PHILIPPINE PORTS AUTHORITY

PROCUREMENT OF TRUSTED OPERATOR PROGRAM – CONTAINER REGISTRY MONITORING SYSTEM (TOP-CRMS) & EMPTY CONTAINER STORAGE SHARED SERVICE FACILITY DESIGN SPECIFICATIONS AND IMPLEMENTATION

BID DOCS
BAC-PGCS-023-2022

Table of Contents

Glossary of Acronyms, Terms, and Abbreviations

ABC – Approved Budget for the Contract.

BAC – Bids and Awards Committee.

Bid – A signed offer or proposal to undertake a contract submitted by a bidder in response to and in consonance with the requirements of the bidding documents. Also referred to as *Proposal* and *Tender*. (2016 revised IRR, Section 5[c])

Bidder – Refers to a contractor, manufacturer, supplier, distributor and/or consultant who submits a bid in response to the requirements of the Bidding Documents. (2016 revised IRR, Section 5[d])

Bidding Documents – The documents issued by the Procuring Entity as the bases for bids, furnishing all information necessary for a prospective bidder to prepare a bid for the Goods, Infrastructure Projects, and/or Consulting Services required by the Procuring Entity. (2016 revised IRR, Section 5[e])

BIR – Bureau of Internal Revenue.

BSP – Bangko Sentral ng Pilipinas.

Consulting Services – Refer to services for Infrastructure Projects and other types of projects or activities of the GOP requiring adequate external technical and professional expertise that are beyond the capability and/or capacity of the GOP to undertake such as, but not limited to: (i) advisory and review services; (ii) pre-investment or feasibility studies; (iii) design; (iv) construction supervision; (v) management and related services; and (vi) other technical services or special studies. (2016 revised IRR, Section 5[i])

CDA - Cooperative Development Authority.

Contract – Refers to the agreement entered into between the Procuring Entity and the Supplier or Manufacturer or Distributor or Service Provider for procurement of Goods and Services; Contractor for Procurement of Infrastructure Projects; or Consultant or Consulting Firm for Procurement of Consulting Services; as the case may be, as recorded in the Contract Form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.

CIF – Cost Insurance and Freight.

CIP – Carriage and Insurance Paid.

CPI – Consumer Price Index.

DDP – Refers to the quoted price of the Goods, which means "delivered duty paid."

DTI – Department of Trade and Industry.

EXW – Ex works.

FCA – "Free Carrier" shipping point.

FOB – "Free on Board" shipping point.

Foreign-funded Procurement or Foreign-Assisted Project– Refers to procurement whose funding source is from a foreign government, foreign or international financing institution as specified in the Treaty or International or Executive Agreement. (2016 revised IRR, Section 5[b]).

Framework Agreement – Refers to a written agreement between a procuring entity and a supplier or service provider that identifies the terms and conditions, under which specific purchases, otherwise known as "Call-Offs," are made for the duration of the agreement. It is in the nature of an option contract between the procuring entity and the bidder(s) granting the procuring entity the option to either place an order for any of the goods or services identified in the Framework Agreement List or not buy at all, within a minimum period of one (1) year to a maximum period of three (3) years. (GPPB Resolution No. 27-2019)

GFI – Government Financial Institution.

GOCC – Government-owned and/or –controlled corporation.

Goods – Refer to all items, supplies, materials and general support services, except Consulting Services and Infrastructure Projects, which may be needed in the transaction of public businesses or in the pursuit of any government undertaking, project or activity, whether in the nature of equipment, furniture, stationery, materials for construction, or personal property of any kind, including non-personal or contractual services such as the repair and maintenance of equipment and furniture, as well as trucking, hauling, janitorial, security, and related or analogous services, as well as procurement of materials and supplies provided by the Procuring Entity for such services. The term "related" or "analogous services" shall include, but is not limited to, lease or purchase of office space, media advertisements, health maintenance services, and other services essential to the operation of the Procuring Entity. (2016 revised IRR, Section 5[r])

GOP – Government of the Philippines.

GPPB – Government Procurement Policy Board.

INCOTERMS – International Commercial Terms.

Infrastructure Projects – Include the construction, improvement, rehabilitation, demolition, repair, restoration or maintenance of roads and bridges, railways, airports, seaports, communication facilities, civil works components of information technology projects, irrigation, flood control and drainage, water supply, sanitation, sewerage and solid waste management systems, shore protection, energy/power and electrification facilities, national buildings, school buildings, hospital buildings, and other related construction projects of the government. Also referred to as *civil works or works*. (2016 revised IRR, Section 5[u])

LGUs – Local Government Units.

NFCC – Net Financial Contracting Capacity.

NGA – National Government Agency.

PhilGEPS - Philippine Government Electronic Procurement System.

Procurement Project – refers to a specific or identified procurement covering goods, infrastructure project or consulting services. A Procurement Project shall be described, detailed, and scheduled in the Project Procurement Management Plan prepared by the agency which shall be consolidated in the procuring entity's Annual Procurement Plan. (GPPB Circular No. 06-2019 dated 17 July 2019)

PSA – Philippine Statistics Authority.

SEC – Securities and Exchange Commission.

SLCC – Single Largest Completed Contract.

Supplier – refers to a citizen, or any corporate body or commercial company duly organized and registered under the laws where it is established, habitually established in business and engaged in the manufacture or sale of the merchandise or performance of the general services covered by his bid. (Item 3.8 of GPPB Resolution No. 13-2019, dated 23 May 2019). Supplier as used in these Bidding Documents may likewise refer to a distributor, manufacturer, contractor, or consultant.

UN – United Nations.

PHILIPPINE PORTS AUTHORITY

INVITATION TO BID

FOR THE PROCUREMENT OF TRUSTED OPERATOR PROGRAM – CONTAINER REGISTRY MONITORING SYSTEM (TOP-CRMS) & EMPTY CONTAINER STORAGE SHARED SERVICE FACILITY DESIGN SPECIFICATIONS AND IMPLEMENTATION

The Philippine Ports Authority, through the Corporate Budget of the Authority for CY 2022, intends to apply the sum of **P980,000,000.00** being the Approved Budget for the Contract (ABC) to payments under the contract for the Procurement of Trusted Operator Program – Container Registry Monitoring System (TOP-CRMS) & Empty Container Storage Shared Service Facility Design Specifications and Implementation (BAC PGCS-023-2022) (Early Procurement). Bids received in excess of the ABC shall be automatically rejected at bid opening.

The Philippine Ports Authority now invites bids for the above Procurement Project. Completion of the services for the Technical Implementation Phase shall not exceed Twelve (12) Months from receipt by the successful bidder of the Notice to Proceed, while for the Managed Services, One (1) year from date of the go-live or operationalization commissioning of the Technical Implementation Phase. Bidders should have completed, within seven (7) years from the date of submission and receipt of bids, a contract similar to the Project. The description of an eligible bidder is contained in the Bidding Documents, particularly, in Section II (Instructions to Bidders).

Bidding will be conducted through open competitive bidding procedures using a non-discretionary "pass/fail" criterion as specified in the 2016 Revised Implementing Rules and Regulations (IRR) of Republic Act (RA) 9184. Bidding is restricted to Filipino citizens/sole proprietorships, partnerships, or organizations with at least sixty percent (60%) interest or outstanding capital stock belonging to citizens of the Philippines, and to citizens or organizations of a country the laws or regulations of which grant similar rights or privileges to Filipino citizens, pursuant to RA 5183.

Prospective Bidders may obtain further information from the Philippine Ports Authority Bids and Awards Committee (BAC) and inspect the Bidding Documents at the address given below during 8:00 a.m. to 5:00 p.m., Monday to Friday.

A complete set of Bidding Documents may be acquired by interested Bidders on **25 February 2022** from the given address and website(s) below and upon payment of the applicable fee for the Bidding Documents, pursuant to the latest Guidelines issued by the GPPB, in the amount of **Seventy Five Thousand (P75,000.00) Pesos.** The Procuring Entity shall allow the bidder to present its proof of payment for the fees in person.

A. Bonifacio Drive, South Harbor, Port Area, Manila 1018 Philippines
P.O. Box 436 Manila, Philippines
Tel. No. (+632) 527-8356 to 83 Fax No. (+632) 527-4855
website: www.ppa.com.ph

The Philippine Ports Authority's Bids and Awards Committee will hold a Pre-Bid Conference on **08 March 2022 at 2:00 p.m.** at the PPA Function Room, 7th Floor, PPA Bldg., Bonifacio Drive, South Harbor, Port Area, Manila, and/or through video conferencing or webcasting via zoom, which shall be open to all prospective bidders.

Bids must be duly received by the BAC Secretariat through manual submission at the office address indicated below on or before **22 March 2022 at 9:00 a.m.** Late bids shall not be accepted.

All Bids must be accompanied by a bid security in any of the acceptable forms and in the amount stated in ITB Clause 14.

Bid opening shall be on **22 March 2022 at 10:00 a.m.** at the 7th Floor, PPA Building, A. Bonifacio Drive, South Harbor, Port Area, Manila. Bids will be opened in the presence of the bidders' representatives who choose to attend the activity.

The Philippine Ports Authority reserves the right to reject any and all bids, declare a failure of bidding, or not award the contract at any time prior to contract award in accordance with Sections 35.6 and 41 of the 2016 revised IRR of RA No. 9184, without thereby incurring any liability to the affected bidder or bidders.

For further information, please refer to:

BAC Secretariat, Philippine Ports Authority
5th Floor, PPA Bldg., A. Bonifacio Drive,
South Harbor, Port Area, Manila
Telephone Nos. 527-47-35
527-83-56 to 83 loc. 539
PPA Website: www.ppa.com.ph
GPPB Website: www.gppb.com.ph

MARK JON S. PALOMAR
Chairperson, PPA Head Office Bids and Awards
Committee for the Procurement of Goods and
Consultancy Services (HO-BAC-PGCS)

Section II. Instructions to Bidders

1. Scope of Bid

The Procuring Entity, PHILIPPINE PORTS AUTHORITY wishes to receive Bids for the **Procurement of Trusted Operator Program – Container Registry Monitoring System (TOP-CRMS) & Empty Container Storage Shared Service Facility Design Specifications and Implementation**, with identification number **BAC-PGCS-023-2022**.

The Procurement Project (referred to herein as "Project") is composed of a single lot, the details of which are described in Section VII (Technical Specifications).

2. Funding Information

2.1. The Philippine Ports Authority through its corporate budget for the Calendar Year (CY) 2022 in the amount of **NINE HUNDRED EIGHTY MILLION PESOS (Php980,000,000.00)**.

2.2. The source of funding is the Corporate Budget of the PHILIPPINE PORTS AUTHORITY.

3. Bidding Requirements

The Bidding for the Project shall be governed by all the provisions of RA No. 9184 and its 2016 revised IRR, including its Generic Procurement Manuals and associated policies, rules and regulations as the primary source thereof, while the herein clauses shall serve as the secondary source thereof.

Any amendments made to the IRR and other GPPB issuances shall be applicable only to the ongoing posting, advertisement, or **IB** by the BAC through the issuance of a supplemental or bid bulletin.

The Bidder, by the act of submitting its Bid, shall be deemed to have verified and accepted the general requirements of this Project, including other factors that may affect the cost, duration and execution or implementation of the contract, project, or work and examine all instructions, forms, terms, and project requirements in the Bidding Documents.

4. Corrupt, Fraudulent, Collusive, and Coercive Practices

The Procuring Entity, as well as the Bidders and Suppliers, shall observe the highest standard of ethics during the procurement and execution of the contract. They or through an agent shall not engage in corrupt, fraudulent, collusive, coercive, and obstructive practices defined under Annex "I" of the 2016 revised IRR of RA No. 9184 or other integrity violations in competing for the Project.

5. Eligible Bidders

5.1. Only Bids of Bidders found to be legally, technically, and financially capable will be evaluated.

5.2 Foreign ownership limited to those allowed under the rules may participate in this Project.

5.3. Pursuant to Section 23.4.1.3 of the 2016 revised IRR of RA No.9184, the Bidder shall have an SLCC that is at least one (1) contract similar to the Project the value of which, adjusted to current prices using the PSA's CPI, must be at least equivalent to at least fifty percent (50%) of the ABC.

5.4. The Bidders shall comply with the eligibility criteria under Section 23.4.1 of the 2016 IRR of RA No. 9184.

6. Origin of Goods

There is no restriction on the origin of goods other than those prohibited by a decision of the UN Security Council taken under Chapter VII of the Charter of the UN, subject to Domestic Preference requirements under **ITB** Clause 18.

7. Subcontracts

7.1 The Bidder may subcontract portions of the Project to the extent allowed by the Procuring Entity as stated herein, but in no case more than twenty percent (20%) of the Project.

The Procuring Entity has prescribed that:

Subcontracting is not allowed.

8. Pre-Bid Conference

The Procuring Entity will hold a Pre-Bid conference for this Project on the specified date and time and either at its physical address at the PPA Function Room, 7th Floor, PPA Building, Bonifacio Drive, South Harbor, Port Area, Manila and/or through videoconferencing/webcasting as indicated in paragraph 6 of the **IB.**

9. Clarification and Amendment of Bidding Documents

Prospective bidders may request for clarification on and/or interpretation of any part of the Bidding Documents. Such requests must be in writing and received by the Procuring Entity, either at its given address or through electronic mail indicated in the **IB**, at least ten (10) calendar days before the deadline set for the submission and receipt of Bids.

10. Documents comprising the Bid: Eligibility and Technical Components

10.1. The first envelope shall contain the eligibility and technical documents of the Bid as specified in **Section VIII (Checklist of Technical and Financial Documents)**.

10.2. The Bidder's SLCC as indicated in **ITB** Clause 5.3 should have been completed within seven (7) years prior to the deadline for the submission and receipt of bids.

10.3. If the eligibility requirements or statements, the bids, and all other documents for submission to the BAC are in foreign language other than English, it must be accompanied by a translation in English, which shall be authenticated by the appropriate Philippine foreign service establishment, post, or the equivalent office having jurisdiction over the foreign bidder's affairs in the Philippines. Similar to the required authentication above, for Contracting Parties to the Apostille Convention, only the translated documents shall be authenticated through an apostille pursuant to GPPB Resolution No. 13-2019 dated 23 May 2019. The English translation shall govern, for purposes of interpretation of the bid.

11. Documents comprising the Bid: Financial Component

11.1. The second bid envelope shall contain the financial documents for the Bid as specified in **Section VIII (Checklist of Technical and Financial Documents)**.

11.2. If the Bidder claims preference as a Domestic Bidder or Domestic Entity, a certification issued by DTI shall be provided by the Bidder in accordance with Section 43.1.3 of the 2016 revised IRR of RA No. 9184.

11.3. Any bid exceeding the ABC indicated in paragraph 1 of the **IB** shall not be accepted.

11.4. For Foreign-funded Procurement, a ceiling may be applied to bid prices provided the conditions are met under Section 31.2 of the 2016 revised IRR of RA No. 9184.

12. Bid Prices

12.1. Prices indicated on the Price Schedule shall be entered separately in the following manner:

a. For Goods offered from within the Procuring Entity's country:

i. The price of the Goods quoted EXW (ex-works, ex-factory, ex-warehouse, ex-showroom, or off-the-shelf, as applicable);

ii. The cost of all customs duties and sales and other taxes already paid or payable;

iii. The cost of transportation, insurance, and other costs incidental to delivery of the Goods to their final destination; and

iv. The price of other (incidental) services, if any, listed in e.

b. For Goods offered from abroad:

i. Unless otherwise stated in the **BDS**, the price of the Goods shall be quoted delivered duty paid (DDP) with the place of destination in the Philippines as specified in the **BDS**. In quoting the price, the Bidder shall be free to use transportation through carriers registered in any eligible country. Similarly, the Bidder may obtain insurance services from any eligible source country.

ii. The price of other (incidental) services, if any, as listed in **Section VII (Technical Specifications).**

13. Bid and Payment Currencies

13.1. For Goods that the Bidder will supply from outside the Philippines, the bid prices may be quoted in the local currency or tradeable currency accepted by the BSP at the discretion of the Bidder. However, for purposes of bid evaluation, Bids denominated in foreign currencies, shall be converted to Philippine currency based on the exchange rate as published in the BSP reference rate bulletin on the day of the bid opening.

13.2. Payment of the contract price shall be made in Philippine Pesos.

14. Bid Security

14.1. The Bidder shall submit a Bid Securing Declaration or any form of Bid Security in the amount indicated in the **BDS**, which shall be not less than the percentage of the ABC in accordance with the schedule in the **BDS**.

14.2. The Bid and bid security shall be valid for One Hundred Twenty (120) calendar days from the date of the opening of bids. Any Bid not accompanied by an acceptable bid security shall be rejected by the Procuring Entity as non-responsive.

15. Sealing and Marking of Bids

Each bidder shall submit one copy of the first and second components of the Bid.

The Procuring Entity may request additional hard copies and/or electronic copies of the Bid. However, failure of the Bidders to comply with the said request shall not be a ground for disqualification.

If the Procuring Entity allows the submission of bids through online submission or any other electronic means, the Bidder shall submit an electronic copy of its Bid, which must be digitally signed. An electronic copy that cannot be opened or is corrupted shall be considered non-responsive and, thus, automatically disqualified.

16. Deadline for Submission of Bids

16.1. The Bidders shall submit on the specified date and time and either at its physical address or through online submission as indicated in paragraph 7 of the **IB.**

17. Opening and Preliminary Examination of Bids

17.1. The BAC shall open the Bids in public at the time, on the date, and at the place specified in paragraph 9 of the **IB**. The Bidders' representatives who are present shall sign a register evidencing their attendance. In case videoconferencing, webcasting or other similar technologies will be used, attendance of participants shall likewise be recorded by the BAC Secretariat.

In case the Bids cannot be opened as scheduled due to justifiable reasons, the rescheduling requirements under Section 29 of the 2016 revised IRR of RA No. 9184 shall prevail.

17.2. The preliminary examination of bids shall be governed by Section 30 of the 2016 revised IRR of RA No. 9184.

18. Domestic Preference

18.1. The Procuring Entity will grant a margin of preference for the purpose of comparison of Bids in accordance with Section 43.1.2 of the 2016 revised IRR of RA No. 9184.

19. Detailed Evaluation and Comparison of Bids

19.1. The Procuring BAC shall immediately conduct a detailed evaluation of all Bids rated "*passed*," using non-discretionary pass/fail criteria. The BAC shall consider the conditions in the evaluation of Bids under Section 32.2 of the 2016 revised IRR of RA No. 9184.

19.2. If the Project allows partial bids, bidders may submit a proposal on any of the lots or items, and evaluation will be undertaken on a per lot or item basis, as the case maybe. In this case, the Bid Security as required by **ITB** Clause 15 shall be submitted for each lot or item separately.

19.3. The descriptions of the lots or items shall be indicated in **Section VII (Technical Specifications)**, although the ABCs of these lots or items are indicated in the **BDS** for purposes of the NFCC computation pursuant to Section 23.4.2.6 of the 2016 revised IRR of RA No. 9184. The NFCC must be sufficient for the total of the ABCs for all the lots or items participated in by the prospective Bidder.

19.4. The Project shall be awarded as one Project having several items that shall be awarded as one contract.

19.5. Except for bidders submitting a committed Line of Credit from a Universal or Commercial Bank in lieu of its NFCC computation, all Bids must include the NFCC computation pursuant to Section 23.4.1.4 of the 2016 revised IRR of RA No. 9184, which must be sufficient for the total of the ABCs for all the lots or items participated in by the prospective Bidder. For bidders submitting the

committed Line of Credit, it must be at least equal to ten percent (10%) of the ABCs for all the lots or items participated in by the prospective Bidder.

20. Post-Qualification

20.1. Within a non-extendible period of five (5) calendar days from receipt by the Bidder of the notice from the BAC that it submitted the Lowest Calculated Bid, the Bidder shall submit its latest income and business tax returns filed and paid through the BIR Electronic Filing and Payment System (eFPS) and other appropriate licenses and permits required by law and stated in the **BDS**.

21. Signing of the Contract

21.1. The documents required in Section 37.2 of the 2016 revised IRR of RA No. 9184 shall form part of the Contract. Additional Contract documents are indicated in the **BDS**.

Bid Data Sheet

ITB Clause	
5.3	For this purpose, contracts similar to the Project shall be: a. Contract that involves designing, implementing, deploying, and operating the managed services of a comprehensive managed services operations and technology solution for a government agency or private company that includes transactional applications that produce official issuances or provide location and identification management, issuance of permits, tickets, identification card processing, identification matching, KYC, or implementing and monitoring location-locked systems, machines, or devices b. completed within seven (7) years prior to the deadline for the submission and receipt of bids.
7.1	Subcontracting is not allowed.
12	The price of the Goods shall be quoted DDP *[Manila]* or the applicable International Commercial Terms (INCOTERMS) for this Project.
14.1	The bid security shall be in the form of a Bid Securing Declaration, or any of the following forms and amounts: a. The amount of not less than Nineteen Million Six Hundred Thousand Pesos (Php19,600,000.00), if bid security is in cash, cashier's/manager's check, bank draft/guarantee or irrevocable letter of credit; or b. The amount of not less than Forty Nine Million Pesos (Php49,000,000.00) if bid security is in Surety Bond.
15	Each Bidder shall submit **ONE (1) original and SIX (6) copies** of its Technical and Financial Components of its Bid in two (2) separate sealed bid envelopes, which should be submitted simultaneously. Each of the bid documents should be individually sealed. All bid documents shall be book-bound with hard cover and properly labelled with index tabs. Failure to comply with the said requirements is a ground for automatic disqualification of the bidder.
19.3	Partial bid is not allowed. The goods are grouped in a single lot and the lot shall not be divided into sub-lots for the purpose of bidding, evaluation, and contract award.
20.1	No additional requirements.
21.1	No additional requirements.

Section IV. General Conditions of Contract

1. Scope of Contract

This Contract shall include all such items, although not specifically mentioned, that can be reasonably inferred as being required for its completion as if such items were expressly mentioned herein. All the provisions of RA No. 9184 and its 2016 revised IRR, including the Generic Procurement Manual, and associated issuances, constitute the primary source for the terms and conditions of the Contract, and thus, applicable in contract implementation. Herein clauses shall serve as the secondary source for the terms and conditions of the Contract.

This is without prejudice to Sections 74.1 and 74.2 of the 2016 revised IRR of RA No. 9184 allowing the GPPB to amend the IRR, which shall be applied to all procurement activities, the advertisement, posting, or invitation of which were issued after the effectivity of the said amendment.

Additional requirements for the completion of this Contract shall be provided in the **Special Conditions of Contract (SCC).**

2. Advance Payment and Terms of Payment

2.1. Advance payment of the contract amount is provided under Annex "D" of the revised 2016 IRR of RA No. 9184.

2.2. The Procuring Entity is allowed to determine the terms of payment on the partial or staggered delivery of the Goods procured, provided such partial payment shall correspond to the value of the goods delivered and accepted in accordance with prevailing accounting and auditing rules and regulations. The terms of payment are indicated in the **SCC**.

3. Performance Security

Within ten (10) calendar days from receipt of the Notice of Award by the Bidder from the Procuring Entity but in no case later than prior to the signing of the Contract by both parties, the successful Bidder shall furnish the performance security in any of the forms prescribed in Section 39 of the 2016 revised IRR of RA No. 9184.

4. Inspection and Tests

The Procuring Entity or its representative shall have the right to inspect and/or to test the Goods to confirm their conformity to the Project specifications at no extra cost to the Procuring Entity in accordance with the Generic Procurement Manual. In addition to tests in the SCC, **Section IV (Technical Specifications)** shall specify what inspections and/or tests the Procuring Entity requires, and where they are to be conducted. The Procuring Entity shall notify the Supplier in writing, in a timely manner, of the identity of any representatives retained for these purposes.

All reasonable facilities and assistance for the inspection and testing of Goods, including access to drawings and production data, shall be provided by the Supplier to the authorized inspectors at no charge to the Procuring Entity.

5. Warranty

6.1. In order to assure that manufacturing defects shall be corrected by the Supplier, a warranty shall be required from the Supplier as provided under Section 62.1 of the 2016 revised IRR of RA No. 9184.

6.2. The Procuring Entity shall promptly notify the Supplier in writing of any claims arising under this warranty. Upon receipt of such notice, the Supplier shall, repair or replace the defective Goods or parts thereof without cost to the Procuring Entity, pursuant to the Generic Procurement Manual.

6. Liability of the Supplier

The Supplier's liability under this Contract shall be as provided by the laws of the Republic of the Philippines.

If the Supplier is a joint venture, all partners to the joint venture shall be jointly and severally liable to the Procuring Entity

Section V. Special Conditions of Contract

Special Conditions of Contract

GCC Clause	
1	**Delivery and Documents –** For purposes of the Contract, "EXW," "FOB," "FCA," "CIF," "CIP," "DDP" and other trade terms used to describe the obligations of the parties shall have the meanings assigned to them by the current edition of INCOTERMS published by the International Chamber of Commerce, Paris. The Delivery terms of this Contract shall be as follows: *[For Goods supplied from abroad, state:]* "The delivery terms applicable to the Contract are DDP delivered [*indicate place of destination*]. In accordance with INCOTERMS." *For Goods supplied from within the Philippines, state:*] "The delivery terms applicable to this Contract are delivered *[indicate place of destination].* Risk and title will pass from the Supplier to the Procuring Entity upon receipt and final acceptance of the Goods at their final destination." Delivery of the Goods shall be made by the Supplier in accordance with the terms specified in Section VI (Schedule of Requirements). For purposes of this Clause the Procuring Entity's Representative at the Project Site is **Philippine Ports Authority Head Office, Manila**. **Incidental Services –** The Supplier is required to provide all of the following services, including additional services, if any, specified in Section VI. Schedule of Requirements: a. performance or supervision of on-site assembly and/or start-up of the supplied Goods; b. furnishing of tools required for assembly and/or maintenance of the supplied Goods; c. furnishing of a detailed operations and maintenance manual for each appropriate unit of the supplied Goods; and d. performance or supervision or maintenance and/or repair of the supplied Goods, for a period of time agreed by the parties, provided that this service shall not relieve the Supplier of any warranty obligations under this Contract. The Contract price for the Goods shall include the prices charged by the Supplier for incidental services and shall not exceed the prevailing rates charged to other parties by the Supplier for similar services. **Spare Parts –**

The Supplier is required to provide all of the following materials, notifications, and information pertaining to spare parts manufactured or distributed by the Supplier:

a. such spare parts as the Procuring Entity may elect to purchase from the Supplier, provided that this election shall not relieve the Supplier of any warranty obligations under this Contract; and

b. in the event of termination of production of the spare parts:

   i. advance notification to the Procuring Entity of the pending termination, in sufficient time to permit the Procuring Entity to procure needed requirements; and
   ii. following such termination, furnishing at no cost to the Procuring Entity, the blueprints, drawings, and specifications of the spare parts, if requested.

The spare parts and other components required are listed in **Section VI (Schedule of Requirements)** and the cost thereof are included in the contract price.

The Supplier shall carry sufficient inventories to assure ex-stock supply of consumable spare parts or components for the Goods for a period of ten (10) years after the last day of manufacturing of the specific model.

Spare parts or components shall be supplied as promptly as possible, but in any case, within two (2) months of placing the order.

Packaging –

The Supplier shall provide such packaging of the Goods as is required to prevent their damage or deterioration during transit to their final destination, as indicated in this Contract. The packaging shall be sufficient to withstand, without limitation, rough handling during transit and exposure to extreme temperatures, salt and precipitation during transit, and open storage. Packaging case size and weights shall take into consideration, where appropriate, the remoteness of the Goods' final destination and the absence of heavy handling facilities at all points in transit.

The packaging, marking, and documentation within and outside the packages shall comply strictly with such special requirements as shall be expressly provided for in the Contract, including additional requirements, if any, specified below, and in any subsequent instructions ordered by the Procuring Entity.

The outer packaging must be clearly marked on at least four (4) sides as follows:

Name of the Procuring Entity
Name of the Supplier
Contract Description
Final Destination

	Gross weight Any special lifting instructions Any special handling instructions Any relevant HAZCHEM classifications A packaging list identifying the contents and quantities of the package is to be placed on an accessible point of the outer packaging if practical. If not practical the packaging list is to be placed inside the outer packaging but outside the secondary packaging. **Transportation –** Where the Supplier is required under Contract to deliver the Goods CIF, CIP, or DDP, transport of the Goods to the port of destination or such other named place of destination in the Philippines, as shall be specified in this Contract, shall be arranged and paid for by the Supplier, and the cost thereof shall be included in the Contract Price. Where the Supplier is required under this Contract to transport the Goods to a specified place of destination within the Philippines, defined as the Project Site, transport to such place of destination in the Philippines, including insurance and storage, as shall be specified in this Contract, shall be arranged by the Supplier, and related costs shall be included in the contract price. Where the Supplier is required under Contract to deliver the Goods CIF, CIP or DDP, Goods are to be transported on carriers of Philippine registry. In the event that no carrier of Philippine registry is available, Goods may be shipped by a carrier which is not of Philippine registry provided that the Supplier obtains and presents to the Procuring Entity certification to this effect from the nearest Philippine consulate to the port of dispatch. In the event that carriers of Philippine registry are available but their schedule delays the Supplier in its performance of this Contract the period from when the Goods were first ready for shipment and the actual date of shipment the period of delay will be considered force majeure. The Procuring Entity accepts no liability for the damage of Goods during transit other than those prescribed by INCOTERMS for DDP deliveries. In the case of Goods supplied from within the Philippines or supplied by domestic Suppliers risk and title will not be deemed to have passed to the Procuring Entity until their receipt and final acceptance at the final destination. **Intellectual Property Rights –** The Supplier shall indemnify the Procuring Entity against all third-party claims of infringement of patent, trademark, or industrial design rights arising from use of the Goods or any part thereof.
2.2	The terms of payment shall be as follows:

	• Payment shall be made in Philippine Currency. The amount due to the winning bidder shall be based entirely on the number of containers tagged/serviced in accordance with this TOR. The invoicing or billing to PPA on a bi-monthly basis shall be allowed. PPA shall not be liable for any operating loss the winning bidder might incur in the conduct of this managed turnkey service.
4	The inspection and tests that will be conducted are: The Philippine Ports Authority-Head Office shall have the right to inspect and/or test the software, security, equipment and peripherals to confirm conformity with the Terms of Reference and Contract. The winning bidder shall furnish test equipment, instrumentation, personnel and supplies necessary to perform all testing. PPA- Head Office shall be given a five (5) working day notice prior to tests.

Section VI. Schedule of Requirements

The delivery schedule expressed as weeks/months stipulates hereafter a delivery date which is the date of delivery to the project site.

Item Number	Description	Quantity	Total	Delivered, Weeks/Months
	Procurement of Trusted Operator Program – Container Registry Monitoring System (TOP-CRMS) & Empty Container Storage Shared Service Facility Design Specifications and Implementation, subject to the following stages:			
	A. TECHNICAL IMPLEMENTATION PHASE			Shall not exceed Twelve (12) Months from Receipt of the Notice to Proceed (NTP)
	1. Detailed Program Implementation Planning and Scheduling			From Receipt of the NTP + 1 month
	2. Solution Technical Architecture (Platform, Applications, Integration, and Data Management), Standard Business Process Framework Design			From Receipt of the NTP + 2 months
	3. Software and Database Management Systems Implementation, 3rd Party Systems Integration, Testing, and Deployment			From Receipt of the NTP + 8 months
	4. Station, Network and Infrastructure Setup, Configuration, Testing, and Deployment			From Receipt of the NTP + 5 months
	5. Device Configuration, Testing, Commissioning, and Deployment			From Receipt of the NTP + 5 months

	6. Procedural Streamlining and Functional On-Boarding a) Functional On-Boardingand Go-Live Plan b) Change Management Plan c) Training and Capacity Development Plan			From Receipt of the NTP + 6 months
	d) Conduct of Capacity Development Workshop e) Conduct of Sys adminTraining Workshop f) Conduct of Functional Admin Training Workshop g) Conduct of Data Administration and Management Workshop			From Receipt of the NTP + 9 months
	7. Draft Issuance of Procedures,Rules and Policies			From Receipt of the NTP + 6 months
	8. Deployment, Go-Live, and Operationalization			From Receipt of the NTP + 9 months
	9. 10-Hectare Empty Storage Shared Services Facility			From Receipt of the NTP + 9 months
	10. Operationalization of Container Tagging			From Receipt of the NTP + 9 months
	B. MANAGED			One (1) Year from date of the go-live or

	SERVICES			operationalization commissioning of the Technical Implementation Phase

Section VII. Technical Specifications

Technical Specifications

Item	Specification	Statement of Compliance
		[Bidders must state here either "Comply" or "Not Comply" against each of the individual parameters of each Specification stating the corresponding performance parameter of the equipment offered. Statements of "Comply" or "Not Comply" must be supported by evidence in a Bidders Bid and cross-referenced to that evidence. Evidence shall be in the form of manufacturer's un-amended sales literature, unconditional statements of specification and compliance issued by the manufacturer, samples, independent test data etc., as appropriate. A

		statement that is not supported by evidence or is subsequently found to be contradicted by the evidence presented will render the Bid under evaluation liable for rejection. A statement either in the Bidder's statement of compliance or the supporting evidence that is found to be false either during Bid evaluation, post-qualification or the execution of the Contract may be regarded as fraudulent and render the Bidder or supplier liable for prosecution subject to the applicable laws and issuances.]
	TRUSTED OPERATOR PROGRAM – CONTAINER REGISTRY MONITORING SYSTEM (TOP-CRMS) & EMPTY CONTAINER STORAGE SHARED SERVICE FACILITY DESIGN SPECIFICATIONS AND IMPLEMENTATION	

	GENERAL DESCRIPTION OF THE PROJECT: The supply, delivery of the full technology stack, the financing, technical implementation services, and managed services to successfully implement TOP-CRMS of PPA. The TOP-CRMS program will be launched and rolled-out covering two (2) pilot ports that house 98% of all container traffic. These are at the Port of Manila (POM): Manila International Container Terminal (MICT); and Manila South Harbor (MSH), inclusive of three (3) PEZA locations (for detachment and re-attachment of tagging devices of containers entering/leaving PEZA zones), as defined/required by the PPA. The TOP-CRMS consists of the following, inter-related program components: the Trust Operator Program: the Container Identification and Control Program, the Container Tracking Program, the Container Accountability and Insurance Protection Program. Each of these sub-programs target specific functional contexts and form the collective whole.	
	The service fee shall not exceed the amount of Four Thousand Nine Hundred Pesos (Php4,900.00), exclusive of 12% VAT, per tagged container.	
	SCOPE OF WORK 1. Physically tag and monitor a minimum of 200,000 containers 2. Deliver, install, customize, configure, deploy, and implement a TOP-CRMS for the Philippine Ports Authority. 3. Set up and operationalize 24/7 field operations for the attachment and detachment of tagging devices in the following locations: The Port of Manila: MICT and MSH; and three (3) PEZA locations, as defined and required by PPA. 3. Provide support services necessary to ensure exchange of information as well as hardware, software, network, databases, and information systems/application systems which are fully integrated and operational. 4. Provide the following implementation services: 4.1 Functional / Procedural Engineering, Re-Engineering, and Change Management 4.2 Policy Evaluation, Design, and Development 4.3 Technology Implementation 4.4 Business Development, Marketing, and Communications	

	4.5 10-hectare Area for Empty Container Re-Export Staging and Tagging Device Detachment 5. Include in its Operations, Maintenance, and Support Plan, among others, the following information: 5.1 Staffing plan and Number of Support Staff 5.2 Location and Operational Processes 5.3 Minimum Service Levels, such as: 5.3.1 Immediate Help desk response time for various classes of problems. 5.3.2 On-site support within 4 hours of reported incident 5.4 Usage statistics 6. Provide risk management plan detailing the strategies and appropriate measures to be undertaken. The plan should detail the following: 6.1 Risk Management Organization and Responsibilities 6.2 Risk Management Structure and Procedures for planning, identification, assessment, handling, and monitoring. 7. Provide a Disaster Recovery Plan which must contain the comprehensive procedures necessary to resume business to its normal operation in the least possible time for emergency response, backup and recovery. 8. Provide a complete documentation for every deliverable. PPA shall own all documents and shall reserve the right to reproduce at no additional cost. 9. Provide sufficient area for staging of containers and detachment of tracking device.	
	RESPONSIBILITY OF THE WINNING BIDDER The winning bidder shall be responsible for the provision of the following components for the entire duration of the contract: 1. Technology 1.1 TOP-CRMS with perpetual licensing and annual support and maintenance included for the whole duration of the Contract.	

		1.2 Hybrid and/or Multi-Cloud Infrastructure (Compute and Storage) 1.3 Cloud-Based High Performance Computing Server 1.4 On-Premise Backup and Enterprise Storage System 1.5 Network, and Application Security Appliance 1.6 Trusted Operator System 1.7 Container Identification and Control System 1.8 Container Accountability and Insurance Protection System 1.9 Tracking Device, Communications Network and Monitoring Systems 1.10Computing and Storage, Cloud Infrastructure, and Connectivity Systems 1.11Frontline and Mobile Transactional Applications Systems 1.12Enterprise Applications, Middleware, Data Processing, Data Management, and Reports and Analytics Systems 1.13Data Protection and Security Systems 1.14 Account and Profile Management System 1.15 Development and Deployment Platform 1.16 Turnkey Environment for Tracking Devices and Communications Network 1.17 Payment Aggregator and secure API connector services to standard, local, and international payment gateway systems, and/or electronic money issuers 1.18 Cloud security and Threat Analytics 2. Services 2.1 Supply, Delivery, Installation and Commissioning of the TOP-CRMS System, Engineering, Implementation, and Support Services 2.2 Project and Technical Implementation Services	

2.3 Systems Administration Services

2.4 Dedicated Technical and Helpdesk Support Staff

2.5 Operations Management Services

3. Network Connectivity

4. Courseware Materials and Training Conducts

The winning bidder shall provide the courseware for training of administrators and private container operator end-users that will use the Container Registry Monitoring System. Training shall be conducted for designated administrators at the main office, and for end-users and functional line personnel. Self-help user guides shall also be made available and accessible via the software system as an online FAQ service.

5. Post- Production Container Operator On-Boarding Support

The winning bidder must provide, upon successful deployment of the system into production environment, the necessary technical and functional support services to on-board container operators onto the system of the PPA.

The winning bidder must also provide, upon successful deployment of the system into a production environment, the necessary technical support services to assist the connectivity of container operators using the PPA prescribed standard API web services. The winning bidder shall be responsible to assure that all API terminations are secure and executed with minimal transactional latency.

6. Post-Production Software and Equipment Support and Maintenance

The winning bidder shall provide, upon the successful deployment of the system into production, a permit to freely to use the software, inclusive of support and maintenance services to PPA for not less than five (5) years, at no additional cost to the government, for the continued maintenance of the system inclusive of the application of security patches, functional de-bugging, and to ensure compliance to the service level uptime commitments as specified by the PPA.

The winning bidder shall also provide a replacement for all damaged parts and equipment that are covered under the

prescribed warranty period, within 24-hours of being reported as inoperable or at the time the same has come to the knowledge of the service provider, whichever comes first.

7. Technical Support and Customer Help Desk

The winning bidder must provide the personnel for technical support and customer help desk services to assist technical administrators and users of the system following the minimum Service Level as specified in this TOR. Services must be available eight (8) hours per day/ seven (7) days a week for the duration of the contract plus one (1) year.

OPERATIONAL AND FUNCTIONAL REQUIREMENTS, DESCRIPTIONS AND SPECIFICATIONS

The program must acquire a secure, turnkey, full-stack, technology (hardware and software) and managed services solution to support and sustain the CRMS program consisting of the following systems, namely: the Trusted Operator System, the Container Identification and Control System, the Container Tracking System, and the Container Accountability and Insurance Protection System. Each program sub-group will provide direct solutions that target a specific operational use case essential to deliver the full and cohesive CRMS solution.

Functional Components:

Trusted Operator System	This functional program sub-group will provide the required conventional and mobility systems and technology infrastructure to capture, store, and process subscription and transactional activities and integrated services made available to trusted operators.
Container Identification and Control System	This functional program sub-group will provide the required conventional systems, mobility systems, and technology infrastructure to enable the PPA to digitally capture using industry-accepted data interchange formats, through secure and encrypted channels, all inbound shipping containers in advance or before its entry in any port of the country.

Container Tracking System	This functional program sub-group will provide the conventional systems, devices, and technology infrastructure (hardware, software, data management) to enable the PPA to digitally tag all inbound shipping containers with a tracking device (attached to the container asset while remaining in the country) giving the PPA full visibility of the utilization, movement, and location of every foreign-ownedcontainer.
Container Accountability andInsurance Protection System	This functional program sub-group will provide local importers access to container insurance services, and will also provide the PPA the ability to monitor financial transactions required by shipping lines for all inbound shipping containers to safeguard the revenue interests ofthe govemment.

HARDWARE APPLIANCES, INFRASTRUCTURE, AND CONNECTIVITY	
Tracking Device, Communications Network and Monitoring Systems Group:	Container Tracking, Tracking Devices, Secure Data Storage, and Dedicated Distributed Network Infrastructure
Computing and Storage,Cloud Infrastructure, and Connectivity Systems Group:	Secure Virtual Private Cloud Infrastructure, On-Premise High-Performance Computing, and Storage Infrastructure, High-Speed Internet Broadband Leased-Line Connectivity
SOFTWARE SYSTEMS	
Frontline and Mobile Transactional Applications Systems Group:	Secure Frontline Transactional and Data CollectionApplications
Enterprise Applications, Middleware, Data Processing and Analytics Systems Group:	Secure Enterprise Management Applications, Data Processing, and Analytics, Enterprise Middleware System, Data Management and Analytics
Data Protection and Security Systems Group:	Data Protection, Network, and Application Security andThreat Monitoring

Software-Based Components	
System Group	System Module / Feature Components
Tracking Device, CommunicationsNetwork, and Monitoring Systems Group	The solution must have the followingminimum devices, standard turnkey capabilities, and services: ▪ IP67 Certified Tracking Devices ▪ Network Gateways ▪ Receiver Base Stations ▪ High-speed Broadband Network Interconnectivity ▪ Tracking Device Management System ▪ Cloud Data Repository ▪ Device Monitoring Service ▪ API Web Service Endpoint Services
Frontline and Mobile TransactionalApplications Systems Group	The solution must have the following minimum standard turnkey capabilities andservices: ▪ Program Portal CMS ▪ System Account Registration and SecureLogin ▪ Enrollment and Registration Services (Shipping Line, Vessel and Voyage, Driver, and Vehicle) ▪ User Profile and Account ManagementServices ▪ Container, Driver, and Transport Management Services Mobile Application(Transaction Dispatch, Driver Acceptance, Delivery Confirmation, Yard Entry/Exit Tagging, Road Emergency Report Service) ▪ Shipping Container Registry ▪ Vehicle Mapping Service ▪ Container Protection Disclosures ▪ Container Insurance Enrollment Services ▪ FAQs, User Help Desk and OnlineSupport ▪ API Web Service Endpoint Services

	Enterprise Applications, Middleware, Data Management, Data Processing, Reports, and Analytics Systems Group	The solution must have the following minimum standard turnkey capabilities andservices: ■ Enterprise Applications • Systems and User AdministrationManagement • System Access and PermissionsManagement • Subscriber Profile Records Management • Subscription Management • Subscriber Benefits Administration and Management • User Transactions Monitoring • Risk Exceptions Processing • Case Management • Invoicing and Billing ■ Middleware and Integration • Application Registry / CatalogService • API Web Service EndpointsCatalog Service • Business Orchestration Service(Business Process and Rules Management, Workflow and Route Management Engine) • Operations Management Platform • API Gateway Management ■ Service ■ Data Management • Open Standards-based Databases (Relational DatabaseManagement System (RDBMS),NoSQL Database Management, Flat-file Storage System) • Big Data Repositories (Data LakeSystem, Data Warehousing, DataMart) • Data Management (Data Management and Administration, ETL Management Tool, ReferenceData Registries) ■ Analytics and Visualization: • Executive Dashboard • Data Streaming Engine • Risk and Compliance Profiling ■ Reports Visualization	

Data Protection and Security SystemsGroup	The solution must have the following minimum standard turnkey capabilities andservices: ▪ Data Encryption and Protection (encryption-in-flight / encryption-at-rest) ▪ Network Security (Edge Protection, CDN,Optimization) ▪ Cloud Security and Workload Protection ▪ Malware Scanning, Detection, Detonation, Inoculation, Attribution, andReporting ▪ Vulnerability and Penetration Testing ▪ Cybersecurity Threat Monitoring

Computing and Storage, Cloud Infrastructure, and Connectivity Systems Group	The solution must have the following minimum standard turnkey capabilities and services: ▪ Server System ▪ Storage ▪ Cloud Infrastructure ▪ High-Speed Connectivity

System Group	Frontline Transactional Application Systems
Business Requirement	**Functional Specification**
Program Portal and Unified CMS	▪ The Unified Portal must provide an open standards-based Content Management System (CMS) that will serve as the unified access service or portal service for public and agency users to centrally access the system. ▪ The CMS must be based on current web-responsive technologies ▪ The CMS must provide features that allow content creators, designers, copywriters to securely publish both static and dynamic content. ▪ The CMS must provide features that allow end-users to extend and scale functionalities to meet current and emerging content publication needs. ▪ The CMS must provide features that consolidate the library of end-user applications accessible via a single portal with a cohesive, end-user configurable, user experience ▪ The CMS must provide end-users access to a rich library of web templates ▪ The CMS must provide features for personalization. ▪ The CMS must provide features to seamlessly integrate with current SAML or OAuth-based Single Sign-On (SSO) capabilities. ▪ The CMS must provide a native API web service endpoint (JSON, XML) for module security,

		integration, and accessibility		
	System User Registration Service	▪ The System User Registration service must provide features and functions for the public to register online to create an account. ▪ The service must provide provenance-enabled features that allow new registrants to: o Create their initial login credentials (username and passwords) o Define the number of applicable system personas o Define organizational affiliations o Provide basic user data (name, DoB, address, primary and secondary email address, mobile number, etc.) ▪ Upon successful access registration, the service must be able to generate a standard user identity QR code that will be readable and usable throughout the entire system. ▪ The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.		
	Program Enrollment Service	▪ The program enrollment service is the primary application for existing registered system users to enroll in the Trusted Operator Program of the CRMS. ▪ It must provide features that enable enrollees to: o Complete the program enrollment using an online application form o Submit a current digital photo o Submit digital copies of required program documentation o Provide digital references to other government identification, permits/license, or accreditation systems ▪ It must provide native digital workflow routing features for application processing, disposition, and approval ▪ It must provide enrollees with a visual process map showing the details and status of their application, indicating who is handling their application and when it was received by the processor. ▪ Upon successful access enrollment, the service must be able to generate a standard QR code that will be readable and usable throughout the entire system.		

		▪ The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.	
	Shipping Container Registration and Identification Service	The shipping container registration and identification service enable all foreign shipping lines to submit a complete inventory of all foreign-owned containers that enter Philippine ports. ▪ The service must allow foreign shipping lines the ability to perform secure bulk uploads (*.csv, *.xlsx, *.odt formats) submission of their container inventory that enters Philippine ports ▪ The service must comply with UN/CEFACT standards for shipping container data exchange format. ▪ The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.	
	Advanced In-Bound Container Declaration	▪ The in-bound container declaration service is an online bulk submission service to enable shipping lines to transmit data on all inbound containers in advance or before arrival. ▪ The service must allow foreign shipping lines the ability to perform secure bulk uploads/submission (*.csv, *.xlsx, *.odt formats) of their in-bound container inventory in advance. ▪ The service must provide a downloadable spreadsheet template that users can use to bulk upload all in-bound containers in advance. ▪ The service must comply with UN/CEFACT standards for shipping container data exchange format. ▪ The module must provide a native API web service endpoint (JSON, XML) for modulesecurity, integration, and accessibility.	
	Advanced Port Services Booking	▪ The advanced port services booking is a service available only to registered and subscribed Trusted Operators of the CRMS enabling subscribers to schedule berth entry, unloading and unloading, schedule with the TABS system of the PPA, and reserve storage. ▪ The service must integrate with current PPA container handling, discharge, transport, and storage services. ▪ The service must integrate with the following current PPA services: o Berth Scheduling o Unloading and Loading Scheduling o Trucker Advanced	

		BookingSystem o Returns Scheduling and Storage ▪ The service must allow Trusted Operators to pay for all required fees for all services availed by the Trusted Operator via services of banks, registered EMV's, or online payment gateway services. ▪ Upon successful access enrollment, the service must be able to generate a standard QR code that will be readable and usable throughout the entire system ▪ The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.	
	Container Protection Disclosures	▪ The container protection disclosures service enables both shipping lines and local importers the ability to disclose financial transactions made against the use of foreign-owned shipping containers. ▪ The service must provide the functionality to enable *shipping lines* or their local representatives with the ability to disclose container protection options (container deposit, container maintenance, container insurance) and values paid by local importers either in bulk or per unit for the use of the shipping container. ▪ The service must provide the functionality to enable *local importers* or their designated brokers with the ability to directly associate the container protection option and the corresponding value or the amount paid for the use of a shipping container (per unit or in bulk). ▪ The system must be able to dynamically reference the foreign shipping line owner of a container ID number referenced by a local importer. ▪ The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.	

Container Insurance Service Provider Registration	▪ The container insurance service provider registration enables private insurance providers to register to make their services accessible to importers or service subscribers via the online CRMS. ▪ Insurance providers must be enrolled andregistered as subscribers to the Trusted Operator Program. ▪ The service must provide features for insurance providers to: o Detail different insurance product offerings, the scope of coverage, value, and premium amount, additional riders (if or when applicable) o Payment settlement options o Detail claims processing requirements ▪ The module must provide a native API web service endpoint (JSON, XML) for modulesecurity, integration, and accessibility.
Container Insurance Enrollment andClaims	▪ The container insurance enrollment service enables local importers the optionto avail of container insurance coverage instead of paying for container deposit or container maintenance fees ▪ The service must: o Allow the local importer to electronically avail of insurance coverage for one or many shipping containers across one or multiple shipping transactions between one or many shipping lines o Enable insurance providers to electronically issue the insurance policy document covering one or multiple shipping transactions across one or multiple shipping lines ▪ The service must enable importers to directly pay for insurance coverage. ▪ The service must provide features for local importers to electronically file for insurance claims. ▪ The service must also provide features that enable both the claimant (local importer) and beneficiary (shipping lines)to monitor the progress of claims submitted and in process. ▪ The module must provide a native API web service endpoint (JSON, XML) for modulesecurity, integration, and accessibility.

Electronic Purse and PaymentServices	▪ The electronic purse and payment services are the payment aggregation service of the system that enables the system and its subscribers to manage their payment transactions and connect to current payment gateways, banks, or electronic wallets. ▪ The service must provide features that provide subscribers with a digital expense wallet with the native feature to connect to one or several payment gateways and/or banks. ▪ The service must provide features that enable users to track and monitor payments as well as detailed ledgers of historical payment transactions. ▪ The module must provide a native API web service endpoint (JSON, XML) for modulesecurity, integration, and accessibility.
Online Support and Chat	▪ The online support and chat service enables users and subscribers to access online help via live chat (regular business hours) or using guided/scripted chatbots 24x7 for the most common questions or help items. ▪ The module must provide a native API web service endpoint (JSON, XML) for modulesecurity, integration, and accessibility.

System Group	Account and Profile Management System
Business Requirement	**Functional Specification**
Organizational Profile and Account Management	▪ The organizational profile and account management service enables CRMS and TOP subscribers the ability to detail and manage organizational-specific data, authorized users (users must first have their user account in the system), define their catalog of services, and organizational credentials. ▪ The system must provide features for theorganization to generate a unique QR Code reference of their organization that can be externally used to reference or identify the organization and linked to the accounts of authorized representatives. ▪ The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.

User Account Profile and PersonaManagement	▪ The user account profile and personal management service enable registered users to detail their personal information and detail the different personas (importer, broker, shipper, logistics provider, trucker, driver, etc.) that apply in the use of the system. ▪ The system must allow users to manage personal details, add, update, or modify personal details. ▪ The system must provide features that generate a secure QR Code unique to each user. ▪ The module must provide a native API web service endpoint (JSON, XML) for modulesecurity, integration, and accessibility.

System Group	Mobile Transactional Application Systems(Android)
Business Requirement	**Functional Specification**
Job/Work Order Management	▪ The job/work order management service enables registered users to issue and receive work orders for the transport of shipping containers from the port of discharge, and job orders to return empty shipping containers to the designated container yard ▪ The service must provide features for local importers access to a list of registered transport/logistics providers containing an inventory and immediate location of the provider's drivers and trucks, along with standard pricing. ▪ The service must provide features for trucking operators to invite/assign/designate drivers to operatespecific trucks with the ability for drivers to accept work orders. ▪ The service must provide features for service providers to submit job proposals in response to the inquiries. ▪ The service must provide features that enable local importers to award work to one or multiple service providers (drivers). ▪ The service must provide features for service providers to issue default contracts, issue invoices, receive payment for completed work orders, andupload a digital copy of official receipts referenceable by both issuer and recipient. ▪ The module must provide native API webservice endpoints (JSON, XML) for module security, integration, and accessibility.

Driver and Truck Dispatch Service	▪ The driver and truck dispatch service enable the service provider to manage the assigning of a driver or drivers to a specific truck or trucks and dispatch the same to fulfill a work order. ▪ The module must provide native API webservice endpoints (JSON, XML) for module security, integration, and accessibility.
Job Acceptance, Delivery, and Fulfillment Confirmation	▪ The service must provide features that enable the driver to tag the actual time a container is hitched to a truck for transport and the time it completes a delivery. ▪ The module must provide native API webservice endpoints (JSON, XML) for module security, integration, and accessibility.
Container Tagging and Recording System	▪ The container tagging and recording service enable designated personnel to physically tag a container with a tracking device and associate the container reference identification with the tracking device. ▪ This service must-have features that enable it to directly exchange data with the Trucker Advanced Booking Systems and the gate management systems of each container port/yard. ▪ The module must provide native API webservice endpoints (JSON, XML) for module security, integration, and accessibility.
Container Release, Receiving, andDevice Detachment	▪ The service must provide a gate management system (RFID or QR Code) to monitor the discharge and return of all shipping containers to and from the container yard. ▪ The application must also provide features that enable the management of device detachment before the re-export of shipping containers. ▪ The service must provide four status options about the container, namely: discharged, returned, in-storage, and re-exported. ▪ The module must provide native API webservice endpoints (JSON, XML) for module security, integration, and accessibility.

Road Emergency Reporting	▪ The emergency reporting service enables drivers to report roadside incidents and communicate directly with the customer. ▪ The service must provide features that directly message all involved parties via the in app messaging service, and electronic mail. ▪ The module must provide native API webservice endpoints (JSON, XML) for module security, integration, and accessibility.	
Advanced Port Services Booking	▪ The advanced port services booking, is a concierge-type, red-carpet service available only to users subscribed under the Trusted Operator Program of CRMS. ▪ The service must provide features that enable users to schedule port services inadvance, that include the following: o Advanced Port Entry Clearance o Advanced Berthing Appointment and Booking o Prioritized Unloading and Loading o Advanced Port Services Payment o Advanced TABS Appointment and Booking ▪ The module must provide native API webservice endpoints (JSON, XML) for module security, integration, and accessibility.	
Container Insurance Enrollment	▪ The container insurance enrollment service enables local importers the optionto avail of container insurance coverage instead of paying for container deposit or container maintenance fees using a mobile application. ▪ The service must: o Allow the local importer to electronically avail of insurance coverage for one or many shipping containers across one or multiple shipping transactions between one or many shipping lines o Enable insurance providers to electronically issue the insurance policy document covering one or multiple shipping transactions across one or multiple shipping lines	

		▪ The service must enable importers to directly pay for insurance coverage. ▪ The service must provide features for local importers to electronically file for insurance claims. ▪ The service must also provide features that enable both the claimant (local importer) and beneficiary (shipping lines) to monitor the progress of claims submitted and in process ▪ The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.
	Electronic Purse and PaymentServices	▪ The electronic purse and payment services are the payment aggregation service of the system that enables the system and its subscribers to manage their payment transactions and connect tocurrent payment gateways, banks, or electronic wallets using a mobile application. ▪ The service must provide features that provide subscribers with a digital expense wallet with the native feature to connect to one or several payment gateways and/or banks. ▪ The service must provide features that enable users to track and monitor payments as well as detailed ledgers of historical payment transactions. ▪ The module must provide a native API web service endpoint (JSON, XML) for modulesecurity, integration, and accessibility.
	Online Support and Chat	▪ The online support and chat service enables users and subscribers to access online help via live chat (regular business hours) ▪ The online support must provide guided/scripted chatbots 24x7 for the most common questions or help items using a browser or mobile application. ▪ The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.
	Vehicle Mapping Services	▪ The vehicle mapping is a software-based service that enables parties involved in a transaction to track the location of a vehicle using a mobile application. ▪ The service must-have features that could send or stream the location of the user to a designated analytics and reporting system. ▪ The module must provide a native API web service endpoint (JSON,

		XML) for module security, integration, and accessibility.	
	System Group	Enterprise Application Systems	
	Business Requirement	Functional Specification	
	Systems Access and Permissions Management	▪ The systems access and permissions management enable system administrators to define, assign, modify,revoke, or terminate end-user permissions at defined levels of granularity. ▪ The module must provide a native API web service endpoint (JSON, XML) for modulesecurity, integration, and accessibility.	
	Systems and User Administration Management	▪ The systems and user administration management enables systems administrators to define, assign, modify,revoke, or terminate systems users or designated functional administrators. ▪ The service must provide centralized administrative features that enable systems administrators to manage every component of the deployed system, inclusive of the CMS, web forms, cloud infrastructure, orchestration, middleware and integration, API management, database management, big data, and analytics system. ▪ The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.	
	Subscriber Administration and Management	▪ The subscriber administration and management enable the systems administrator to define and configure subscriber programs. ▪ The service must provide functions that enable systems administrators to define requirements, define permissions, define and configure allowed functions (such as personalization and messaging). ▪ The service must provide functions thatenable systems administrators to define and configure features available to functional users. ▪ The service must provide functions that enable authorized functional users to process enrollments, approve, and issue the required credentials or electronic documents as may be necessary. ▪ The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.	
	Subscriber Benefits Management	▪ The subscriber benefits management is a service that enables both systems administrators	

		and functional users with features to define, create, configure, or retire benefits available to enrolled entities or persons of the Trusted Operator Program. ▪ The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.
	User Transaction Monitoring	▪ The user transaction monitoring is an executive dashboard service that enables authorized systems administrators and functional users with features and visual interfaces that allow for the monitoring of granular behavior of the system and its users as visual reports in a dashboard. ▪ The system must provide features that forsystem administrators to view changes made to configurations and data repositories; view active users, inactive users, and suspended users; view connection statuses of authorized API service endpoints and the metadata of transactions between any part of the system with external web services. ▪ The module must provide a native API web service endpoint (JSON, XML) for modulesecurity, integration, and accessibility.
	Records and Document Management	▪ The records and document management are a specific service to enable public users and functional users with features to manage the submission of electronic documents (PDF, images, etc.), the routing of electronic documents, the viewing of who has accessed and viewed those documents, and when they were viewed. ▪ The systems must provide features that creates a unique hash identifier to secure and encrypt every document submitted within the system. ▪ The system must provide the requisite public-private keys to enable documents to be encrypted and de-crypted accordingly. ▪ The system must provide features that store document metadata under a key- value pairing repository with the actual artifact stored in either a relational or flat file database system. ▪ The module must provide native API web service endpoint (JSON, XML) for module security, integration, and

	accessibility.
Risk Exceptions Processing and Profiling	▪ The risk exceptions processing and profiling enable authorized users to apply rules-based parameters to produce visualized reports that allow for the granular viewing of source data. ▪ The system must provide features that present a set of visualized exception reports on all occurring systems exceptions in real-time and present a corresponding profile containing attribution details covering all applications that form the full system. ▪ The system must be seamlessly integrated into the case management system service. ▪ The module must provide a native API web service endpoint (JSON, XML) for modulesecurity, integration, and accessibility.
Case Management	▪ The case management service enables authorized functional administrators to create new cases from the risk exceptions and profiling service of the system. ▪ The service must be rules-based and enabled with multi-nodal capable workflow automation and management features. ▪ The service must provide features and functions that enable functional administrators to configure workflows that conform to the internal procedural environment of the organization. ▪ The service must be integrated into the records and document management service. ▪ The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.
Container Location Mapping Service	▪ The container location mapping service enables authorized functional users the ability to track the movement and location of a shipping container and is distinct from the truck mapping service. ▪ The service must provide a visual dashboard that displays the actual movement and location of all shipping containers whether in transport or storage. ▪ The service must have features and functions for functional users to generate standard and ad hoc reports as may be defined by functional users that can be importable into a target format such as a comma-separated value,

	portable document format, a JSON-format, or XMLformat. ▪ The module must provide a native API web service endpoint (JSON, XML) for modulesecurity, integration, and accessibility.	
Invoicing and Billing	▪ The invoice and billing service enables functional users and registered subscribers of the system to automate the generation, electronic transmission, and monitoring of invoices. ▪ The service must provide functional users the ability to generate invoices for shipping lines, local importers, and those and functional users with features to manage the submission of electronic documents (PDF, images, etc.), the routing of electronic documents, the viewing of who has accessed and viewed those documents, and when they were viewed. ▪ The systems must provide features that create a unique hash identifier to secure and encrypt every document submitted within the system. ▪ The system must provide the requisite public-private keys to enable documents to be encrypted and decrypted accordingly. ▪ The system must provide features that store document metadata under a key-value pairing repository with the actual artifact stored in either a relational or flat-file database system. ▪ The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.	

	Payment Aggregation Service	▪ Must have payment aggregation capability for fee-based services ▪ Must be at least PCI DDS Level 1 compliant ▪ Must support up to a minimum of 5,000,000 transactions per month. ▪ Must be able to process payments via major cards like Visa and Mastercard. Must be linked to at least 1 card provider. ▪ Must allow payments on IOS and Android-based mobile platforms. ▪ Must be able to generate a bill or invoiceor statement of account. ▪ Must provide updates on the payment status of issued bills or invoices. ▪ Must provide updates on the payment status of issued bills or invoices ▪ Must be able to deliver the client invoices over SMS, email, and push notifications. ▪ Must be able to provide payment options and guidelines as the invoice is served ▪ Must be able to support Over the Counter (OTC) Payments. ▪ Must be able to interface with other channels of payment via API ▪ Must be able to utilize multiple Points of Payment (POP) to add convenience or easy access for payment. ▪ Must be able to process payments within 2 minutes from receipt of billing.	
	System Group: Enterprise Middleware System		
	Business Requirement	Functional Specification	
	Application Registry Service	▪ The application registry service is a central registry containing a detailed description, web service endpoints, and security protocols of all microservices that form part of the system and is managed as a function of the enterprise middleware layer of the system. ▪ The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.	

Business Process Management	▪ The business process management engine is an enterprise middleware service that enables system and functional administrators to centrally define, configure, manage, and monitor business process flows that will be linked or referenced in the business rules management engine. ▪ The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.
Business Rules Management	▪ The business rules management engine is an enterprise middleware service that enables system and functional administrators to centrally define, configure, manage, and monitor business rules that will be linked or referenced in the workflow and route management service. ▪ The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.
Workflow and Route Management	▪ The workflow and route management engine are an enterprise middleware service that enables system and functional administrators to define, configure, manage, and monitor the procedural flows that frame the behavior and procedural efficiency of microservices. ▪ This service de-couples the definition of routes of all microservices that are part of the system. ▪ The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.
Operations Management Platform	▪ Must be a modern, cloud or web-based application that facilitates access and harmonization of information across specified information systems. ▪ Must allow access to the information systems thru browsers and a variety of mobile devices. ▪ Must enable usage of most major brands of the currently available SQL or NoSQL-based database systems. Once a particular database is chosen, the platform ensures the consistency, security, and accessibility of the data on this chosen database platform. ▪ Must allow independent modifications to the functionalities of the system. The whole system must not go down when code changes are done and must also contain a microservice architecture, which is key to scalability and the high availability of the system.

			▪ Must be able to demonstrate compliance with all the requisite security features of a web or internet-based application. Must also be able to provide an identity management and access control layer for another layer of security for the system, on top of the security features of the commercial cloud platform. ▪ Must enable the modeling of applications as processes of the various departments, created in a drag-and-drop workflow editor. Must also be able to design entry forms and assign to steps in the workflow as well as business rules, or output forms. ▪ Must have Software Development Tools ▪ Must provide Source Repository Tool ▪ Must have Issue Tracking Tool ▪ Must provide Continuous Integration Tool ▪ Must support at least 20 builds/projects ▪ Must provide Artifact Repository Tool ▪ Must provide Code Coverage Tool ▪ Must include development tool with the following capabilities: ▪ Must be capable of evaluating the static code, checking for potential security issues ▪ Must be able to dynamically analyze the review application to identify potential security issues. ▪ Must be able to evaluate third-party dependencies to identify potential security issues. ▪ Must be able to analyze Docker images and check for potential security issues. ▪ Must have a security dashboard to visualize the latest security status for each project and across projects. ▪ Must provide license compliance by identifying the presence of new software licenses included in your project and tracking project dependencies. Also, approve or deny the inclusion of a specific license. ▪ Must provide a Compliance dashboard that gives you the ability to see your group's Merge Request activity by providing a high-level view for all projects in the group and approvers for the merge request. ▪ Must be able to visualize project insights to improve developer efficiencies. ▪ Must provide the capability to organize, plan, and prioritize business ideas and initiatives into	

	multi-level epics. ▪ Must enable granular access controls to allow specific people access to specific resources like groups and their underlying projects by IP Address. ▪ The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.	
API Gateway Management	▪ The API gateway management engine is an enterprise middleware service that enables secure two-way communication between system components using RESTful or WebSocket API methods. ▪ The service must have the environment, features, and functions that enable it to process a minimum of 4 million two-way API calls per month. ▪ The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.	
API Web Service Endpoint Catalog	▪ The API web service endpoint catalog is an enterprise middleware service that provides a standard registry, library, or repository of all categorized API artifacts. ▪ The service must have features and functions that structure and organize API artifacts according to the service function. ▪ The service must provide secure access protocols when allowing microservice access to published API artifacts. ▪ The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.	
System Group	Data Management and Data Processing System	
Business Requirement	**Functional Specification**	
Standard Reference Registries	The standard reference registry is a service that provides a centrally managed set of databases containing static, not frequently updated data sets. ▪ The service must provide the followingbase registries: o Location Reference Registry o UN/LOCODE Registry o Enrolled Subscribers o Registered Containers	

	Standards-Based Enterprise-Grade, Open-Source Databases	▪ Must provision RDBMS Database ▪ Must also provision NoSQL Database ▪ Must be configured in an active-active HA configuration across data centers. ▪ Must have 24 X 7 Enterprise Support for the above-listed services ▪ Must have Virtualized environment to support virtualized database services ▪ Must provide Skills transfer for managingthe platform ▪ The product must be able to operate in both a private data center and a public infrastructure-as-a-service (IaaS)provider. It must run on top of following IaaS o Public – Amazon Web Services (AWS), Google Cloud (GCP), Microsoft Azure IAAS, and Containers o Private – vSphere VMs and containers, BareMetal ▪ The proposed solution stack should be based on the latest release ▪ Proposed solution stack should be based on open-source technology with commercial enterprise support 24*7 to ensure no lock-in ▪ The product must be cloud-agnostic and cloud-native (runs on any cloud or containerized environment) to provide flexibility of infrastructure choice. ▪ The product must support both the SQL and NoSQL APIs under a common storage substrate to ensure support for different database services currently and in future ▪ The product must support row-level locking and Multi-Version Concurrency Control ▪ The product must support database compression, with minimal or no impact on performance ▪ The product must offer low latency, timeline-consistent reads even in remote regions. ▪ The product must support change data capture features. Drive external apps with data change streams. ▪ The product must allow row-level geo-partitioning capabilities allowing pinning of data to geographic locations, thereby allowing the data residency to be managed at the database level to improve data locality access. ▪ The product architecture must leverage share-nothing architecture to yield a good performance and latency for OLTP workloads	

		▪ The solution should be 100% open source with the option to run a community edition to allow flexibility of aligning adoption strategy ▪ The product must be able to support a single synchronous cluster stretched across multiple AZ's/regions/cross clouds and support multiple advanced replication architectures for the resiliency of the system. ▪ The product must allow databases to be vertically or horizontally scale (up and down) without downtime to support elasticworkloads ▪ The product must offer a single user interface across various clouds with simplified database management and monitoring like DB upgrades, backups, security & on-demand scaling of nodes to simplify operation and management ▪ The product must support distributed ACID with both serializable & snapshot isolation ▪ The product must provide the ability to increase computing capacity in a linear fashion by adding new nodes to the existing database system with no downtime. ▪ The product architecture must be designed with no single point of failure entire system (include hardware level, system level, and software level) ▪ The product must support distributed Backups. One-click distributed backups and restores for clusters of any size. The database must support backup and restore at the instance level, table level, and offer point in time recovery. ▪ The product must be able to support data at rest encryption ▪ The product must be able to support data-in-transit encryption ▪ The product must be able to support at least a single node, single AZ, or single region failure with no impact on availability. ▪ The DBAAS should be able to bring the failed instances services back automatically when the resources are provisioned.	

		▪ The DBAAS platform must be able to support synchronous and asynchronous replication across sites or cloud ▪ Should support creating active-active (both read and write) clusters across multiple data centers from a single console. ▪ The DBAS platform must be able to support upgrades without any downtime ▪ The product must be able to support an RPO of 0	

	Big Data Management	▪ The Big Data Management platform proposed must include the following features. Data ▪ The solution must be able to define several assets (table, files, partition) created ▪ The solution must be able to define assets altered during the filter time interval ▪ The solution must be able to define Data Growth Rate Compute/Process ▪ The solution must be able to define and monitor the density of recurring & non-recurring jobs ▪ The solution must be able to define and monitor Failure & Distribution Rates – Failure by type – SQL/Non-SQL ▪ The solution must be able to define and monitor the Division of the job by action type: Create, Insert, Select ▪ The solution must be able to perform trend based analysis for all the queries going through the system. ▪ The solution must be able to provide data object analysis for Hive/Impala. ▪ The solution must be able to define and monitor Resource Allocation actions – DDL vs DML ▪ The solution must be able to define RCA job/query disruption. Users ▪ The solution must be able to define and monitor active users during the interval of the selection ▪ The solution must be able to define and monitor average query times across clients (users from different systems) ▪ The solution must be able to define user-level disruption during the selection period ▪ The solution must be able to define the exact count of instances and root causes that caused user/application outages ▪ The solution must be able to define RCA of environment and users' disruption for Hadoop ecosystem Optimization ▪ The solution must be able to monitor Jobs/Queries with optimization opportunities by way of Data Layout ▪ The solution must be able to monitor Jobs/Queues which are	

		not running appropriate container sizes wastage of resources across MR, Spark, Hive, LLAP, Sparkline. Infrastructure Service Monitoring • The solution must be able todefine and monitor Service disruptions • The solution must be able todefine and monitor Infrastructure disruptions • The solution must be able to define and monitor Disruptions experienced by other Applications/users because of the above disruption • The solution must be able to accurately provide the RCA of service disruptions. • The solution must be able to define the RCA of the infrastructure disruption (Hadoop ecosystem) • Must be able to provide kernel-level alerts and logging. • Must be able to provide detailed trend-based analysis andalerts for CPU, Memory, Network,IOPS, and Disk infrastructure. Service Monitoring • The solution must be able to monitor Kafka Job & Service e.g.: service up/down and job success/failure: o Kafka broker Status o Kafka topic lag and backpressure analysis and alerts o Kafka Replication o Kafka rate of data flow o Kafka topic skewness analysis • The solution must be able to monitor Spark2 Job & Service e.g.: service up/down and job success/failure • The solution must be able to monitor Flink Job & Service e.g.: service up/down and job success/failure • The solution must be able to monitor Sqoop Job & Service e.g.: service up/down and job success/failure. • The solution must be able to monitor Zookeeper Job & Service e.g.: service up/down and job success/failure • The solution must be able to monitor HBase: o HBase Master Status o Regions in Transition	

		○ Master Heap ○ Region Server Status ○ Provide region and table levelhot spotting • The solution must be able to monitor Hive: ○ Hive Master Status ○ Metastore Status ○ Webchat Status • The solution must be able to monitor Yarn: ○ Node Manager Status ○ Resource Manage Heap ○ Containers Status ○ Application Status ○ Cluster Memory ○ Resource consumption trend analysis and prediction. • The solution must be able to monitor HDFS: ○ Name node Status ○ Data node Status ○ Disk Usage ○ Block Errors ○ Safe Mode Status HDFS consumption analysis by the user, by file type, by size, and by age of files.
Data Warehousing and Data Mart Management		Data Warehouse Platform must have the following attributes and capabilities: Scalability and Extensibility • The solution platform must take a scale-out approach, achieving scale by pooling industry-standard commodity servers and storage devices. • The solution must also be scalable in the performance dimension, that applications experience no degradation in performance as the volume of data inthe system is increased. • The solution should have the ability to combine multiple sources ina single repository • The solution should support no limits on the number of users. It shall support all the users that need to simultaneously utilize it. It shall be able to accommodate increasing data volumes and additional users over time. • The solution should providedata-aware MPP capabilities out of the box and should separate metadata from data nodes • The product architecture must be open source and is a truly Massively Parallel Processing (MPP)Architecture that leveraging

		share- nothing architecture to yield very good performance for the Data Warehouse. • The solution should be able to run on-premise using bare Metal, on VM, or public cloud (AWS, Azure, GCP) or in a container • The solution should be able to support federated queries and have built-in machine learning libraries. Multi-tiered Architecture • The solution should have the capability to support dynamic tieringof hot, warm, and cold data that applications can deliver. • The solution should have the capability to support a large number of nodes in a cluster and should be able to accommodate additional nodes over time and increasing volumes. • Can run on x86 hardware, not tied into single proprietary hardware • Support runs on multiple platforms: bare metal, virtual, container • Single licensing model, no additional cost for features • Integrated machine learning capabilities • Table storage can be configured to external(Hadoop, S3 storage, etc.) • Support columnar and row-store on the same table • Support multiple User Defined Functions (SQL, Java, R,Python) • Capability to do parallel load and unload from the data node • Support native update and delete operation on the data • Have text search capabilities like Solr/ Lucene • Have workload management • Support semi-structured table/ data types: key-value, XML, JSON • Have geospatial capabilities	

	Database Management and Administration	• Must be tested on and support at least the following databases: Greenplum, Hive, MariaDB, MongoDB, PostgreSQL, Sybase, Vertica, MySQL, MS SQL Server, RedShift, Hive, Cassandra, Couchbase, Oracle, DB2, and Aurora • Must be able to browse database objects such as schemas, tables, columns, primary and foreignkeys, views, indexes, procedures, functions, and more. • Must provide visual tools to create,alter, describe, execute, and drop database objects such as tables, views, indexes, stored procedures, functions, triggers, and more. • Must be able to import data from various formats such as delimited files, Excel spreadsheets, and fixed-width files • Must be able to create select, insert,update, and delete SQL statements. Create multi-table joins. • Must be able to insert, update, and delete table data in a spreadsheet-like format. Find and replace data, preview generated SQL and more. • Must be able to edit SQL scripts. Run SQL queries. Auto column and auto table lookup. Must have a powerful code editor that supports over 20 programming languages including SQL, PL/SQL, Transact-SQL, SQL PL,HTML, Java, XML, and more. • Must include the multi-tabular display ofqueries with options for filtering, sorting, searching, and much more. • Must be able to compare table data across databases or compare the results of queries. • Must be able to export data in various formats such as delimited files, XML, HTML, Excel spreadsheets, JSON, and SQL insert statements. • Must have a perpetual license, for 4users, with 1-year support	

	Extract Transform and Load (ETL)Management System	▪ The platform could be on any environment, for example, single cloud,multiple cloud, or hybrid. ▪ The tool shall provide a drag-n-drop GUI for the design and development of ETL flows with minimal need to write any scriptor program. ▪ The tool shall provide the functionality to perform data profiling, data integration, and data quality via the same interface. ▪ The tool shall support granular role-basedsecurity authorization. ▪ The tool shall support version control of ETL flows and should allow rollback to previous versions. ▪ The tool shall support functionality for breakpoint testing, debugging, and troubleshooting of ETL flows. ▪ The tool shall support varieties of connectors for source and target. ▪ These connectors shall minimally include: ▪ Relational databases such as MicrosoftSQL, MySQL; ▪ In-memory databases such as SAP HANA and Vertica; ▪ Cloud databases such as Snowflake,Amazon Redshift; ▪ Flat file such as Excel files, Delimitedfiles, Text files, XML files, JSON files; ▪ REST API endpoints. ▪ The tool shall be capable of building and configuring different complex types of transformation such as but not limited to,data-type conversions, joins, filter, aggregations, lookup and replace, normalization, parsing of free-form text. ▪ The tool shall have the features of dataencryption and data masking. ▪ The tool shall support the development of user defined functions by using standard scripting syntaxes such as SQL, Python, andJava. ▪ The tool shall support parallel processing of multiple data flows and processing of multiple files towards the same target. ▪ The tool shall provide a GUI for management, administering, and monitoring of ETL flows, as well as defining access control. ▪ The tool shall have the capability for ETL jobs scheduling with predefined and customizable scheduling options. ▪ The tool shall provide the capability to send out emails during	

		exceptions or failures. ▪ The tool shall provide a system and job execution logs in a readable format and preferably accessible via an interface client. ▪ The tool shall have the feature of integration to the version control system. ▪ Software Licensing ▪ Licensing must be subscription-based ▪ All connectors must be inclusive ▪ Must not have a separate price for run-time & to include all non-prod environment ▪ ETL 'drag & drop' must translate into an editable program that is visible & re-usable ▪ License must be able to support on-prem, cloud, or hybrid environment	
	System Group: Data Protection and Security		
	Business Requirement	**Functional Specification**	
	Code Encryption	▪ The solution must be a cloud-native and API-based system configured as an abstraction between the application, API gateway, and between the API gateway and target repository. ▪ The solution must comply with the following security specifications: o AES 256bit GCM encryption algorithm o Key storage in FIP140-2 Type3 compliant HSMs o Key rotation policies from 3-24 months including automatic tracking of data/key pairs o Support encryption of any datatype including records or files ▪ The solution must provide capabilities that are embedded into both the web front end as well as the webserver to ensure end-to-end encryption to maximize security.	
	Data Vaulting and Protection	▪ The solution must be integrated into a platform that converts data into a verifiably authenticable entity in a heterogeneous communications network environment. ▪ The data must be converted into a one-way cryptographic hash using a secure hash algorithm. ▪ The artifacts committed to the data vaultmust be immutable – data stored cannotbe tampered with nor deleted.	

			▪ The data vaulting platform must be integrated into a PKI (public key infrastructure) to enforce a zero-trustsecurity environment. ▪ The data vault system must include a publisher computer in operative communication with a server computer system over a communications networksuch as the Internet. ▪ The publisher computer must be configured to (i) obtain a digital reproduction of at least one portion of the original entity on which at least one physical identifier or "PII" may be appearing; (ii) create an electronic file of the digital reproduction of the at least one portion of the original entity; and (iii) deliver, over the communications network, to the server computer system the electronic file. ▪ The server computer system must be configured to (i) extract at least one physical identifier from the electronic file; (ii) associate a set of unique identifiers or "SUI" to the extracted at least one physical identifier to create an electronic record of the original entity; and (iii) store in a memory system of the server computer system the electronic record of the original entity having the associated set of unique identifiers and at least one physical indicia identifier. ▪ The server computer system must be configured to (i) encrypt the electronic record of the original entity using a public key associated with the publisher computer and a digital signature including a private key associated with the publisher computer to generate a uniquely encrypted message or "UEM" carrying the associated set of unique identifiers and at least one physical indicia identifier; (ii) publish, over the communications network, the uniquely encrypted message to a chain of data on a public record-keeping system residing in one or more nodes in a decentralized computational network using at least one decentralized computational network protocol; and (iii) subsequently send, over the communications network, to the publisher computer the set of unique identifiers. ▪ The system must include a	