to improve the Ease of Doing Business (EoDB) in the country for marine trade ecosystem and its stakeholders.

MOS will be acting as 'confirming party'

MOC and IPA agree to subsequently integrate the National Logistics Portal – Marine with the India Logistics Platform (hereinafter referred to as I-Log) after the completion of its development by MOC.

In pursuance of the aforesaid, the Parties hereto wish to record under this Memorandum of Understanding (MoU), the terms of their mutual understanding in order to implement the National Logistics Portal - Marine (NLP).

NOW, THEREFORE, THE PARTIES HERETO AGREE AS UNDER:

ARTICLE 1 SCOPE OF MoU

Ministry of Commerce (MOC) has envisioned establishment of the India Logistics Platform (I-Log) comprising of Marine, Land, Air and E-Commerce Platform for the EXIM Trade as well as Domestic Trade from and to India with a view to increase the Ease of Doing Business quotient in India and increase the Logistics Performance Index (LPI).I-Log will be the first of its kind to provide B2B (Business to Business) and B2G (Business to Government) services. Whereas MOS has entrusted IPA to develop the NLP and implement looking at the success of Port Community System 'PCS 1x" which was implemented in a record time. It was recommended that PCS 1x platform be taken as base to create NLP. PCS 1x has the potential to be developed into the NLP through upgradation and strengthening of the system facilitating other stakeholders of marine trade.

The **Objectives** of the **National Logistics Portal - Marine(NLP-M)** project are:

The Government of India appreciates the need to bring about an integrated development of the Logistics Sector in the country through the I-Log Platform. Accordingly, the second schedule of the Government of India (Allocation of Business) Rules, 1961, was amended on 7th, July 2017, and the subject "Integrated Development of Logistics Sector" was allocated to the Department of Commerce under the Ministry of Commerce & Industry (MOCI).

NLP has been planned to encourage multimodal transport through the creation of a one-stop shop for availing export, import and domestic trade related logistics services related to marine trade ecosystem. Some of the key attributes of NLP inter-alia include:

Route optimization

Statutory certifications and clearances

Trade related compliance assistance

By associating with the National Logistic Portal Marine (NLP-M) and its integration with the I-Log Platform, Logistic Service Providers will be able to, achieve better assets utilization and improve their operational efficiency. The NLP is being set-up with a view to be subsequently integrated with the I-Log platform whenever the latter is ready..

Multi-modal Logistics e-marketplace: This will be a platform to bring together the users and providers of logistic services for marine trade ecosystem. Users can book transport services for export, import of goods using a combination of transport modes to best optimize logistics. These modes shall include trucks, ICDs, shipping lines,. All existing players including aggregators shall be encouraged to integrate with the portal to enable them to gain greater demand visibility.

Integrated Regulatory Platform: By integrating with customs, clearance updates and document sharing shall be provided within the NLP Marine.

Banking and Financial Services: Different aspects of trade finance shall also be integrated with the NLP.

Providing 24x7 efficient and effective response system for customer service and grievance redressal through a Customer Service Organization..

NLP Marine will be having following outcomes and deliverables:

–Maritime trade Logistics stakeholders across the value chain can interact with the users to provide different services. The platform will also have a component for the single window clearance for EXIM certification Simplification & Elimination of Physical Documents –Subsequently, NLP Marine through its integration with the I-Log Platform will also facilitate all certification requirements in a single window, and interact with various agencies to track compliance status. The portal aims to replace physical paperwork and human interventions for information sharing through a clearly defined flow of information.

Efficiency Enhancement and Increased Competition –NLP Marine will digitise many of the offline activities and provide transparent, reliable and competitively priced services Once integrated to ILOG Platform It will lead to the reduction in time and effort for obtaining regulatory clearances. It will simplify the process of discovery of competitive rates for various marine logistics-related services.

Promotion of MSME Sector - Pan India visibility of services and access to prospective users from across the country will provide an opportunity for various MSME sectors and save their cost related to marine logistics.

Improving Transparency – NLP Marine would facilitate increased visibility and access to various Logistics Service Providers from all over the country.

Standardization of Service Quality & Traceability -It will help in standardisation of logistical services, traceability of consignments, background verification of service providers and their rating. NLP-M will also provide In-transit tracking of consignments.

The Implementation strategy of this project has the following salient features:

NLP Marine will be implemented in coordination with stakeholders.

Appropriate Governance mechanism would be created to enable successful implementation.

In order to ensure the accountability and performance from IT service provider (ITSP), service levels are built in the contract and appropriate penalties would also be levied. Single IT service provider would be engaged to implement the project nationwide.

IT service provider will supply, commission, implement the IT components as per contract conditions in consultation with IPA, take the inputs of the stakeholders and will also provide the IT manpower for operation and maintenance of the system.

ITSP would cater to the needs of the stakeholders while customizing the system for its deployment.

In order to ensure accountability of ITSP in implementation of NLP Marine, release of payments is linked to their successful implementation of the system, Go-Live performance, which is measured by timely completion of milestones, adherence to pre-defined Service Level Agreements (SLA) and the performance of the system.

ARTICLE 2

GOVERNANCE OF NLP Marine PROJECT

MOS, MOC and IPA agree to have a multi-tier governance structure for guidance, supervision and management of day-to-day operations of NLP implementation. NLP Governance Structure would be in conformance with guidelines provided by MOC, MOS & IPA.

The Governance Structure would include an "**Apex Committee**" with Joint Secretary (Shipping), Joint Secretary (Logistics) and Chairman, IPA.

A "**Steering Committee**" Chaired by the MD, IPA and "**Domain Experts**".

Joint Working Group (JWG) will be constituted to coordinate activities for the integrated development of NLP and its soft-launch initially for handling government cargos. The role of JWG would be co-ordination, integration and technical Inputs. JWG will consist of representatives from Ministry of Commerce & Industry, Ministry of Civil Aviation, Ministry of Road Transport & Highways, Ministry of Railways, CONCOR, Ministry of Shipping and Customs.

Technical team will be constituted for review of the processes, standardization and Harmonization with IT experts and domain experts from the trade, IPA, MOC, MOS and respective government agencies.

IPA agrees to constitute the afore-mentioned committees. The details of the proposed structure of the committees will be provided in the guidelines of NLP.

ARTICLE 3

RESPONSIBILITIES OF MOC

Logistics division of the Department of Commerce has proposed to develop the India Logistics Platform (I-Log Platform) to integrate and broad base the availability of logistics services with the overall objective of reducing logistics cost. Four key online modules of the portal have been envisaged – logistics services, certificate system, regulatory clearance and financial services.

Logistics division shall extend all necessary support to IPA towards the integration of PGAs and other stake holders in the shipping domain. with the NLP Marine.

.

Extend support to secure participation of State/UT Governments and other stakeholders, as necessary.

MOC will work with MOS and IPA to develop and to strengthen the framework

ARTICLE 4

RESPONSIBILITIES OF IPA

IPA will hold the responsibilities for the successful and time bound implementation of NLP MAarine. IPA commits itself, agrees and assures to discharge the following responsibilities effectively by allocating the required manpower and resources and by taking appropriate policy and operational decisions in furtherance thereof.

Formation of Governance Structure as per guidelines provided by the MOC within 15 days of the signing of the MoU.

Provide for continuity of officials involved in the implementation of the project

Implementation of the project in a time bound manner and with accountability

Provide physical infrastructure like physical space, furniture, amenities etc.

Take up awareness campaign with the national campaign with respect to this system

Provide support in monitoring the entire system

Provide suggestions and support to integrate the NLP with other departments and services based on the inputs, suggestions, feedback received from MoC and MoS.

Monitoring and Evaluation of the program

Defining Standard Operating Procedure (SOP) for the operation of the NLP Marine in consultation with MOC

Agreeing to the technical architecture of hosting the data on MietY approved cloud central system.

Development of overall strategy for achieving the objectives of the NLP Marine and overseeing implementation.

Constituting institutional structures, as modified/agreed from time to time for speedy decision-making, monitoring and review.

To operationalize various components of NLP viz. LeM , LCP , IRF , financials , following key activities are proposed to be taken up by IPA in consultation with MoC.

Define the strategic road map for the NLP and be responsible for its overall implementation and functioning including development, operations maintenance along with marketing and on boarding of vendors / stakeholders.

Approve and sanction the projects including their technical appraisal.

Execute the development of NLP- Marine with complete operational freedom.

Take measures to comply with the requirements of Ministry of Commerce & Industry concerning the implementation and operation of NLP - Marine.

Take suitable measures for mobilization of resources within timelines for self-sustenance through internal revenue generation and promoting investments.

Approve and act upon the reports of a third party Review and Monitoring Agency

Overview Capacity Building activities, assess the need for upgradation and adapt to the market requirements.

Develop and benefit from inter-linkages with academic institutions and organizations.

Ensure timely completion of projects according to set timelines.

Undertake review of activities of the NLP - Marine including budgetary provisions for implementation of the project.

Monitor and review quality control related matters and act upon issues arising thereof.

Enter into contracts, partnerships and service delivery arrangements as may be required for the implementation and operations of the NLP - Marine.

Determine and collect user charges, subscription fee, transaction fee, etc.

Manage all services related to the management of the portal such as marketing & branding, IEC Management, service provider verification system, call-center services for the grievance management, and services to promote and adoption of the portal by service providers and traders, etc.

IPA shall be functioning to develop, operate and maintain the NLP throughout the life cycle of the NLP

Guidance to State/UT and other agencies.

Engagement of an agency as Program Management Unit (PMU) to effectively coordinate and support implementation of NLP project.

Providing overall implementation guidelines and support & assist in planning and implementing the NLP.

Planning and monitoring the nationwide implementation of the NLP.

Undertaking regular forecasting exercise in consultation with IPA to assess the progress and plan for future requirement.

Conforming to the implementation guidelines provided by the MOC as well as subsequent guidelines, in the interest of the successful implementation of the NLP.

Ensuring quality of service through regular monitoring and audit.

Ensuring the continuity of the Nodal officer appointed for handling the NLP and his team for a reasonable tenure for better delivery of services to the people in distress.

Providing access as and when required, for a third party audit into the NLP project. This audit may include people, processes and technology. IPA would submit action plan on the audit findings and periodic action taken report on the same to the MOC.

Providing time to time status report and intimation to the MOC

ARTICLE 5

MISCELLANEOUS

No amendments to the MoU shall be valid unless executed in writing and signed by all the parties.

To begin with, only NLP Marine services are to be provided. However other services may get integrated in this project later. MOC and IPA will work together for integration of other services as per mutually agreed timelines.

The Parties would follow the implementation guidelines issued by the MOC/MoS. These guidelines may be changed in consultation between the Parties.

VALIDITY OF MOU

This MoU will be valid initially for a period of Five Years . However, it is expected to be further extended with mutual consent of all the parties, in order to ensure continuous development, integration and refinement of the tools and modelling frameworks being used to support robust and in-depth national level planning and strategy formulation.

TERMINATION

This MoU may be terminated by either party by serving three months' written notice to the other parties.

ARBITRATION

All disputes arising between the parties in any way connected with this agreement or in regard to the interpretation of the context hereof shall be served by mutual consent failing which the same would be referred at the option of either party. Arbitrator mutually agreed upon and in default of such mutual agreement, to the arbitration of two arbitrators one to be nominated by MOC and the other by the IPA. In such a case the provisions of the Arbitration Act, 1996 or any other statutes, modification therein shall apply. The place of Jurisdiction will be New Delhi. The award of the arbitrators shall be final and binding upon the parties.

IN WITNESS WHEREOF the Parties hereto have carefully gone through the contents of this Memorandum of Understanding (MoU) and have signed and put their seals and agreed to abide by the terms and conditions as laid down therein in totality as of the day and year first above written.

Signatories

For Ministry of Commerce

For Ministry of Shipping

For Indian Ports Association

Witness

1. ……

2. ……...

3. ……...

Left Blank