	▪ 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 aservice 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 module security, 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.

System Group	Enterprise Application Systems
Business Requirement	**Functional Specification**
Risk Exceptions Processing and Profiling	▪ The risk exceptions processing and profiling enable authorized users to apply rules-based parameters to producevisualized 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 applicationsthat form the full system. ▪ The system must be seamlessly integrated into the case managementsystem service. ▪ The module must provide a native API web service endpoint (JSON, XML) for module security, 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 shippingcontainers 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 module security, 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 usersthe 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.

System Group	Enterprise Application Systems
Business Requirement	Functional Specification
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 invoice or 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-wayAPI 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 accessprotocols 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 following base 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 managing the 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 bebased 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 provideflexibility of infrastructure choice. ▪ The product must support both the SQL and NoSQL APIs under a commonstorage substrate to ensure support for different database services currently and in future ▪ The product must support row-level locking and Multi-Version Concurrency Control

System Group	Data Management and Data Processing System
Business Requirement	Functional Specification
	▪ 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 elastic workloads ▪ 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 asynchronousreplication 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.

System Group	Data Management and Data Processing System
Business Requirement	Functional Specification
	Users ▪ The solution must be able to define and monitor active users duringthe 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 theselection 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 notrunning appropriate container sizeswastage 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 Infrastructuredisruptions

System Group	Data Management and Data Processing System
Business Requirement	Functional Specification
	• 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 servicedisruptions. • The solution must be able todefine 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 and alerts 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 tomonitor 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 tomonitor HBase: o HBase Master Status o Regions in Transition o Master Heap o Region Server Status o Provide region and table levelhot spotting • The solution must be able tomonitor Hive: o Hive Master Status o Metastore Status o Webchat Status • The solution must be able tomonitor Yarn: o Node Manager Status

	○ Resource Manage Heap ○ Containers Status ○ Application Status ○ Cluster Memory ○ Resource consumption trendanalysis and prediction. • The solution must be able tomonitor HDFS: ○ Name node Status ○ Data node Status ○ Disk Usage ○ Block Errors ○ Safe Mode Status HDFS consumption analysisby 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 theability 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 provide data-aware MPP capabilities out ofthe box and should separate metadata from data nodes • The product architecture mustbe 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 tosupport federated queries and have built-in machine learning libraries.

	Multi-tiered Architecture • The solution should have thecapability 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 learningcapabilities • Table storage can beconfigured 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 loadand 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

System Group	Data Management and Data Processing System
Business Requirement	Functional Specification
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-likeformat. 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.

System Group	Data Management and Data Processing System
Business Requirement	**Functional Specification**
	• Must include the multi-tabular display of queries with options for filtering, sorting, searching, and much more. • Must be able to compare table dataacross databases or compare the results of queries. • Must be able to export data in variousformats 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 toperform data profiling, data integration, and data quality via the same interface. ▪ The tool shall support granular role-based security authorization. ▪ The tool shall support version control of ETL flows and should allow rollback to previous versions. ▪ The tool shall support functionality forbreakpoint testing, debugging, and troubleshooting of ETL flows. ▪ The tool shall support varieties of connectors for source and target.

System Group	Data Management and Data Processing System
Business Requirement	Functional Specification
	▪ These connectors shall minimally include: ▪ Relational databases such as Microsoft SQL, MySQL; ▪ In-memory databases such as SAPHANA 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 data encryption 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 asdefining access control. ▪ The tool shall have the capability for ETLjobs scheduling with predefined and customizable scheduling options. ▪ The tool shall provide the capability tosend 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.

System Group	Data Management and Data Processing System
Business Requirement	Functional Specification
	▪ 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 Type 3 compliant HSMs o Key rotation policies from 3-24 months including automatic tracking of data/key pairs o Support encryption of any data type 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 vault must be immutable – data stored cannot be tampered with nor deleted. ▪ The data vaulting platform must be integrated into a PKI (public key infrastructure) to enforce a zero-trust security 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 theoriginal 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 oneportion 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 marking apparatus operatively coupled to the publisher's computer through any appropriate communication bus and/or circuitries. The marking apparatus is preferably arranged to form the set of unique identifiers on any portion of the original entity.

System Group	Data Protection and Security
Business Requirement	Functional Specification
	▪ The system must include a customer computer accessing the server computer system over the communications network.By means of which, a customer who is operating the customer computer is enabled to verify whether an entity of interest is authentic relative to the originalentity as a point of reference or reference point. ▪ The server computer system must be configured to (i) accept from the customer computer a set of unique identifiers of interest formed on the entity of interest having at least one physical identifier of interest, and (ii) determine whether the set of unique identifiers of interest and the at least one physical identifier of interest are associated with one another and exist in the memory system of the server computer system. ▪ The server computer system can be further arranged and/or configured to: (i) if the set of unique identifiers of interest and the at least one physical identifier of interest are associated with one another and exist in the memory system of the server computer system, fetch from the memory system of the server computer system the electronic record of the original entity corresponding to the associated set of unique identifiers of interest and at least one physical identifier of interest existing in the memory system of the server computer system. Any one or more of the tasks in the server computer system, including the fetching step, for example, may be executed by a processor from thememory system of the server computer system. ▪ The server computer system must have features that can be further arranged and/or configured to (i) communicate, over the communications network, with the decentralized computational network using at least one decentralized computational network protocol; and (ii) identify, as one of the one or more nodes in the decentralized computational network, whether the set of unique identifiers of interest carried by the uniquely encrypted message is publishedto the chain of data on the public record-keeping system by decrypting the uniquely encrypted message associated with the fetched electronic record of the original entity using the public key

	associated with the publisher computer which causes the creation of the fetched electronic record of the original entity in the memory system of the computer server system of the one or more aspectsof the data vault system. The server computer system must have features that can be further arranged and/or configured to (vi) if at least a setof unique identifiers of interest is recordedin the chain of data, acquired from the memory system of the server computer system in whole or in part the electronic file of the digital reproduction of the at least one portion of the original entity based on the associated set of the uniqueidentifiers of interest and physical indicia identifier of interest; and (vii) transmit, over the communications network, to the customer computer the acquired electronic file of the digital reproduction of at least one portion of the original entity. ▪ The customer computer must be configured to (i) receive, over the communications network, the transmitted digital reproduction of at least one portionof the original entity associated with the acquired electronic file from the server computer system; and (ii) output on an output unit of the customer computer the received digital reproduction of at least one portion of the original entity.
Cloud Security and Workload Protection	▪ The solution must be a cloud-hosted platform that centrally manages the security "posture" of all "cloud assets" associated with the organization and/or business units. ▪ The solution must provide an additional layer of visibility into the configuration and behavior of workloads, correlated and merged with the cloud security context of those workloads. ▪ The solution must be able to unify security posture management and workload protection activities across cloud accounts, cloud providers, cloud services, geographies, operating systems & more ▪ The solution must automatically detect and correlate workload vulnerabilities throughout the cloud landscape; analyze and report on the complete history of vulnerabilities, risks & remediations. ▪ The solution must establish sensible limits on cloud self-service; Detect violations of

	organizational policy; Customize security incident management workflows as automated responses. ▪ The solution must support allowed and authorized traffic to minimize the attack surface; Prevent threats from spreading laterally through the enterprise; Leverage Machine Learning to automatically build least-privilege policies from actual network traffic. ▪ The solution must collect workload data and support agentless workload monitoring and management ▪ The solution must leverage hundreds of built-in Compliance Checks for AWS, Google cloud, and Azure, able to convert ad-hoc compliance audits into custom reports that span clouds, operating systems, and workload types. ▪ The solution must be able to auto-discover existing infrastructure objects in AWS, Azure, Google Cloud, Kubernetes, OpenStack, etc. ▪ The solution must be able to visualize the infrastructure and data flows for AWS, Azure, Kubernetes, OpenStack, etc. ▪ The solution must be able to view the existing security policies/security groups in AWS, Azure, Kubernetes, OpenStack, etc. ▪ The solution must be able to create ad-hoc queries across security group (i.e., "network policy") rules discovered for AWS, Azure, Kubernetes, OpenStack, etc. to help identify risks ▪ The solution must be able to turn ad-hoc queries against security group rules into custom compliance checks, which – once enabled for a given "group" of compliance assets – run automatically based on a configurable interval. The compliance check results of such user-created custom compliance checks may then be used for one or more purposes, including auto-generation of alerts upon remediation and/or failure events; auto-generation of compliance reports upon compliance scan completion; compliance check results may be searched/audited by Users.

System Group	Data Protection and Security
Business Requirement	Functional Specification
	▪ The solution must be able to schedule the automatic generation of compliance check results reports for viewing and/or download ▪ The solution must support push-button or automatic customer email notifications fornetwork security compliance violation and remediation events in AWS, Azure, Kubernetes, Openstack, etc. ▪ The solution must support push-button or automatic remediation of network security compliance violations in AWS, Azure,Openstack, etc. ▪ The solution must be able to create a time-based exception(s) for any compliance violations. ▪ The solution must be able to cancel exceptions configured for complianceviolations. ▪ The solution must be able to uniquely identify, track, and audit compliance violations. ▪ The solution must support the following Compliance Standard Checks and report for AWS, AZURE, and GCP: CIS Benchmark, GDPR, NIST 800-53 Rev 4,PCI DSS 3.2, HIPAA, HITRUST CSF, CSA IoT Controls. ▪ The solution must support the creation ofCustom Compliance Checks ▪ The solution must support customization of enabled Compliance Checks ▪ The solution must support custom responses to detected Compliance Failures (Risks), including the ability toremediate Risks either automatically or manually (i.e., push-button or offline remediation)

System Group	Data Protection and Security
Business Requirement	Functional Specification
	▪ The solution must detect threats quickly, enabling rapid incident response while also powering historical analysis of forensic data ▪ The solution must standardize and automate the assessment of risks associated with different types of Workloads distributed throughout multipleCloud Providers and/or Cloud Regions ▪ The solution must be able to discover application flows and turn them into appropriate security group rules in AWS,Azure, OpenStack, etc. ▪ The solution must be able to discover and accept recommendations for least- privilege micro-segmentation security group rules for workloads in AWS, Azure,OpenStack, etc. ▪ The solution must be able to roll back accepted recommendations for least- privilege micro-segmentation security group rules for workloads in AWS, Azure,OpenStack, etc. ▪ The solution must be able to create and organize micro-segmentation policies in AWS, Azure, OpenStack, etc., based on aVM's cloud context (application, application tier, VPC, RGs, Projects, etc.) ▪ The solution must identify and deliver least-privilege Security Group policies to newly created VMs/instance-based on VM/instance context such as cloud provider metadata (i.e., VPC, Resource Groups, Projects, etc.) or user-provided tags (i.e., labels). ▪ The solution must monitor the traffic based on security groups and visually identify blocked flows not covered by the policy

System Group	Data Protection and Security
Business Requirement	Functional Specification
	▪ The solution must be able to quarantine a workload after identifying blocked flow that is trying to communicate out to a known threat ▪ The solution must detect and alert on VM instance to VM instance communication that is not allowed. ▪ The solution must allow users to search and export the current inventory of cloud infrastructure assets spanning cloud boundaries such as multiple cloud providers, accounts, regions, etc.; Insteadof limiting cloud visibility to one provider/account/region "in scope" at a time, allow users to search for assets using cloud attributes as filters and/or ignoring cloud attributes for inventory audits spanning cloud providers, accounts, regions, services, etc. ▪ The solution must allow users to search and export the historical record of discovered cloud infrastructure assets, including the specific ability to filter/search for in-scope assets that were "created" and/or "deleted" within a given period. ▪ The solution must allow users to search and export the historical record of compliance check results for all managed/scanned Assets, including the specific ability to filter/search for in-scope compliance check results from a given period to provide proof of continuous compliance over an extended period and/or to allow for historical audits of compliance policy adherence.

System Group	Data Protection and Security
Business Requirement	Functional Specification
Endpoint Protection and Response	▪ The solution must support Endpoint and Detection Response capabilities that include a controller/console that should be hosted in the cloud. The solution should have as part of the platform an End Point solution that allows for detection, validation, and containment. ▪ All functionalities must work on or off the corporate network and without a requirement for VPN back to the corporate network ▪ The solution must block common malware with a signature-based engine, stop advanced threats with the machine learning engine, halt application exploits with the behavior analysis engine, and be able to protect from new threat vectors with Endpoint Security Modules. ▪ The solution should support the investigationof lateral movement within Windows and Linux machines, aggregating historical activity and monitoring new activity. The solution should support a user interface designed for analyzing investigative leads (e.g., a compromised account) and hunting for suspicious activity (e.g., RDP activity by privileged accounts). ▪ The solution should support insights into detected malware, server scheduled scan(s) summary events, quarantined items, and agent version information. End users can also optionally manage the quarantined items. ▪ The solution should support host remediation allowing administrators to remotely connect to endpoints and execute commands for remediation. The controller should securely communicate to agents using mutual TLS v1.2 and AEAD mode cipher. This eliminates the need to configure any additional firewall rules or ports for the module to be able toperform normal operations. ▪ The solution should recognize unique file executions on an endpoint and report these executions. The solution should be able to enrich all process execution events utilizing the standard workflow andstandard triage collection will initiate automatically on the endpoint associated with the alert. ▪ The solution must be able to detect advanced attacks using proactive and real-time Threat Intelligence. ▪ The solution must provide continuousdetection

	and response activities for advanced threats. (e.g., should not require scheduling) ▪ The solution must be able to push out new upgrade versions of the endpointagent ▪ Endpoint agents must be able to be controlled on and off the corporate network for detection, triage, and containment ▪ Endpoint solution must be able to take asinputs custom indicators of compromise ▪ The solution must provide an easy-to-use interface and require no more than an entry-level SOC analyst and/or IR responder skillset to operate. ▪ In assisting with an investigation, the agent can remotely send memory dumps, files, running processes, services, drivers, DLLs, open handles, and network information. ▪ The solution must have an intelligence-sharing network, where information learned about APT and Advanced Malware can be shared across the vendor's customer base ▪ The endpoint agent should be able to detect previously unrecognized exploits and other online attacks, commonly known as zero-day attacks. ▪ The endpoint agent should be able to monitor common applications for specific exploit behaviors, including Adobe Reader, Adobe Flash, Internet Explorer, Mozilla Firefox, Google Chrome, Java, Microsoft Word, Microsoft Excel, and Microsoft PowerPoint. ▪ When an exploit is detected on a host endpoint, an alert should be triggered, and the detection details submitted to the Controller. ▪ The solution must be able to learn about Zero-day and other advanced threats from security platforms performing behavioral analysis using a virtual execution environment. ▪ The solution must be able to continuously learn about new security content from its threat intelligence. ▪ The solution must have a two-stage process for containment requests, with the ability to separate the requestor and approver roles. ▪ The solution must be able to remotely acquire files and other triage information for investigation purposes. Triage data must include exploiting detection information. ▪ The solution must offer a built-in graphical triage viewer to ease security operations.

	▪ The solution must be able to differentiate between presence and the execution of the indicators of compromise.

System Group	Data Protection and Security
Business Requirement	Functional Specification
	▪ The endpoint agents must support detection, triage, and containment both on and off the corporate network, without a requirement for VPN back to the corporate network. ▪ The solution must allow the grouping of endpoints into host sets based on distinguishing attributes. It must also be able to identify and label high-value hosts.
Threat Analytics	▪ The solution must be a cloud-hosted Threat Analytics Platform that provides native security detection and analytics module, entity-based alert correlation uses machine learning to identify normal behavior and alert on risky deviations that suggest insider threats, lateral movement, or attacks at the end stages of the cyber kill-chain. ▪ The Threat Analytics service must support the events/logs from the existing security solution to include the FW, WAF,DDOS solution, EPP/EDR, cloud securityposture management, etc. ▪ The solution must collect data from across on-prem or cloud environments and analyze billions of data points for both known and unknown attacker indicators. The solution must use machine learning and statistical methods to baseline an organization's 'normal' behavior. It then uses mathematical predictions to calculate the risk of deviantactions and create alerts. ▪ The Threat Analytics platform solution must include Endpoint Forensic solution that will be installed across all supported servers. The endpoint forensic solution must be fully integrated with the Threat Analytics platform for quick host containment and investigation. ▪ The Threat Analytics platform solution must support a Web GUI portal that is 99.9% available during each calendar month. ▪ The proposed solution must use machine learning and artificial intelligence to baseline your organization's 'normal' behavior and create alerts when anomalies and deviations occur. ▪ The proposed solution must have an extensive set of threat detection rules managed by the vendor ▪ and updated daily based on the vendor's strong

	threat intelligence data acquisition capabilities. ▪ The proposed solution must have Integrated real-time threat intelligence and customizable threat detections to facilitate sub-second searches to detect multi-vector, non-malware-based threats. ▪ The proposed solution must be able to send email notifications when the average events per second (EPS) exceeds the subscribed EPS during the past hour. ▪ The proposed solution must support the emailing of reports as password protected. ▪ PDF files. When scheduling a custom dashboard report, it must provide the option of emailing a password-protected PDF to a list of subscribers. Password protection uses a custom password, and the reports can be delivered to a specific recipient. ▪ The proposed solution must support a native chat icon/window for Customer Support, gaining expedited access to the specific product expert for any technical concerns or issues. ▪ The Solution must support predefined or custom dashboards and widgets to visually aggregate, present, and explore the most important information to a user while meeting compliance requirements. ▪ The solution must support role-based access control: the creation of role-based groups and assigning granular permissions to access the console. ▪ The solution must support full index and archive search against alerts and event data from all sources across the infrastructure to support flexible pivoting and fast hunting. ▪ The solution must support open and flexible APIs for integration into 3rd party products, and seamless embedding into customer environments. ▪ The solution must include detection rules and context from the vendor's threat intelligence ▪ The solution must support case/workflow management to organize, assign, collaborate and action steps through the investigative process through automated and manual workflows. ▪ The solution must support automatically coalesce related data to help drive faster decisions, including context across intelligence, alerts, host and user data ▪ The solution must support central management and configurations, policies/health status across all the sensors for email, endpoint, and network

	▪ The solution must automate and accelerate the investigative and response process via product integrations and defined actions for specific alerts. ▪ The solution must be a cloud-hosted unified console that supports threat intelligence, orchestration, security analytics, device policy configuration of the proposed network sensor deployed at the customer's premise. ▪ The solution must support rapid detection of the threats that matter to the organization by using analytics, machine learning, and threat intelligence ▪ The solution must be able to prioritize alerts by highlighting those that pose the greatest risk to the organization ▪ The solution must support broad types/kinds of devices for any log sources ▪ The solution must support detection and analytics rulesets focus on threats unique to the cloud environments ▪ The solution must support third-party alerts and logs, investigative workflows, searches, and analysis of possible malware on a single pane of glass ▪ The solution must support Single Sign-On (SSO) user authentication for all its component's endpoint security, network security, and threat analytics ▪ The solution must combine network metadata and alerts from across the security infrastructure and delivers them to a unified console ▪ The solutions must support full index search, archive search, and malware analysis against alerts and event data from all sources across the infrastructure. ▪ The solution must provide visibility into known and unknown threats by combining network and endpoint detection with a unified console that centralizes alerts from the rest of an organization's security infrastructure. ▪ The solution must provide intelligence with context to simplify threat alert monitoring, triage, and investigation ▪ The solution must include rule sets that created and constantly updated by the vendor ▪ The solution must have capabilities to monitor and notify the end-user if the log ingestion stops ▪ The solution must have capabilities to monitor and notify the end-user if the Log ingestion spikes per event class ▪ The solution must have capabilities to monitor and notify the end-user if the Log ingestion deviates

	from a baseline per event class ▪ The solution must support behavioral analytics to identify threats by analyzing user behavior – identifying risky entities and protecting organizations from insider threats, lateral movement, and other common cloud risks. The solution must implement machine learning to establish baseline behavior and alert to risky deviations. ▪ The solution must analyze organizational-level assets (or entities) such as users and hosts to identify potential insider threats. This detects behavior anomalies by these assets, creates detections, and alerts the system immediately. ▪ The solution must have native investigative tips providing a series of next steps for investigating an alert ▪ The solution must have native case management allowing to view, create, manage and assign cases.

System Group	Reports and Analytics System
Business Requirement	**Functional Specification**
Executive Dashboard	▪ Must be able to readily combine at least 4 visualizations templates in a single dashboard ▪ Must provide an option to include controlsto adjust parameters of the visualizations included in the dashboard ▪ Must provide the ability to embed or provision permalinks of dashboard/sthrough: ▪ Snapshot URL ▪ Shortened Snapshot URL
	▪ Must provide users the ability for them to be able to download the dashboard/s as afile with type: o .pdf o .png

Report Visualization Templates	▪ Must provide this selection of visualization templates: o Charts or Graphs o Pie o Bar o Horizontal o Vertical o Line o Maps o Coordinate o Heat o Any type which can localize its view to street-level roads and addinsight layers o Others o Data Table o Word Clouds o Gauge ▪ Must provide controls to adjust the parameters of a visualization. This includes an aggregation of different charts or graphs into a single visualization ▪ Must provide the ability to embed or provision permalinks of visualizationsthrough: o Snapshot URL o Shortened Snapshot URL ▪ Must provide users the ability for them tobe able to download the visualizations asfiles with type: o .pdf file o .png file
Data Streaming Engine	▪ Must be able to collect and parse thesetypes of logs from different log sources: o access o error o slow o debug o system o transaction ▪ Must be able to connect data sources via: ▪ Static IP addresses ▪ ReST API web service endpoints ▪ Must provide the ability to configure dataretention policies

System Group	Reports and Analytics System
Business Requirement	**Functional Specification**
Risk Profiling Reports	▪ Must be able to automatically detect and alert anomalies in logs using predetermined thresholds ▪ Must have machine learning capabilities to analyze logs ▪ Must provide the ability to combine different logs and/or reports into a single dashboard ▪ Must provide the ability to embed or provision permalinks of the reports through: o Snapshot URL o Shortened Snapshot URL ▪ Must provide users the ability for them to be able to download the reports as files with type: o .pdf file o .png file
Standard Reports	▪ Must be able to provide at least 1 dashboard, with at least 4 reports, that is viewable by all types of users ▪ The dashboard above must be able to immediately reflect changes by users with proper credentials in its visualizations

System Group	Development and Deployment Platform
Business Requirement	**Functional Specification**
Infrastructure	▪ The development and deployment platform must be able to run both in a private data center or a public infrastructure-as-a-service provider. It must support running on top of public infrastructure-as-a-service environments such as AWS, Google Cloud Platform, Microsoft Azure, and the following private infrastructure-as-a-service environments such as vSphere or OpenStack. ▪ The platform must be infrastructure aware and, therefore must provide natively detect underlying infrastructure (VMs) failure and self-heal without human intervention. ▪ The platform must support multiple availability zones deployment architecture to allow application continuity during catastrophic availability zone failure.

System Group	Development and Deployment Platform
Business Requirement	**Functional Specification**
Architecture	▪ The platform must embrace microservices and cloud-native principles in its product architecture. The architecture must enable the system to scale required components of the platform on-demand, rather than scale all components of the platform. ▪ The platform must support injecting environment variables (or service credentials) into application instances during deployment runtime to influence the application behavior during deployment time, and without changing any configuration or application code. ▪ The platform must allow zero downtime application upgrade from one version to another. Upgrade techniques like A/B Testing, Blue/Green deployment must be well supported. ▪ The platform must provide enterprise support for the underlying enterprise Linux and middleware being used without any additional licensing charges.
Administration and Performance Management	▪ The platform must provide a web browser-accessible console for operators to manage the underlying system, infrastructure (VMs), and resources, and developers to view and take actions on applications (scale, log, bind service, delete, application health, performance monitoring) and service marketplace (create service, delete service, manage service, bind service). ▪ The platform must allow operators to logically segment/separate physical resources into multiple organizations (or projects). Each organization then must be able to accommodate further logical separations based on each stage of the application lifecycle (like develop, stage, test, etc.) ▪ The platform must natively support running one-off tasks (like database migration, batch jobs) periodically. The entire lifecycle management of these tasks (like provision, patching, security, upgrades) must be handled by the platform. ▪ The platform must have built-in application performance management outlining key performance metrics of application instances in real-time. The platform must support at least the following metrics:

System Group	Development and Deployment Platform
Business Requirement	Functional Specification
	○ Network metrics (HTTP requests for an application, HTTP request errors for an application with a latency of 1second) ○ Container metrics (CPU, disk, and memory utilization) ○ Container-related events metrics (create a container, update container, start container, stop container,crashed container). ▪ The platform must support JMX monitoring and allow feeding performance metrics to systems running outside of the platform. ▪ The platform shall support integration withpopular third-party performance management tools (not limited to New Relic, AppDynamics only) for deep application performance management. Developers must be able to bind to these services easily while deploying their application code to the platform. ▪ The platform must support storing and retrieving information related to application-related events (like but not limited to following - create application instance, delete application instance, application resource usage, etc.) so that appropriate billing could be done for platform users. ▪ The platform must support integrated performance metrics with application/platform logs out of the box.Operators must be able to correlate performance spikes with the application logs for a selected interval.

System Group	Development and Deployment Platform
Business Requirement	Functional Specification
	▪ The platform must support managing spring framework-based applications (microservices) via configuration server, service registry, and circuit breaker services. These services must be deployed and managed (patching, upgrades, security upgrades, failures) byplatform.

Build and Code Compilation	▪ The platform must natively support the process of building and compiling application code every time application code is deployed on the platform to eliminate all the time spent on configuring servers, middleware, or creating container images. ▪ The platform must automatically detect what type of application is deployed, compile it with relevant runtime components, and bind it to services like databases, eliminating the time-consuming and complex steps for developers and operators to configure. ▪ The platform must standardize detection, compilation, and deployment of application code written in any of the following languages – PHP, Spring, Play, Scala, Java, Grails, Rails, Ruby, Go, .NET, Groovy, Python, and NodeJS.
Code Containerization	▪ Application instance must run in a container when application code is deployed on the platform. Container deployment is a must for improving infrastructure utilization and faster horizontal scalability needs.
Platform Independence	▪ The platform must be open source so that modifications to an artifact (like component used for application compilation, code/plugins dependencies detection and download, and middleware runtime selection) could be done in an event that the current artifact from a third-party vendor is inoperable.
Self-Healing and Scalability	▪ The platform must identify application instance failure automatically and self-heal the instance without any human intervention. Upon self-healed application instance, the platform must restore any service binding that was applied before failure. ▪ The platform must scale (out and in) application instances upon increasing traffic (spikes) without human intervention. The platform must handle dynamic routing and load balancing out of the box upon scaling. ▪ The platform must be able to upgrade/patch itself from one version to another with zero downtime and shall not affect (or minimally) applications running on the platform. Vendor must show a track record on version upgrade from earlier major version to latest version without requiring a completely new setup

System Group	Development and Deployment Platform
Business Requirement	**Functional Specification**
Logging	▪ The platform must allow streaming consolidated logs (like application log, middleware log, platform components related logs) for all instances of an application and platform components witha simple command-line statement. Logs must also be shown on graphical UI. ▪ The platform must allow searching andfiltering logs via the web console.
Lifecycle Management	▪ The platform must natively support data microservices to extract, transform and load data from one system to another via streaming pipelines. The entire lifecycle management of the streaming microservices (like provision, patching, security, upgrades) must be handled by the platform. ▪ The platform must support running DevOps tools (like build tools, source code repository, etc.) natively on the platform. The entire lifecycle management of these tools (like provisioning, patching, upgrades, high availability, fault-tolerance, etc.) must be managed by the platform. ▪ The platform shall support mobile services like push notification and mobile

System Group	Development and Deployment Platform
Business Requirement	**Functional Specification**
	development and collaboration as a service on the underlying infrastructure used by the platform. The entire lifecycle management of these tools (like provisioning, patching, upgrade, high availability, fault-tolerance, etc.) must bemanaged by the platform.

Technical Environment and Infrastructure Specifications

System Group	Turnkey Environment for Tracking Devices and Communications Network
Business Requirement	**Functional Specification**
Industry Standards	▪ Compliance to International Cellular Communications Standards; 3GPP Release 14 and above
Radio Access Network Air Interface Specification Standard	▪ The radio interface must support GPRS,LTEm, or nbloT
Radio Access Network Base StationSpecification	▪ The system must be compatible with allcarriers on the nationwide cellular data network. ▪ Minimum requirement is carrier support for GPRS (2G) Data connections ▪ Preferred radio requirements are to support3GPP R14 and above.
Radio Interface	▪ System must support all national frequencies used in the Philippines, specifically GSM 900, 1800, LTE Band28, Band 3
Backhaul Connectivity	▪ The solution must support VPN tunnelingbetween the gateway and the Network Server. ▪ The solution must provide a system to monitor the KPI's and performance of the backhaul connectivity.
System Group	Turnkey Environment for Tracking Devices and Communications Network
Business Requirement	**Functional Specification**
	▪ The solution must be equipped with failover mechanisms for the backhaulconnectivity. ▪ The solution must support IPv6standards. ▪ The must support buffering and gracefulrecovery in the event of backhaul unavailability or failure.
Geo-Location Support	▪ Support for multiple GNSS Standards; GPS/BeiDou/Galileo/GLONASS ▪ Support for Wi-Fi Geo-location ▪ Support for GSM Geo-location

Gateway Appliance Specifications	▪ The system must use pre-existing infrastructure
Device and Network Management	▪ The solution must be able to allow and bar endpoints from the network. ▪ The solution must be able to manage an endpoint's data usage including the ability to disable a unit that is consuming too much bandwidth ▪ The solution must be able to remotelyupdate an endpoint's configuration via the radio interface and backhaul ▪ The solution must be able to remotely update an endpoint's firmware via the radio interface and backhaul ▪ The solution must be able to remotely addand remove features on endpoints. ▪ The solution must be able to provide bandwidth/airtime usage for each endpoint.
Network Server and Communication Services	▪ The solution must have the capability to implement service provider traffic policiesthrough connectivity profiles allocated to devices.

System Group	Turnkey Environment for Tracking Devices and Communications Network
Business Requirement	Functional Specification
	▪ The solution must provide high-availability mechanisms for its network server services, support active/active redundancy, and geo-redundancy. ▪ The network server must support bidirectional message routing to/from 3rd party applications using HTTPS-based REST API. ▪ The solution must provide off-the-shelf connectors to major IoT cloud platforms (e.g., AWS). ▪ The solution must support bi-directionality support, multi-protocol & authentication modes, provisioning lifecycle for devices.

System Group	Turnkey Environment for Tracking Devices and Communications Network
Business Requirement	Functional Specification
Device Provisioning, Monitoring, and Management	▪ The solution must provide tools to ensure the provisioning of devices via a web interface – unitary & mass provisioning orvia REST APIs. ▪ The solution must support ABP and OTAA activation protocols and methods ▪ The solution must provide all necessary management applications for Device Administration, Device Monitoring (status and performance), Traffic Analysis, and Map Visualization
Base Station Provisioning, Monitoring,and Management	▪ The solution must provide tools to ensure the provisioning of base stations via web interface – unitary & mass provisioning, orvia REST APIs. ▪ The solution provides all necessary management applications for Network Access, Configuration, and Firmware Upgrades, Map Visualization, Performance Dashboard ▪ The solution must provide tools that detect/provide data to improve networkcoverage and quality of service.
Security: Device	▪ The solution must employ FCC & PTCRB -certified devices that use 3GPP standards for Secure Computing Platform trusted by global cellular networks, i.e., two unique unchangeable serial numbersfor identification and security: 1. The 15-digit IMEI burnt into the Cellular Module by Thales at the manufacturing stage 2. SIMs 20-digit ICCID burnt into the SIM by Thales at the manufacturing stage. ▪ Firmware must be locked in device memory and cannot be read from the device even with physical access to thedevice. ▪ When devices are manufactured, they must register the correct IMEI/ICCID topair it with the platform system when provisioning.

System Group	Turnkey Environment for Tracking Devices and Communications Network
Business Requirement	**Functional Specification**
	▪ Device can generate an encryption key that can be used for higher-level securitypurposes
Security: Cellular Network	▪ The solution must operate its own private APN (Access Point Name) and virtual network using 3GPP encryption and security techniques to provide a global private network. ▪ All devices on the network must contain valid SIM and module security permissions. ▪ Only authenticated sessions are permitted on the APN and devices can be remotely disabled or suspended by the SIM control center. The solution must provide an IPsec VPN Tunnel between Private APN and platform to ensure only devices controlledby the platform can access the platform.
Security: Platform API	▪ The platform must contain two major interfaces: the Web Console (browser-based system) and the Portal API (JSON-based interface that enables direct communication with 3rd Party systems). ▪ The platform must maintain an immutable event store. ▪ The platform must contain Authorized and Encrypted Endpoints. ▪ API access and authentication much be performed using OAuth2 over SSL (TLS)connections. ▪ RSA 256 signed token must be available for additional timed authentication. ▪ Access to the Web Console must be standard security (SSL) for establishing encrypted links between web servers and browsers.

System Group	Turnkey Environment for Tracking Devices and Communications Network
Business Requirement	Functional Specification
Security: Cloud	▪ Development & Releases must adhere to strict testing schedules that do not affect operations. ▪ All ingress points must be globally diverse and deployed in multiple regions and availability zones with high- availability and active redundancy. ▪ Web Application Firewalls must be compliant with the latest OWSAP standards and suspicious requests automatically logged and reviewed. ▪ Must support TLS 1.2 upwards with elliptical curve cryptography. ▪ All data including backup data must always be stored in an encrypted format. ▪ The platform must contain strict identity and access management policies. ▪ Strict container rules must be applied so no container can talk to another container. ▪ Only worker containers can write to the database (event store). ▪ Only API containers can write to the web database (web store). ▪ No shell access permitted. ▪ All containers must log to centralized logging services.

System Group	Turnkey Environment for Tracking Devices and Communications Network
Business Requirement	Functional Specification
The device, Network, and Protocol Management:	▪ The system must support 3GPP Release 13/14 and 5G with LTE enhancements for Machine-Type Communications. ▪ The solution must support:

	1. Global LTE-M and NB-IoT connectivity across all available FDD-LTE Bands 1, 2, 3, 4, 5, 8, 12, 13, 18,19, 20, 25, 26, 27, 28, 66, 71, 85. 2. The solution must also support quad-band GSM:850, 900, 1800, 1900 MHz support 3. The solution must support integrated GNSS (GPS/BeiDou/Galileo/GLONASS). 4. The solution must support control via standard commands and proprietary AT Commands. 5. The system must support embedded IPv4/6 TCP/IP stack + TCP/UDP client/endpoint, HTTP client, FTP Client, MQTT Client, and CoAP Client. 6. The solution must support 2G Fallback.
System Group	Turnkey Environment for Tracking Devices and Communications Network
Business Requirement	Functional Specification
Platform User Accounts	▪ The solution must contain user application in JSON form: o Numerical ID, the username (always email address), first & last name, details of customer user/organization user is affiliated with, timestamp of user creation, timestamp of user modification. o The solution must support old password subject to change, new password assigned to a user account, password confirmation with matching values with standard responses in the event of successful change, or 400 invalid request parameters and validation errors.

OAuth2 Applications	▪ All users must be able to create and manage OAuth2 applications to enableAPI access for 3rd party applications. ▪ Must support OAuth2 authorization flowswith valid tokens for API authentication. ▪ Client credentials must be supported formachine-to-machine authentication where client ID & secret are secure.
Configurations & Firmware	▪ The solution must support OTA (Over the Air) configuration and firmware updates that can override device parameters such as reporting schedules, temperature logging intervals, or shock threshold values. ▪ The solution must support configuration applications via device groups and assign custom configurations for all devices in a group. ▪ The solution configurations are to be managed in the draft and published states and only draft configurations may be

System Group	Turnkey Environment for Tracking Devices and Communications Network
Business Requirement	**Functional Specification**
	edited – however, published and read-only configurations may be assigned todevise groups. ▪ The configurations must support queries and multiple filters against a set of filtering criteria to allow fine-grained control for results – all executed based onquery-string parameters ▪ The system must support partial update configurations through ID, delete configuration, and configurationpublishing.
Device Management (in the fieldand server-side)	▪ The solution must provide bi-directional support for uplink/downlink event packet, configuration, and firmware communications. ▪ The solution must provide device operations support queries and multiple filters against a set of filtering criteria to allow fine-grained control for results – all executed based on query-string parameters. ▪ Device ordering and query parameter fields must facilitate orderable fields (imei,mac,last_event_timestamp) & search via imie, mac, fault, group ID, radios, latitude, longitude, geogroup_inside, geogroup_outside, geogroup_distance.

	▪ Devices must have the capacity to maintain historical events stored within the device memory, including IMEI ID of reporting device, approximated location, battery levels, temperature, and shock values.

System Group	Turnkey Environment for Tracking Devices and Communications Network
Business Requirement	Functional Specification
	The device must publish its position accuracy with timestamp via the following: o 0-location determined withmarker o 1- location determined withGPS o 2- location determined withcell towers o 3-location determined with Wi-Fi proximity o 5-unknown location
	▪ The solution must support device groups for logically grouping devices in the system, to apply settings to a setof devices, such as configuration changes or requested webhook processing settings. ▪ The solution must provide the necessary management applications for: o device group listing o device group creation o device group details o device group updating o device group partial update o device group deleting o adding devices to device groups o removing devices from devicegroups ▪ The solution must support device tagging to logically tag devices in a tree-like structure, whereby each device can belong to one or more tags so tags can overlap. The solution must support tag querying and multiple filters against a set of filtering criteria to allow fine-grained control for results – all executed based on query-string parameters

System Group	Turnkey Environment for Tracking Devices and Communications Network
Business Requirement	Functional Specification
	▪ The solution must provide the necessary management applications for: o device tag creation o device tag listing in a tree structure o device tag details o device tag updating o device tag partial update o device tag delete o device tag add o device tag removal ▪ The solution must support geo-group querying and multiple filters against a set of filtering criteria to allow fine-grained control for results – all executed based on query-string parameters. ▪ The solution must provide the necessary management application for: o device geo-group creation o device geo-group listing o device geo-group details o device geo-group updating o device geo-group partial update o device geo-group delete o device geo-group add o device geo-group removal

System Group	Turnkey Environment for Tracking Devices and Communications Network
Business Requirement	Functional Specification
Systems Integrations	▪ The solution must provide API endpoints to allow querying and manipulation of enabled 3rd party systems integrations. ▪ The solution must enable integrations with external systems to execute actions with external systems as soon as the event from monitored/connected devices has been registered. ▪ The solution must support mapping between devices and integrations throughgroups & tags so that device event processing with external systems is matched with enabled integrations

	for authorized devices. ▪ Each system integration requires the capacity to have multiple device groups and tags assigned to it. ▪ Integrations can be enabled and disabled. ▪ The solution must provide Webhook integrations that post full event data to the given HTTP endpoint of external integrations. ▪ The solution needs to keep the worker payload consistent with the response containing event details. ▪ The solution must provide the necessary management application for: o system integration creation o system integration listing o system integration details o system integration updating o system integration partial update o system integration delete o system integration add o system integration removal

System Group	Cloud-Based High-Performance Computing Server
Business Requirement	**Functional Specification**
Physical Footprint	▪ High-performance computing server mustbe a secure and dedicated cloud-based service

Server Processing and Architecture	▪ Server must allow concurrent addition of processor core ▪ Server must have an on-chip accelerator for compression ▪ Server must have a dedicated core co-processor for encryption ▪ Server must support up to 40TB of te redundant memory feature ▪ Server must support open standards andtool across all cloud consumption models ▪ Server must support leading open-source databases, runtimes, languages, and tools ▪ Server must be scalable, robust, andefficient ▪ Server must have the core sparing capability ▪ Server must have ASHRAE Class A3design ▪ Server must support on-demand activation and deactivation of capacity ▪ Server must support capacity backup for disaster recovery ▪ Server must support concurrent repair of drawer & concurrent install of all I/O features (hot plug)
Performance and Caching	▪ Server must have dedicated cores for I/O processing that do not factor into SW licensing. ▪ Server must have 4 levels of cache ▪ Server must have raw I/O bandwidth ofup to 1152 GBPS theoretical maximum
Security	▪ Server must have a highly rated hardware security module(HSM) certified at FIPS140-2 level 4. ▪ Server must support logical partitioning (LPAR) with EAL5+ certification for air-gap isolation ▪ Server must allow sharing of resources across LPARs
Data Protection	▪ Server must support encryption of data-at-rest and data-in-flight using hardware-based technology

System Group	Cloud-Based High-Performance Computing Server
Business Requirement	Functional Specification
	▪ Server must-have the capability for bringingup highly secured operating enclaves ▪ Server must support 2TB memory for a single VM instance to run an open-source database without sharding.

Warranty and Support	▪ Server must have at least a 1-year warranty covering parts and service for 24 x 7 support. ▪ Server must have an option for succeeding hardware maintenance afterwarranty.

System Group	On-Premise Backup and Enterprise Storage System
Business Requirement	Functional Specification
Architecture, Performance, and Flexibility	▪ The storage should offer both hybrid andall-flash array deployment ▪ The storage should be modular and must have a scalable 19-inch frame that can beupgraded by adding an additional expansion enclosure ▪ The storage must have a fully redundant canister and power supply ▪ The storage must support mix and matchhost adapter cards ▪ The storage must support industry standards NVMe drives, Flash Core Modules or Storage Class Memory drives ▪ The storage must support Distributed RAID1/RAID5/RAID6 deployment ▪ The storage should support industry-leading data services such as dynamic tiering, flash copy management, data mobility, and high-performance data encryption ▪ The storage must support innovative data reduction pool (DRP) technology that includes deduplication and hardware-accelerated compression technology ▪ The storage must support FIPS 140-2Level1 encryption with centralized keymanagement ▪ The storage should support both internaland external virtualization functionality ▪ The storage should have the ability to cluster, and support scale-out or scale-updeployment ▪ The storage must be capable of migratingor replicating data between on-premise hardware deployment and into public cloud storage

System Group	On-Premise Backup and Enterprise Storage System
Business Requirement	Functional Specification
High-Availability and Disaster Recovery	▯ The storage must be able to provide a High Availability Solution (Active-Active capable) ▯ The storage must be capable of supporting a Disaster Recovery setup (2- site or 3-site replication)

Management and Reporting	▪ The storage must utilize a modern userinterface for centralized management ▪ The storage management should provide a single dashboard to see the status of the storage at a glance ▪ The storage management should gather telemetry approximately 23 million data points for better and more informed decisions
Support and Maintenance	▪ The storage should have enterprise class support for improved support response times. ▪ 24 x 7 x 365 technical support (remoteaccess)

System Group	Network, and Application Security Appliance
Business Requirement	**Functional Specification**
Network Management Router	▪ TACACS+, RADIUS, local, role-based access control ▪ OSPF, external BGP (eBGP), internal BGP (iBGP), EIGRP, ECMP, static, connected, OMP ▪ 802.1Q, native VLAN, bridge domains, Integrated Routing and Bridging (IRB), host-mode bridging ▪ Built-in security: Intrusion prevention system, web security, enterprise firewall, Malware Defense, Next-Generation Antivirus (NGAV), URL filtering, and SSL inspection ▪ Cloud security – Web security with SSL proxy, DNS-layer enforcement, URL filtering, Cloud Access Security Broker (CASB), and enterprise firewalls. ▪ Device- and network-level security: Zero trust, segmentation, whitelisting, tamper-proof module, Datagram Transport Layer Security (DTLS)/TLS, IPsec, ESP-256-CBC, authentication header, HMAC-SHA1, distributed denial-of-service (DDoS) protection, control plane protection, Network Address Translation (NAT) traversal ▪ SIP, Public Switched Telephone Network (PSTN) voice and fax support, Survivable Remote Site Telephony (SRST), 911 calling, conferencing

	▪ FEC and packet duplication for User Datagram Protocol (UDP), TCP optimization, Cloud OnRamp optimization for SaaS applications ▪ Public cloud integrations into AWS, Azure, and Google Cloud Cloud OnRamp optimization for SaaS applications ▪ Cloud OnRamp for Colocation ▪ Classification, prioritization, low latency queuing, remarking, shaping, scheduling, policing, mirroring, NAT/Port Address Translation (PAT) ▪ Internet Group Management Protocol (IGMP) v1/v2/v3, Protocol Independent Multicast (PIM), Auto-RP, scale-out traffic replication ▪ Route policies, app-aware routing, control policy, data policy, Access Control List (ACL) policy, VPN membership policy ▪ Route policies, app-aware routing, control policy, data policy, ACL policy, VPN membership policy ▪ Integrated 4G/LTE modem on some devices ▪ Wi-Fi 802.11a/b/g/n/ac, WPA2-Enterprise, WPA2-Personal, MAC filtering, 8 SSIDs per radio, 802.11i security enhancement and 802.11e QoS, wireless intrusion detection and protection ▪ IPv4, Simple Network Management Protocol (SNMP), Network Time Protocol (NTP), DNS client, Dynamic Host Configuration Protocol (DHCP) client, DHCP server, DHCP relay, configuration archival, Syslog, Secure Shell (SSH), Secure Copy (SCP), NAT/PAT, Cflowd v10 IPFIX export ▪ NETCONF over SSH, Command-Line Interface (CLI), REST (vManage), Linux shell

System Group	Network, and Application Security Appliance
Business Requirement	Functional Specification
Network Switches	▪ Up to 48 ports of full Power over EthernetPlus (PoE+) capability ▪ Resiliency with Field-Replaceable Units (FRU) and redundant power supply, fans,and modular uplinks ▪ Flexible downlink options with data, PoE+ or

System Group	Network, and Application Security Appliance
Business Requirement	Functional Specification
	mGig ▪ Operational efficiency with optional backplane stacking, supporting stackingbandwidth up to 160 Gbps ▪ UADP 2.0 Mini with integrated CPU offers customers optimized scale with the better cost structure ▪ Enhanced security with AES-128 MACsec encryption, policy-based segmentation, and trustworthy systems ▪ Layer 3 capabilities, including OSPF, EIGRP, ISIS, RIP, and routed access ▪ Advanced network monitoring using Full Flexible NetFlow ▪ Software-Defined Access (SD-Access): ▪ Simplified operations and deployment with policy-based automation from edge to cloud-managed with ▪ Identity Services Engine (ISE) ▪ Network assurance and improved resolution time ▪ Plug and Play (PnP) enabled: A simple, secure, unified, and integrated offering to ease new branch or campus device rollouts or updates to an existing network ▪ Support for model-driven programmability and streaming telemetry ▪ ASIC with programmable pipeline and micro-engine capabilities, along with the template-based, configurable allocation of Layer 2 and Layer 3 forwarding, Access Control Lists (ACLs), and Quality of Service (QoS) entries

System Group	Network, and Application Security Appliance
Business Requirement	**Functional Specification**
Core and Aggregation Layer Switches	▪ Ready for next-generation technologieswith its programmable pipeline, micro engine capabilities, and template-based, configurable allocation of Layer 2and Layer 3 forwarding, Access Control Lists (ACLs), and Quality-of-Service (QoS) entries ▪ 2.4-GHz x86 CPU with up to 120 GB of USB 3.0 or up to 960 GB of SATASSD storage for container-based application hosting ▪ Up to 6.4-Tbps switching capacity with upto 2 Bpps of forwarding performance ▪ Up to 32 nonblocking 100 Gigabit Ethernet QSFP28 ports ▪ Up to 32 nonblocking 40 Gigabit Ethernet QSFP+ ports ▪ Up to 48 nonblocking 25 Gigabit EthernetSFP28 ports ▪ Up to 48 nonblocking 10 Gigabit EthernetSFP+ ports

System Group	Network, and Application Security Appliance
Business Requirement	**Functional Specification**
Core and Aggregation Layer Switches	▪ Platinum-rated AC/DC power supplies ▪ Up to 512,000 Flexible NetFlow (FNF)entries in hardware ▪ Up to 36 MB of unified buffer per ASIC ▪ Up to 212,000 routing entries (IPv4/IPv6) for high-end campus core and aggregation deployments ▪ IPv6 support in hardware, providing wire-rate forwarding for IPv6 networks ▪ IEEE 802.1ba AV Bridging (AVB) built in to provide a better AV experience through improved time synchronization and QoS ▪ Precision Time Protocol (PTP; IEEE 1588v2) provides accurate clock synchronization with sub-microsecondaccuracy, making it suitable for distribution and synchronization of time and frequency over the network ▪ Dual-stack support for IPv4/IPv6 and dynamic hardware forwarding table allocations, for ease of IPv4- to-IPv6 migration ▪ Support for both static and dynamic NATand Port Address Translation (PAT) ▪ Scalable routing (IPv4, IPv6, and multicast) tables and Layer 2 tables

	▪ Modern operating system for the enterprise with support for model-driven programmability, on-box Python scripting, streaming telemetry, container-based application hosting, and patching for critical bug fixes. The OS also has built-in defenses to protect against runtime attacks ▪ Network system virtualization technology that increases operational efficiency and boosts nonstop communications and scaled system bandwidth. Multichassis EtherChannel can be configured across StackWise-Virtual members for high resiliency ▪ Highest wireless scale for Wi-Fi 6 and 802.11ac Wave 2 access points supported on a single switch ▪ Policy-based automation from edge to cloud

System Group	Network, and Application Security Appliance
Business Requirement	**Functional Specification**
Core and Aggregation Layer Switches	▪ Segmentation and micro-segmentation made easy, with predictable performance and scalability ▪ Automation and network assurance ▪ A simple, secure, unified, and integrated offering to ease new branch or campus device rollouts or updates to an existing network ▪ Support for AES-256 with the powerfulMACsec 256-bit encryption algorithm available on all models ▪ Trustworthy solutions: Secure Unique Device Identification (SUDI) support for Plug and Play, enabling tamper-proof device identity capability, which secures zero-touch provisioning by allowing yourdevice to show a certificate to the server to be able to get onto your network

System Group	Network, and Application Security Appliance
Business Requirement	**Functional Specification**
Access Points	▪ 2.4 GHz 802.11b/g/n/ax client accessradio ▪ 5 GHz 802.11a/n/ac/ax client accessradio ▪ 2.4 GHz & 5 GHz dual-band WIDS/WIPS, spectrum analysis, & location analytics radio ▪ 2.4 GHz Bluetooth Low Energy (BLE)radio with Beacon and BLE scanningsupport ▪ Concurrent operation of all four radios ▪ Supported frequency bands (country-specific restrictions apply) □ ▪ Supported frequency bands (country-specific restrictions apply): o 2.412-2.484 GHz o 5.150-5.250 GHz (UNII-1) o 5.250-5.350 GHz (UNII-2) o 5.470-5.600, 5.660-5.725 GHz(UNII-2e) o 5.725 -5.825 GHz (UNII-3) ▪ Internal Antenna (5.1dBi max gain at 2.4GHz, 5.9dBi max gain at 5 GHz) ▪ DL-OFDMA**, UL-OFDMA**, TWT support**, BSS Coloring** ▪ 2.4GHz: 2 x 2 multiple-input, multiple-output (MIMO) with two spatial streams

System Group	Network, and Application Security Appliance
Business Requirement	**Functional Specification**
Access Points	▪ 5GHz: 4 x 4 multiple input, multiple output (MIMO) with four spatial streams ▪ SU-MIMO, UL MU-MIMO** and DL MU-MIMO support ▪ Maximal ratio combining (MRC) & beamforming ▪ 20 and 40 MHz channels (802.11n); 20,40, and 80 MHz channels (802.11ac Wave 2); 20, 40 and 80 MHz channels (802.11ax) ▪ Up to 1024-QAM on both 2.4 GHz & 5GHz bands ▪ Packet aggregation ▪ Power over Ethernet: 42.5 - 57 V (802.3at) or 37 - 57 V (802.3af) - lowpower mode ** ▪ Alternative: 12 V DC input ▪ Power consumption: 30W max (802.3at) or 15W max (802.3af) - low power mode **

System Group	Network, and Application Security Appliance
Business Requirement	Functional Specification
	▪ 1x 100/1000/2.5G BASE-T Ethernet(RJ45) ▪ 1x DC power connector (5.5 mm x 2.5mm, center positive) ▪ All standard mounting hardware included ▪ Desktop, ceiling, and wall mount capable ▪ Ceiling tile rail (9/16, 15/16 or 1 12" flush or recessed rails), assorted cable junctionboxes ▪ Bubble level on the mounting cradle for accurate horizontal wall mounting ▪ Two security screw options (included) (13.5 mm long and 2.5 mm diameter and5 mm head) ▪ Kensington lock hardpoint ▪ Concealed mount plate with anti-tampercable bay ▪ Operating temperature: 32 °F to 104 °F (0 °C to 40 °C) ▪ Humidity: 5 to 95% non-condensing ▪ Mean Time Between Failure (MTBF): 500,000 hours at +25°C operating temperature ▪ 12.05" × 5.06" × 1.74" (30.6 cm × 12.84 cm × 4.43 cm), not including desk mountfeet or mount plate ▪ Weight: 26.07 oz (739 g) ▪ Integrated Layer 7 firewall with mobiledevice policy management ▪ Real-time WIDS/WIPS with alerting and automatic rogue AP containment with Air Marshal ▪ Flexible guest access with deviceisolation ▪ VLAN tagging (802.1q) and tunneling with IPsec VPN ▪ PCI compliance reporting ▪ EAP-TLS, EAP-TTLS, EAP-MSCHAPv2,EAP-SIM ▪ TKIP and AES encryption ▪ Enterprise Mobility Management (EMM) & Mobile Device Management (MDM) integration ▪ Guest access and BYOD Posturing ▪ Advanced Power Save (U-APSD) ▪ WMM Access Categories with DSCP and 802.1p support ▪ Layer 7 application traffic identification and shaping ▪ PMK, OKC, & 802.11r for fast Layer 2roaming ▪ Distributed or centralized layer 3 roaming ▪ Embedded location analytics reporting and device tracking ▪ Global L7 traffic analytics reporting per

System Group	Network, and Application Security Appliance
Business Requirement	Functional Specification
	network, per device, & application ▪ 1 power/booting/firmware upgrade status
	▪ RoHS IEEE Standards ▪ 802.11a, 802.11ac, 802.11ax, 802.11b, 802.11e, 802.11g, 802.11h, 802.11i, 802.11k, 802.11n,802.11r Safety Approvals ▪ CSA and CB 60950 & 62368 ▪ Conforms to UL 2043 (Plenum Rating)Radio Approvals ▪ Canada: FCC Part 15C, 15E, RSS-247 ▪ Europe: EN 300 328, EN 301 893 ▪ Australia/NZ: AS/NZS 4268 ▪ Mexico: IFT, NOM-208 ▪ Taiwan: NCC LP0002EMI Approvals (Class B) ▪ Canada: FCC Part 15B, ICES-003 ▪ Europe: EN 301 489-1-17, EN 55032, EN 55024 ▪ Australia/NZ: CISPR 22 ▪ Japan: VCCI Exposure Approvals ▪ Canada: FCC Part 2, RSS-102 ▪ Europe: EN 50385, EN 62311, EN 62479 ▪ Australia/NZ: AS/NZS 2772 ▪ policing, mirroring, NAT/Port Address Translation (PAT) ▪ Internet Group Management Protocol (IGMP) v1/v2/v3, Protocol Independent Multicast (PIM), Auto-RP, scale-out traffic replication ▪ Route policies, app-aware routing, control policy, data policy, Access Control List (ACL) policy, VPN membership policy ▪ Route policies, app-aware routing, control policy, data policy, ACL policy, VPN membership policy ▪ Integrated 4G/LTE modem on some devices ▪ Wi-Fi 802.11a/b/g/n/ac, WPA2-Enterprise, WPA2-Personal, MAC filtering, 8 SSIDs per radio, 802.11i security enhancement and 802.11e QoS, wireless intrusion detection and protection ▪ IPv4, Simple Network Management Protocol (SNMP), Network Time Protocol (NTP), DNS client, Dynamic Host Configuration Protocol (DHCP) client, DHCP server, DHCP relay, configuration archival, Syslog, Secure Shell (SSH), Secure Copy (SCP), NAT/PAT, Cflowd v10 IPFIX export

System Group	Network, and Application Security Appliance
Business Requirement	Functional Specification
	▪ NETCONF over SSH, Command-Line Interface (CLI), REST (vManage), Linux shell

System Group	Network, and Application Security Appliance
Business Requirement	Functional Specification
Application Performance Monitoring	▪ End-to-end Visibility on the following: o End-User Experience o Code-level Visibility o Microservice Observability o Infrastructure Visibility o Database Visibility o Business Metrics ▪ Single real-time view of business and technical performance ▪ Alerting and Baselining available for all application and business metrics ▪ No code changes required for instrumenting applications Support for enterprise language,platforms, apps, and services

System Group	Network, and Application Security Appliance
Business Requirement	Functional Specification
Application Security Platform	▪ Zero-trust model using micro-segmentation ▪ Extend policy definitions based on additional context ▪ One-click policy enforcement across amulti-cloud data center ▪ Defense in-depth ▪ Detect policy non-compliance events ▪ Identification of workload behavior deviations ▪ Software vulnerability detection ▪ Flexible telemetry collection options ▪ Endpoint device and user context ▪ Support for data center scalability
Multi-factor Authentication	▪ Zero Trust implementation ▪ Verify the identity of all users with strongmulti-factor authentication ▪ Make multi-factor authentication usable for both end-users and admins ▪ Gain full visibility into government-managed and personal devices ▪ Understand who is using what devices and which applications they're accessing ▪ Evaluate the trustworthiness of eachdevice at the time of access

System Group	Network, and Application Security Appliance
Business Requirement	Functional Specification
	▪ Leverage a variety of security factors toverify the trust ▪ Implement access control policies based on resource sensitivity ▪ Enable administrators to quickly adapt tothe ever-changing security landscape ▪ Secure access for on-prem and cloudapps, in a consistent and frictionless manner ▪ Shift access control decisions to applications themselves

System Group	Cloud Infrastructure
Business Requirement	Functional Specification
Industry Standards Certification	▪ The cloud service provider must be o ISO 9001 certified o ISO 27001 certified o ISO 27017 certified o ISO 27018 certified
Cloud Services	▪ The cloud service must have three (3) ormore geographically separate data centers in at least four (4) Countries In the Asia-Pacific region for disaster recovery and high availability. ▪ The cloud service must have the capability to deploy a Highly Available solution across multiple physical sites in a given geography. This capability will be toprevent single points of failure due to geographical or natural disasters. This capability to deploy across multiple sites shall be made available through a self-service portal with a Graphical User Interface (GUI). ▪ The cloud service must have three (3) ormore geographically separate data centers in at least four (4) Countries In the Asia-Pacific region for disaster recovery and high availability

System Group	Cloud Infrastructure
Business Requirement	Functional Specification
Administration and Management	☐ Must provide an interactive Graphical User Interface (GUI) with 2-Factor Authentication that allows users to manageall hosting services instantly. ☐ Must provide a self-service portal. The self-service portal is a graphical user interface accessible over the web that allows cloud administrators and users to conveniently access, provision, modify and automate cloud-based resources (compute, storage, and networking resources). ☐ Must provide a dashboard for cloud administrators. The dashboard shall provide an overall view of the size andstatus of the Cloud Environment. ☐ Must provide a template-based service that makes deployments simpler, more orderly, and predictable instead of deploying each element of an application.This service must allow the Customer and the contractor to input as well as save the infrastructure setup, either piecemeal or, to redeploy the full service in the event of an error.
Performance Monitoring andManagement	☐ Must provide performance monitoringfeatures ☐ The performance monitoring component must provide tools and means to actively capture performance-related information of Cloud Environment services or resources. ☐ The performance monitoring tool must have the ability to send email notifications to administrations based on threshold alarms which can be customized by the administrator. ☐ The performance monitoring component shall capture the initial performance information of the systems and provide a performance baseline, which can be used to analyze the performance variation in the services. ☐ The performance metrics collected shall be made available to customers via the self-service portal. The performance metrics shall be presented in a unified manner with appropriate visualizations. ☐ Must provide built-in audit logging features that capture all API requests/changes to the infrastructure foraudit purposes. The Customer will have the ability to determine the retention length for these audit logs.

System Group	Cloud Infrastructure
Business Requirement	**Functional Specification**
Isolated Private Network and Private Cloud Options	▪ All cloud instances and services must be hosted within an isolated private network or virtual private cloud that can support upto 2000 GB per month data transfer out from the cloud. ▪ Furthermore, should The Customer decide, the cloud service providers must have the ability/option to provide dedicated virtual machines and hosts. ▪ Must provide built-in audit logging features that capture all API requests/changes to the infrastructure foraudit purposes. The Customer will have the ability to determine the retention length for these audit logs. ▪ Must provide a template-based service that makes deployments simpler, more orderly, and predictable instead of deploying each element of an application. This service must allow The Customer and the contractor to input as well as save the infrastructure setup, either piecemeal or, to redeploy the full service in the event of an error. ▪ To guarantee the reliability of the cloud solution being offered, the cloud service must be a leader in Gartner's IaaS Magic Quadrant for at least five (5) consecutive years.
Virtual CPUs	▪ 128 Virtual CPUs
Memory (GB)	▪ 648 GB
Disk Space	▪ 4,600 GB
Target Environments	▪ Development/Staging ▪ Production
Object Storage	▪ 1 unit @ 5000 GB
Data Transfer (Out) per Month	▪ 2000 GB
Support	▪ Shall provide 24x7 technical support to the opted cloud services (option shall include over phone, chat, email, live screen sharing, etc. with response timewithin 1 hour.
Inter-operable with Other Systems	▪ Must provide API interfaces with PPA's current systems as well as systems external to PPA like the Bureau of Customs, Bureau of Internal Revenue, terminal operator systems, other third-party systems, etc.

9. DATA SECURITY AND ENCRYPTION

9.1 Authentication, Verification, and Digital Vaulting

The system must be integrated into a platform for authenticating all documents that are produced by the system. The authenticated documents should be verifiable.

9.2 Public Key Infrastructure (PKI)

9.3 Identity Access Management (IAM)

9.4 Payment Channel Aggregation System

Must provide secure and encrypted API-based payment channel management capabilities that enable secure connectivity with external payment gateway systems, banking systems, and electronic money issuer systems. It must feature the capability for a provenance-enforced, immutable, and automated disaggregation and direct remittance of payments to ensure that fare payments due private vessel operators are directly remitted to the private vessel operator's nominated bank accounts, and to ensure that fees and payments due the PPA are likewise directly remitted to the nominated government depository account of the PPA. The provider must employ the highest level of industry security and standards, high availability, and support for the channel aggregation services.

9.5 Security and Threat Analytics Specifications

The bidder must ensure the security of the production systems (traffic, applications, and database systems). This must include vulnerability and penetration testing (VAPT), along with regular threat monitoring services to ensure the security of the system, throughout the contract period.

9.6 Required Standard Reports

The system must provide a set of standard and ad hoc reports as may be required by the PPA.

Additional tools should be provided for other PPA reports, data mining, and integration requirements. For the following purposes, the production data should be replicated to a dedicated report on-premise server located in the nominated Primary Data Center of the PPA:

- Queries and reports can be run without affecting the performance of the live system or production instance.

- Comparative reports can be created and re-used based on static points in time.
- Optimal performance in a management information environment.
- Exported data can be ported to third-party applications or data warehouse for ongoing analyses.

9.7 Other Considerations

9.7.1 Provide complete reference materials to properly use the system, including Brochures, Training Manuals, Quick guides, technical manuals for the use of end-users and administrators.

9.7.2 Provide complete documentation and turn over all on-premise database administrator/root passwords and other account credentials, when necessary for complete and unencumbered access to the system, its services, and related databases.

9.7.3 Documentation must be written in English of durable construction with concise and high-quality presentation. All documentation must be submitted in physical (high-quality bookbinding) and electronic formats.

9.7.4 Provide the list of hardware, network resources, and applications to be provided which will be used for the project.

10. IMPLEMENTATION REQUIREMENTS

To safeguard the interests of the PPA, the winning bidder must comply with the conditions for implementation specified in this section.

10.1 Integration

10.1.1 The system must be capable of integrating via APIs with third-party or external systems as may be required by PPA. The secure API system must be cloud-based.

10.1.2 The system must be capable of interfacing with PPA's computerized accounting system for the reporting of collection and remittance.

10.1.3 The system must be capable of interfacing with PPA's existing application used in port operations to capture relevant data.

10.2 Inspection and Tests: 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 before tests.

10.3 Duration: The total duration of the Technical Implementation Phase of the project must not exceed twelve (12) months from receipt of the Notice to Proceed (NTP).

10.4 Managed Services Duration: The total duration for the managed services will be one (1) year from the date of the go-live or operationalization commissioning of the Technical Implementation Phase of the project.

10.5 Ownership and Confidentiality of Data

10.5.1 All data/information related to the TOP-CRMS Project shall be owned by the Philippine Ports Authority (PPA).

10.5.2 All data/information related to the development of the information system that may be shared by PPA in the course of evaluating the various modules, functions, and features of the customized solution, shall remain confidential and shall not be copied, divulged, transmitted, or shared in any way to third parties.

10.5.3 All required database licenses purchased, including the on-premise storage equipment/appliances of the solution shall be named under the Philippine Ports Authority.

10.5.4 The Winning bidder shall ensure that personal information recorded in the system shall be treated with confidentiality through a non-disclosure agreement.

10.5.5 The Winning bidder shall abide by the provisions stipulated in the Data Privacy Act.

10.6 Deployment Period:

The system must be deployed within the specified duration from the receipt of NTP, as follows:

Work Segment	Output	Activity Duration (mos.)	Delivery Period (NTP + mos.)
1. Detailed Program Implementation Planningand Scheduling	• Program Implementation Charter and Detailed Schedule	1	NTP+1

2. Solution Technical Architecture (Platform, Applications, Integration, and Data Management), Standard Business Process Framework Design	▪ Technical Architecture ▪ Data Quality and Architecture ▪ Integration Architecture ▪ Security Architecture ▪ Infrastructure Architecture	2	NTP+2
3. Software and Database Management Systems Implementation, 3rd Party Systems Integration, Testing, and Deployment	▪ Deployed Applications ▪ Deployed Mobile Applications ▪ Deployed Data Management Systems ▪ Deployed Business Orchestration Platform ▪ Tracking Device Services Integration	8	NTP+8
4. Station, Network and Infrastructure Setup, Configuration, Testing, and Deployment	▪ Cloud Services Setup and Configuration ▪ High-Performance Server Setup and Configuration ▪ Network Security Appliances Setup and Configuration ▪ Cloud Security Services Setup and Configuration ▪ Application Security Setup and Configuration ▪ Attachment and Detachment Physical Stations ▪ Gate Scanning Stations	5	NTP+5

5. Device Configuration, Testing, Commissioning, and Deployment	▪ Tracking Device Delivery, Setup, Configuration, Testing, and Commissioning	4	NTP+5
6. Procedural Streamliningand Functional On-Boarding	▪ Functional On-Boardingand Go-Live Plan ▪ Change Management Plan ▪ Training and Capacity Development Plan	6	NTP+6
	▪ Conduct of Capacity Development Workshop ▪ Conduct of Sysadmin Training Workshop ▪ Conduct of Functional Admin Training Workshop ▪ Conduct of Data Administration and Management Workshop	3	NTP+9
7. Draft Issuance of Procedures, Rules, and Policies	▪ Draft Issuance of Policies (referto the policy development specifics under the performance target section of this document.	4	NTP+6
8. Deployment, Go-Live, and Operationaliz ation	▪ Network Testing ▪ System Usability Testing ▪ Systems Integration Testing ▪ Stress Testing ▪ Vulnerability and Penetration SecurityTesting ▪ Security Hardening ▪ System Go-Live	4	NTP+9

9. 10-hectare Empty Storage Shared Services Facility	▪ Construction ▪ Commissioning ▪ Operationalization	7	NTP+9
10. Operationalization of Container Tagging	▪ PPA approved Field Operations Plan ▪ Minimum of 200,000 devices tagged containers ▪ Deployed field personnel for device attachment/detachment in PPA designated areas	7	NTP+9

10.7 Deployment Organization

The deployment organization must consist of the following minimum project personnel:

1. Project Manager (at least 10-yr experience)
2. Policy Expert (Legal) (at least 5-yr experience)
3. Procedural Specialist (at least 5-yr experience)
4. Data Architect (at least 5-yr experience)
5. Software Architect (at least 5-yr experience)

11. SCHEDULE OF INVOICING OR BILLING

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.

12. DELIVERY PERIOD (GO-LIVE OPERATIONALIZATION & COMMISSIONING OF THE PROJECT)

The TOP-CRMS is intended to establish a "high-trust" foundation between government and private economic operators to optimize procedural efficiencies that are based on the premise of "trust". Trust, in this context, is established by the level of transactional transparency that international and local private operators (that constitute what is referred to as the "port community") extends or shares with regulatory authorities to reduce procedural delays arising from the need of the regulator to have every transaction subjected to scrutiny and re-validation. To simplify the go-live commissioning process of this managed turnkey system and service, PPA shall ensure that the supplier has successfully delivered:

12.1. Specific to the Software and Data Management Systems: A secure, fully functional, and fully tested TOP-CRMS system meeting the specifications as detailed in this TOR within the specified delivery period. The testing includes functional, integration, regression, and penetration testing.

12.2. Specific to Field Operations: A complete, and PPA-approved, field operation and staffing plan detailing operational requirements for device attachment and detachment operations in the designated terminal/container yards, re-export staging facility/depot operations, and PEZA locations as defined and prescribed by the PPA.

12.3. A secure and fully tested standard API web service endpoint for use to connect to the gate clearance and container release systems of a minimum of 2 private container yard operators, to the PPA TABS system and Berth or Docking Schedule Management System, and internal systems as may be required the PPA, the interfacing system as may be defined by the Bureau of Internal Revenue and the Bureau of Customs.

12.4. A secure, fully configured, and tested payment aggregation system with the capability to automate the disaggregation of payment transactions and the ability to push disaggregated transactions to specific authorized settlement banks.

12.5. A secure and fully tested standard API web service endpoint connecting the TOP-CRMS system payment aggregation service to the payment gateway service as may be prescribed by PPA.

12.6. A fully configured and operational data warehouse and repository that is accessible via a secure standard API web service endpoint.

12.7. A fully configured and operational reports and visualization system. This includes the creation of reports and dashboards as may be required by the PPA.

12.8. Upon completion of all the works covered under the twelve (12) months Technical Implementation Phase, the project contractor shall turn over the project to PPA as completed for the issuance of the certificate of completion for the Technical Implementation Phase.

12.9. On the date indicated on the certificate of completion for the Technical Implementation Phase, the start of the effectivity of the one (1)-year managed services phase shall commence.

12.10. Upon completion of all works covered under the one (1)-year managed services phase, the project contractor shall initiate and request for the issuance of the certificate of completion for the one (1)-year managed services phase.

However, the delivery period may be extended, upon written request of the project contractor and upon written approval by PPA, in the event of unforeseen circumstances such as natural disaster, pandemic/epidemic, civil unrest, armed conflict (force majeure) that might occur during the project implementation and affect the progress in the completion of the project. The period of extension shall be in accordance with the actual condition and upon confirmation by PPA.

13. WARRANTY

13.1 The project contractor shall provide, a post-production service and equipment warranty for all components of the system (covering all hardware and equipment) components as specified in this TOR, at no additional cost to the government.

13.2 The project contractor shall ensure that all hardware equipment is covered by a replacement/maintenance agreement throughout the term of the contract.

13.3 The project contractor shall ensure that all subscriptions, licenses, and support agreements remain active throughout the contract.

GERVACIO ALFREDO N. BALATBAT
Acting Manager, ICTD/End-User

M.A. HYASMIN H. DELOS SANTOS
Manager, POSD/End-User

ANNEX "A"

MATRIX OF FUNCTIONAL REQUIREMENTS SPECIFICATION

FOR POST QUALIFICATION (at least 50%)

TOR REF	*CATEGORY REF*	BUSINESS REQUIREMENT	FUNCTIONAL REQUIREMENT	AVAILABLE Y/N
5.4	*5.4.a*	Demonstrate an operational tracking device with the following out-of-the-box (OOTB) features		
			Must be able to present a simulated use case, and detailed walk-through of the features and capabilities of the item in scope, in presentation format, to demonstrate the providers understanding of the PPA's business case	
			Tagging Device must be physically present and operational (based on TOR device specifications). Must also demonstrate the actual device and secure attachment provisions.	
			Provide a manufacturers certification of 2-year battery lifespan under a manufacturer-defined regular use condition	
			Tagging Device connects to a mobile / LTE communications network	
			Tagging Device Monitoring has at least a 200km reach	

TOR REF	*CATEGORY REF*	BUSINESS REQUIREMENT	FUNCTIONAL REQUIREMENT	AVAILABLE Y/N
			Demonstrate real-time actual movement of tagging device. Must show real-time device attachment, simulated binding to the vehicle, and real-time movement tracking. Demonstrate real-time device detachment process.	
			Must show real-time data ingestion of device data in a Pro-forma dashboard Must show a device management console to remotely manage the device. Must show battery lifespan, and central control functions and capabilities Must demonstrate actual data elements transmitted by the tracking/tagging device Must show the movement of the device overlayed on a map	
	5.4.b	Demonstrate the following operational mobility features and cloud-native applications		
			Must be able to present a simulated use case, and detailed walk-through of the features and capabilities of the item in scope, in presentation format, to demonstrate the providers understanding of the PPA's business case	

TOR REF	*CATEGORY REF*	BUSINESS REQUIREMENT	FUNCTIONAL REQUIREMENT	AVAILABLE Y/N
		Web Applications	Demonstrate OOTB Configurable Web Forms Demonstrate KYC functions and capabilities Demonstrate Person Management functions Demonstrate Basic Account Registration functions Demonstrate Basic Persona Registration Functions Demonstrate insurance availment functions Present the integration functions and capabilities of the web application Demonstrate the OOTB capabilities and functions to ingest large volumes of data using pre-defined data template (CSV, xlsx) Demonstrate the OOTB to present ingested data in a structured table or view Demonstrate the OOTB capability and functions to ingest tracking/tagging device location or telemetry data Present a detailed portfolio of OOTB functions and capabilities of the provider's system Demonstrate the OOTB capability and functions to	

TOR REF	*CATEGORY REF*	BUSINESS REQUIREMENT	FUNCTIONAL REQUIREMENT	AVAILABLE Y/N
			generate and read QR Codes	
			Demonstrate OOTB payment aggregation functions and capabilities received from external fund sources and consolidate all funds to a single settlement account. Demonstrate OOTB integration to the data vaulting system	
		Mobile Applications (Android App)	Mobile application demonstration must be performed using a common and widely available smartphone running on the Android operating system Demonstrate the OOTB capability and functions to ingest tracking/tagging device location or telemetry data Demonstrate OOTB Mobile Applications has the features and functions to accept work orders, receive dispatch orders, capture drive and truck information, transmit real-time location data, and must have real-time communications capability Demonstrate the OOTB capability of the mobile application to securely transmit harmonized, mixed type media (data and photos) to a secure backend repository	

TOR REF	*CATEGORY REF*	BUSINESS REQUIREMENT	FUNCTIONAL REQUIREMENT	AVAILABLE Y/N
			Demonstrate driver and vehicle location tracking using the mobile application Demonstrate insurance availment functions (mobile app) Present the integration functions and capabilities of the mobile applications to external 3rd party systems Present a detailed portfolio of OOTB functions and capabilities of the provider's mobile application or systems Demonstrate OOTB payment settlement capabilities and connectivity to banking systems, electronic money issuer systems, or accredited payment gateway systems. Demonstrate OOTB delivery and fulfillment notification capabilities and functions	
		Data Exchange, Integration, and Interoperability	Demonstrate the seamless exchange of data between the primary web application system and all mobile systems Demonstrate the ability to generate and read QR Codes Demonstrate end-to-end data exchange/integration capabilities from registration to transaction using simulated data	

TOR REF	*CATEGORY REF*	BUSINESS REQUIREMENT	FUNCTIONAL REQUIREMENT	AVAILABLE Y/N
			Demonstrate OOTB functions and capabilities to securely integrate with external 3rd party systems	
		Reports Visualization	Demonstrate the ability of the system to ingest data from multiple sources, and present the sourced data in standard report format or a defined visual format. Demonstrate the ability to stream live data to a targeted dashboard Demonstrate OOTB functions and capabilities that display transactional data in real-time under roles-based permission parameters.	
		Technology Stack		
			Demonstrate OOTB CMS functions and capabilities	
			Demonstrate the OOTB capabilities and features of the Business Orchestration and Middleware component of the system Demonstrate the OOTB automated workflow and routing capabilities and functions of the provider's system Demonstrate OOTB visual monitoring capabilities of workflows	

TOR REF	*CATEGORY REF*	BUSINESS REQUIREMENT	FUNCTIONAL REQUIREMENT	AVAILABLE Y/N
			Demonstrate the capabilities and functions for dynamic workflow routing with zero systems or application downtime Demonstrate OOTB API Gateway functions and capabilities. API Gateway system must be able to send/receive/process both Rest, WebSocket's, XML data.	
		Cloud, Container and VM Instance Management, Business Continuity and Security	Demonstrate secure cloud containerization capabilities and functions Demonstrate Hot-Deploy functions (zero downtime) Demonstrate OOTB security functions and capabilities Present planned active-active system availability/business continuity / disaster recovery schema Present a secure network design topology for a mixed-cloud and hybrid cloud infrastructure	
		Network Security and Cybersecurity Threat Monitoring	Present a security topology and design covering networks, application, data, and threat analytics schema	

TOR REF	*CATEGORY REF*	BUSINESS REQUIREMENT	FUNCTIONAL REQUIREMENT	AVAILABLE Y/N
5.4.c	Demonstrate the data management and data registries capabilities			
			Must be able to present a simulated use case, and detailed walk-through of the features and capabilities of the item in scope, in presentation format, to demonstrate the providers understanding of the PPA's business case	
		Data Registries	Demonstrate OOTB UNLOCODE Data Registry	
			Demonstrate OOTB AHTN Data Registry	
			Demonstrate PSGC Data Registry	
			Demonstrate Countries Registry	
		Data Protection	Demonstrate Secure Data Management Schema	
		Data Encryption and Privacy	Demonstrate OOTB data encryption and data vaulting functions and capabilities	
5.4.d	10 Hectare Empty Container Staging Facility			
			Must be able to present a simulated use case, and detailed walk-through of the features and capabilities of the item in scope, in presentation format, to demonstrate the providers understanding of the	

TOR REF	*CATEGORY REF*	BUSINESS REQUIREMENT	FUNCTIONAL REQUIREMENT	AVAILABLE Y/N
			PPA's business case	
			Must be able to present a TCT, consolidated TCT, or a conditional lease agreement for a continuous 10-hectare facility with a 50km radius from the Port of Manila.	

Section VIII. Checklist of Technical and Financial Documents

Checklist of Technical and Financial Documents

I. TECHNICAL COMPONENT ENVELOPE

Class "A" Documents

Legal Documents

☐ (a) Valid PhilGEPS Registration Certificate (Platinum Membership) (all pages) in accordance with Section 8.5.2 of the IRR;

Technical Documents

☐ (b) Statement of the prospective bidder of all its ongoing government and private contracts, including contracts awarded but not yet started, if any, whether similar or not similar in nature and complexity to the contract to be bid; **and**

☐ (c) Statement of the bidder's Single Largest Completed Contract (SLCC) similar to the contract to be bid, except under conditions provided for in Sections 23.4.1.3 and 23.4.2.4 of the 2016 revised IRR of RA No. 9184, within the relevant period as provided in the Bidding Documents; **and**

☐ (d) Original copy of Bid Security. If in the form of a Surety Bond, submit also a certification issued by the Insurance Commission;
Or

Original copy of Notarized Bid Securing Declaration; **and**

☐ (e) Conformity with the Technical Specifications, which may include production/delivery schedule, manpower requirements, and/or after-sales/parts, if applicable; **and**

☐ (f) Original duly signed Omnibus Sworn Statement (OSS); **and** if applicable, Original Notarized Secretary's Certificate in case of a corporation, partnership, or cooperative; or Original Special Power of Attorney of all members of the joint venture giving full power and authority to its officer to sign the OSS and do acts to represent the Bidder.

Financial Documents

☐ (g) The prospective bidder's computation of Net Financial Contracting Capacity (NFCC);
or
A committed Line of Credit from a Universal or Commercial Bank in lieu of its NFCC computation.

Class "B" Documents

☐ (h) If applicable, a duly signed joint venture agreement (JVA) in case the joint venture is already in existence;
or

duly notarized statements from all the potential joint venture partners stating the following:

a. that they will enter into and abide by the provisions of the JVA in the instance that the bid is successful; and

b. failure to enter into JVA in the event of a contract award shall be a ground for bid disqualification and subsequent forfeiture of the bid security.

Other documentary requirements under RA No. 9184 (as applicable)

☐ (i) *[For foreign bidders claiming by reason of their country's extension of reciprocal rights to Filipinos]* Certification from the relevant government office of their country stating that Filipinos are allowed to participate in government procurement activities for the same item or product.

☐ (j) Certification from the DTI if the Bidder claims preference as a Domestic Bidder or Domestic Entity.

II. FINANCIAL COMPONENT ENVELOPE

☐ (a) Original of duly signed and accomplished Financial Bid Form; **and**

☐ (b) Original of duly signed and accomplished Price Schedule(s).

BID FORM

Date : _____
Project Identification No. : _____

To: [name and address of Procuring Entity]

Having examined the Philippine Bidding Documents (PBDs) including the Supplemental or Bid Bulletin Numbers [insert numbers], the receipt of which is hereby duly acknowledged, we, the undersigned, offer to [supply/deliver/perform] [description of the Goods] in conformity with the said PBDs for the sum of [total Bid amount in words and figures] or the total calculated bid price, as evaluated and corrected for computational errors, and other bid modifications in accordance with the Price Schedules attached herewith and made part of this Bid. The total bid price includes the cost of all taxes, such as, but not limited to: [specify the applicable taxes, e.g. (i) value added tax (VAT), (ii) income tax, (iii) local taxes, and (iv) other fiscal levies and duties], which are itemized herein or in the Price Schedules,

If our Bid is accepted, we undertake:

a. to deliver the goods in accordance with the delivery schedule specified in the Schedule of Requirements of the Philippine Bidding Documents (PBDs);

b. to provide a performance security in the form, amounts, and within the times prescribed in the PBDs;

c. to abide by the Bid Validity Period specified in the PBDs and it shall remain binding upon us at any time before the expiration of that period.

Until a formal Contract is prepared and executed, this Bid, together with your written acceptance thereof and your Notice of Award, shall be binding upon us.

We understand that you are not bound to accept the Lowest Calculated Bid or any Bid you may receive.

We certify/confirm that we comply with the eligibility requirements pursuant to the PBDs.

The undersigned is authorized to submit the bid on behalf of [name of the bidder] as evidenced by the attached [state the written authority].

We acknowledge that failure to sign each and every page of this Bid Form, including the attached Schedule of Prices, shall be a ground for the rejection of our bid.

Name: _____
Legal capacity: _____

Signature: _____

Duly authorized to sign the Bid for and behalf of: _____

Date: _____

Price Schedule for Goods Offered from Abroad
[shall be submitted with the Bid if bidder is offering goods from Abroad]

For Goods Offered from Abroad

Name of Bidder _____ Project ID No._____ Page ___ of ___

1	2	3	4	5	6	7	8	9
Item	Description	Country of origin	Quantity	Unit price CIF port of entry (specify port) or CIP named place (specify border point or place of destination)	Total CIF or CIP price per item (col. 4 x 5)	Unit Price Delivered Duty Unpaid (DDU)	Unit price Delivered Duty Paid (DDP)	Total Price delivered DDP (col 4 x 8)

Name: _____

Legal Capacity: _____

Signature: _____

Duly authorized to sign the Bid for and behalf of: _____

Price Schedule for Goods Offered from Within the Philippines
[shall be submitted with the Bid if bidder is offering goods from within the Philippines]

For Goods Offered from Within the Philippines

Name of Bidder _____ Project ID No._____ Page ___of___

1	2	3	4	5	6	7	8	9	10
Item	Description	Country of origin	Quantity	Unit price EXW per item	Transportation and all other costs incidental to delivery, per item	Sales and other taxes payable if Contract is awarded, per item	Cost of Incidental Services, if applicable, per item	Total Price, per unit (col 5+6+7+8)	Total Price delivered Final Destination (col 9) x (col 4)

Name: _____

Legal Capacity: _____

Signature: _____

Duly authorized to sign the Bid for and behalf of: _____

Bid Securing Declaration Form
[shall be submitted with the Bid if bidder opts to provide this form of bid security]

REPUBLIC OF THE PHILIPPINES)
CITY OF _____) S.S.

BID SECURING DECLARATION
Project Identification No.: [Insert number]

To: [Insert name and address of the Procuring Entity]

I/We, the undersigned, declare that:

1. I/We understand that, according to your conditions, bids must be supported by a Bid Security, which may be in the form of a Bid Securing Declaration.

2. I/We accept that: (a) I/we will be automatically disqualified from bidding for any procurement contract with any procuring entity for a period of two (2) years upon receipt of your Blacklisting Order; and, (b) I/we will pay the applicable fine provided under Section 6 of the Guidelines on the Use of Bid Securing Declaration, within fifteen (15) days from receipt of the written demand by the procuring entity for the commission of acts resulting to the enforcement of the bid securing declaration under Sections 23.1(b), 34.2, 40.1 and 69.1, except 69.1(f),of the IRR of RA No. 9184; without prejudice to other legal action the government may undertake.

3. I/We understand that this Bid Securing Declaration shall cease to be valid on the following circumstances:

   a. Upon expiration of the bid validity period, or any extension thereof pursuant to your request;
   b. I am/we are declared ineligible or post-disqualified upon receipt of your notice to such effect, and (i) I/we failed to timely file a request for reconsideration or (ii) I/we filed a waiver to avail of said right; and
   c. I am/we are declared the bidder with the Lowest Calculated Responsive Bid, and I/we have furnished the performance security and signed the Contract.

IN WITNESS WHEREOF, I/We have hereunto set my/our hand/s this ____ day of [month] [year] at [place of execution].

[Insert NAME OF BIDDER OR ITS AUTHORIZED REPRESENTATIVE]
[Insert signatory's legal capacity]
Affiant

[Jurat]
[Format shall be based on the latest Rules on Notarial Practice]

Contract Agreement Form for the Procurement of Goods (Revised)
[Not required to be submitted with the Bid, but it shall be submitted within ten (10) days after receiving the Notice of Award]

CONTRACT AGREEMENT

THIS AGREEMENT made the _____ day of _____ 20_____ between [name of PROCURING ENTITY] of the Philippines (hereinafter called "the Entity") of the one part and [name of Supplier] of [city and country of Supplier] (hereinafter called "the Supplier") of the other part;

WHEREAS, the Entity invited Bids for certain goods and ancillary services, particularly [brief description of goods and services] and has accepted a Bid by the Supplier for the supply of those goods and services in the sum of [contract price in words and figures in specified currency] (hereinafter called "the Contract Price").

NOW THIS AGREEMENT WITNESSETH AS FOLLOWS:

1. In this Agreement words and expressions shall have the same meanings as are respectively assigned to them in the Conditions of Contract referred to.

2. The following documents as required by the 2016 revised Implementing Rules and Regulations of Republic Act No. 9184 shall be deemed to form and be read and construed as integral part of this Agreement, viz.:

    i. Philippine Bidding Documents (PBDs);
        i. Schedule of Requirements;
        ii. Technical Specifications;
        iii. General and Special Conditions of Contract; and
        iv. Supplemental or Bid Bulletins, if any

    ii. Winning bidder's bid, including the Eligibility requirements, Technical and Financial Proposals, and all other documents or statements submitted;

        Bid form, including all the documents/statements contained in the Bidder's bidding envelopes, as annexes, and all other documents submitted (e.g., Bidder's response to request for clarifications on the bid), including corrections to the bid, if any, resulting from the Procuring Entity's bid evaluation;

    iii. Performance Security;

    iv. Notice of Award of Contract; and the Bidder's conforme thereto; and

    v. Other contract documents that may be required by existing laws and/or the Procuring Entity concerned in the PBDs. Winning bidder agrees that additional contract documents or information prescribed by the GPPB that are subsequently required for submission after the contract execution, such

as the Notice to Proceed, Variation Orders, and Warranty Security, shall likewise form part of the Contract.

3. In consideration for the sum of [total contract price in words and figures] or such other sums as may be ascertained, [Named of the bidder] agrees to [state the object of the contract] in accordance with his/her/its Bid.

4. The [Name of the procuring entity] agrees to pay the above-mentioned sum in accordance with the terms of the Bidding.

IN WITNESS whereof the parties hereto have caused this Agreement to be executed in accordance with the laws of the Republic of the Philippines on the day and year first above written.

[Insert Name and Signature]	[Insert Name and Signature]
[Insert Signatory's Legal Capacity]	[Insert Signatory's Legal Capacity]
for:	for:
[Insert Procuring Entity]	[Insert Name of Supplier]

Acknowledgment
[Format shall be based on the latest Rules on Notarial Practice]

Omnibus Sworn Statement (Revised)
[shall be submitted with the Bid]

REPUBLIC OF THE PHILIPPINES)
CITY/MUNICIPALITY OF _____) S.S.

AFFIDAVIT

I, [Name of Affiant], of legal age, [Civil Status], [Nationality], and residing at [Address of Affiant], after having been duly sworn in accordance with law, do hereby depose and state that:

1. [Select one, delete the other:]

   [If a sole proprietorship:] I am the sole proprietor or authorized representative of [Name of Bidder] with office address at [address of Bidder];

   If a partnership, corporation, cooperative, or joint venture:] I am the duly authorized and designated representative of [Name of Bidder] with office address at [address of Bidder];

2. [Select one, delete the other:]

   [If a sole proprietorship:] As the owner and sole proprietor, or authorized representative of [Name of Bidder], I have full power and authority to do, execute and perform any and all acts necessary to participate, submit the bid, and to sign and execute the ensuing contract for [Name of the Project] of the [Name of the Procuring Entity], as shown in the attached duly notarized Special Power of Attorney;

   [If a partnership, corporation, cooperative, or joint venture:] I am granted full power and authority to do, execute and perform any and all acts necessary to participate, submit the bid, and to sign and execute the ensuing contract for [Name of the Project] of the [Name of the Procuring Entity], as shown in the attached [state title of attached document showing proof of authorization (e.g., duly notarized Secretary's Certificate, Board/Partnership Resolution, or Special Power of Attorney, whichever is applicable;)];

3. [Name of Bidder] is not "blacklisted" or barred from bidding by the Government of the Philippines or any of its agencies, offices, corporations, or Local Government Units, foreign government/foreign or international financing institution whose blacklisting rules have been recognized by the Government Procurement Policy Board, by itself or by relation, membership, association, affiliation, or controlling interest with another blacklisted person or entity as defined and provided for in the Uniform Guidelines on Blacklisting;

4. Each of the documents submitted in satisfaction of the bidding requirements is an authentic copy of the original, complete, and all statements and information provided therein are true and correct;

5. [Name of Bidder] is authorizing the Head of the Procuring Entity or its duly authorized representative(s) to verify all the documents submitted;

6. [Select one, delete the rest:]

   [If a sole proprietorship:] The owner or sole proprietor is not related to the Head of the Procuring Entity, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

   [If a partnership or cooperative:] None of the officers and members of [Name of Bidder] is related to the Head of the Procuring Entity, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

   [If a corporation or joint venture:] None of the officers, directors, and controlling stockholders of [Name of Bidder] is related to the Head of the Procuring Entity, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

7. [Name of Bidder] complies with existing labor laws and standards; and

8. [Name of Bidder] is aware of and has undertaken the responsibilities as a Bidder in compliance with the Philippine Bidding Documents, which includes:

   a. Carefully examining all of the Bidding Documents;

   b. Acknowledging all conditions, local or otherwise, affecting the implementation of the Contract;

   c. Making an estimate of the facilities available and needed for the contract to be bid, if any; and

   d. Inquiring or securing Supplemental/Bid Bulletin(s) issued for the [Name of the Project].

9. [Name of Bidder] did not give or pay directly or indirectly, any commission, amount, fee, or any form of consideration, pecuniary or otherwise, to any person or official, personnel or representative of the government in relation to any procurement project or activity.

10. In case advance payment was made or given, failure to perform or deliver any of the obligations and undertakings in the contract shall be sufficient grounds to constitute criminal liability for Swindling (Estafa) or the commission of fraud with unfaithfulness or abuse of confidence through misappropriating or converting any payment received by a person or entity under an obligation involving the duty to

deliver certain goods or services, to the prejudice of the public and the government of the Philippines pursuant to Article 315 of Act No. 3815 s. 1930, as amended, or the Revised Penal Code.

IN WITNESS WHEREOF, I have hereunto set my hand this __ day of ___, 20__ at _____, Philippines.

[Insert NAME OF BIDDER OR ITS AUTHORIZED REPRESENTATIVE]
[Insert signatory's legal capacity]
Affiant

[Jurat]
[Format shall be based on the latest Rules on Notarial Practice]

Performance Securing Declaration (Revised)
[if used as an alternative performance security but it is not required to be submitted with the Bid, as it shall be submitted within ten (10) days after receiving the Notice of Award]

REPUBLIC OF THE PHILIPPINES)
CITY OF _____) S.S.

PERFORMANCE SECURING DECLARATION

Invitation to Bid: [Insert Reference Number indicated in the Bidding Documents]

To: [Insert name and address of the Procuring Entity]

I/We, the undersigned, declare that:

1. I/We understand that, according to your conditions, to guarantee the faithful performance by the supplier/distributor/manufacturer/contractor/consultant of its obligations under the Contract, I/we shall submit a Performance Securing Declaration within a maximum period of ten (10) calendar days from the receipt of the Notice of Award prior to the signing of the Contract.

2. I/We accept that: I/we will be automatically disqualified from bidding for any procurement contract with any procuring entity for a period of one (1) year for the first offense, or two (2) years for the second offense, upon receipt of your Blacklisting Order if I/We have violated my/our obligations under the Contract;

3. I/We understand that this Performance Securing Declaration shall cease to be valid upon:

    a. issuance by the Procuring Entity of the Certificate of Final Acceptance, subject to the following conditions:
        i. Procuring Entity has no claims filed against the contract awardee;
        ii. It has no claims for labor and materials filed against the contractor; and
        iii. Other terms of the contract; or

    b. replacement by the winning bidder of the submitted PSD with a performance security in any of the prescribed forms under Section 39.2 of the 2016 revised IRR of RA No. 9184 as required by the end-user.

IN WITNESS WHEREOF, I/We have hereunto set my/our hand/s this ____ day of [month] [year] at [place of execution].

[Insert NAME OF BIDDER OR ITS AUTHORIZED REPRESENTATIVE]
[Insert signatory's legal capacity]
Affiant

[Jurat]
[Format shall be based on the latest Rules on Notarial Practice]

NET FINANCIAL CONTRACTING CAPACITY (NFFC)
COMPUTATION

A. The values of the bidder's current assets and current liabilities shall be based on the data submitted to the BIR, through its Electronic Filing and Payment System (EFPS).

		Year 20__
1.	Total Assets	
2.	Current Assets	
3.	Total Liabilities	
4.	Current Liabilities	
5.	Net Worth (1-3)	
6.	Net Working Capital (2-4)	

B. The Net Financial Contracting Capacity (NFCC) based on the above data is computed as follows:

NFCC = [(Current asset minus current liabilities) (15)] minus the value of all outstanding or uncompleted portions of the projects under ongoing contracts, including awarded contracts yet to be started, coinciding with the contract to be bid

NFCC = Php _____

K = 15

Herewith attached are certified true copies of the income tax return and audited financial statement: stamped "RECEIVED" by the BIR or BIR authorized collecting agent for the immediately preceding year.

Submitted by:

_____
Name of Supplier/Distributor/Manufacturer

Signature of Authorized Representative

STATEMENT OF THE BIDDER'S ONGOING GOVERNMENT AND PRIVATE CONTRACTS, INCLUDING CONTRACTS AWARDED BUT NOT YET STARTED

This is to certify that _____ has the following ongoing government and private contracts, including contracts awarded but not yet started:

NAME OF THE CONTRACT	DATE OF THE CONTRACT	CONTRACT DURATION	OWNER'S NAME & ADDRESS	KINDS OF GOODS/SERVICES DELIVERED	AMOUNT OF CONTRACT	VALUE OF OUTSTANDING CONTRACT	DATE OF DELIVERY

*PROOF OF CONTRACT TO BE PRESENTED AT POST-QUALIFICATION.

_____ _____

Name and Signature of Authorized Representative Date

STATEMENT OF THE BIDDER'S SINGLE LARGEST COMPLETED CONTRACT (SLCC) SIMILAR TO THE CONTRACT TO BE BID

This is to certify that _____ has completed the following:

NAME OF THE CONTRACT	DATE OF THE CONTRACT	CONTRACT DURATION	OWNER'S NAME & ADDRESS	KINDS OF GOODS	AMOUNT OF COMPLETED CONTRACT/S	DATE OF DELIVERY	END USER'S ACCEPTANCE OR OFFICIAL RECEIPT(S) OR SALES INVOICE ISSUED FOR THE CONTRACT*

*TO BE ATTACHED TO THE STATEMENT

_____ _____

Name and Signature of Authorized Representative Date