		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. ▪ 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 original entity 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 entityof 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 theelectronic 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 nodesin 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 set of unique identifiers of interest is recorded in 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 portion of 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. ▪ 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 for network 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 compliance violations. ▪ 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 of Custom 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 to remediate Risks either automatically or manually (i.e., push-button or offline remediation) ▪ 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 multiple Cloud 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 a VM'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 ▪ 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.; Instead of 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.
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 machinelearning engine, halt application exploitswith 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. Endusers 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 and standard 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 continuous detection and response activities for advanced threats. (e.g., should not require scheduling) ▪ The solution must be able to push outnew 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. ▪ 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 security posture 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 4visualizations 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/s through: ▪ Snapshot URL ▪ Shortened Snapshot URL ▪ Must provide users the ability for them to be able to download the dashboard/s as afile with type: • .pdf ▪ .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 to be able to download the visualizations asfiles with type: o .pdf file o .png file	
Data Streaming Engine	▪ Must be able to collect and parse these types 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 data retention policies	

	Risk Profiling Reports	▪ Must be able to automatically detect and alert anomalies in logs using predetermined thresholds ▪ Must have machine learning capabilitiesto 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 tobe 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 isviewable 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 environmentssuch 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.	
	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 bewell 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 operatorsto 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 beable 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 followingmetrics: o Network metrics (HTTP requests for an application, HTTP request errors for an application with a latency of 1 second) o Container metrics (CPU, disk, and memory utilization) o 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	

	with popular 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. • 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 likedatabases, eliminating the time-consuming and complex steps for developers and operators to configure. ▪ The platform must standardize detection, compilation, and deployment of applicationcode 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 thatmodifications 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 applicationinstance, 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 ofthe 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
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 with a 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 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 be managed by the platform.	

Technical Environment and Infrastructure Specifications

System Group	Turnkey Environment for Tracking Devices andCommunications Network
Business Requirement	**Functional Specification**
Industry Standards	▪ Compliance to International Cellular Communications Standards; 3GPP Release 14 and above
Radio Access Network Air InterfaceSpecification Standard	▪ The radio interface must support GPRS,LTEm, or nbIoT
Radio Access Network Base StationSpecification	▪ The system must be compatible with all carriers 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 Band 28, 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 thebackhaul connectivity. ▪ The solution must be equipped with failover mechanisms for the backhaul connectivity. ▪ The solution must support IPv6

	standards. ▪ The must support buffering and graceful recovery 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 andbar 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 remotely update 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 add and remove features on endpoints. ▪ The solution must be able to provide bandwidth/airtime usage for each endpoint.
Network Server and CommunicationServices	▪ The solution must have the capability to implement service provider traffic policies through connectivity profiles allocated to devices. ▪ 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 3rdparty 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.

Device Provisioning, Monitoring, and Management	▪ The solution must provide tools to ensurethe 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 network coverage 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 numbers for 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 the device. ▪ When devices are manufactured, they must register the correct IMEI/ICCID to pair it with the platform system when provisioning. ▪ 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.
Security: Cloud	▪ Development & Releases must adhere tostrict 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 webdatabase (web store). ▪ No shell access permitted. ▪ All containers must log to centralized logging services.	
	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 embeddedIPv4/6 TCP/IP stack + TCP/UDP client/endpoint, HTTP client, FTP Client, MQTT Client, and CoAP Client. 6. The solution must support 2G Fallback.	

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 enable API access for 3rd party applications. ▪ Must support OAuth2 authorization flows with valid tokens for API authentication. ▪ Client credentials must be supported for machine-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 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 configuration publishing.	

	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 – allexecuted 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. ▪ The device must publish its position accuracy with timestamp via the following: o 0-location determined with marker o 1- location determined with GPS o 2- location determined with cell 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 set of 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 ▪ 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 necessarymanagement 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	
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 asthe event from monitored/connected devices has been registered. ▪ The solution must support mapping between devices and integrations through groups & 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 necessarymanagement 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 must be a secure and dedicated cloud-based service
Server Processing and Architecture	▪ Server must allow concurrent addition ofprocessor core ▪ Server must have an on-chip accelerator forcompression ▪ Server must have a dedicated core co-processor for encryption ▪ Server must support up to 40TB ofredundant memory feature ▪ Server must support open standards and tool across all cloud consumption models ▪ Server must support leading open-source databases, runtimes, languages, and tools ▪ Server must be scalable, robust, and efficient ▪ 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 fordisaster 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/Oprocessing 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 ▪ Server must have the capability for bringing up highly secured operating enclaves ▪ Server must support 2TB memory for asingle VM instance to run an open-source database without sharding.	
Warranty and Support	▪ Server must have at least a 1-year warrantycovering 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 and all-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 140-2 Level1 encryption with centralized keymanagement ▪ The storage should support both internal and external virtualization functionality ▪ The storage should have the ability to cluster, and support scale-out or scale-updeployment ▪ The storage must be capable of migrating or replicating data between on-premise hardware deployment and into public cloud storage
High-Availability and DisasterRecovery	□ 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 user interface for centralized management ▪ The storage management should providea 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	
	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 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 FullFlexible 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	
Core and Aggregation Layer Switches	▪ Ready for next-generation technologies with 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 up to 2 Bpps of forwarding performance ▪ Up to 32 nonblocking 100 Gigabit Ethernet QSFP28 ports ▪ Up to 32 nonblocking 40 Gigabit EthernetQSFP+ ports ▪ Up to 48 nonblocking 25 Gigabit EthernetSFP28 ports ▪ Up to 48 nonblocking 10 Gigabit EthernetSFP+ ports	
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-microsecond accuracy, making it suitable for distribution and synchronization of time and frequency over the network ▪ Dual-stack support for IPv4/IPv6 anddynamic hardware forwarding table allocations, for ease of IPv4-to-IPv6migration ▪ Support for both static and dynamic NAT and 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 and802.11ac Wave 2 access points supported on a singie switch ▪ Policy-based automation from edge tocloud	
	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 powerful MACsec 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 your device to show a certificate to the server to be able to get onto your network	

	Access Points	▪ 2.4 GHz 802.11b/g/n/ax client access radio ▪ 5 GHz 802.11a/n/ac/ax client access radio ▪ 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**, TWTsupport**, BSS Coloring** ▪ 2.4GHz: 2 x 2 multiple-input, multiple-output (MIMO) with two spatial streams
	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 ** ▪ 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 1⁄2" 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 × 12.84cm × 4.43 cm), not including desk mount feet 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 AirMarshal ▪ Flexible guest access with device isolation ▪ VLAN tagging (802.1q) and tunneling withIPsec 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 and802.1p support ▪ Layer 7 application traffic identificationand 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 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 LP0002 EMI 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 ▪ NETCONF over SSH, Command-Line Interface (CLI), REST (vManage), Linux shell	

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	
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 each device at the time of access ▪ Leverage a variety of security factors toverify the trust ▪ Implement access control policies basedon resource sensitivity ▪ Enable administrators to quickly adapt to the ever-changing security landscape ▪ Secure access for on-prem and cloud apps, 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 to prevent 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
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 and status 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 and Management	▫ Must provide performance monitoring features ▫ 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.
	Isolated Private Network and PrivateCloud Options	▪ All cloud instances and services must be hosted within an isolated private network or virtual private cloud that can support up to 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.

DATA SECURITY AND ENCRYPTION

1. Authentication, Verification, and Digital Vaulting

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

2. Public Key Infrastructure (PKI)

3. Identity Access Management (IAM)

4. Payment Channel Aggregation System

   Must provide the 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 back 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.

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.

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 report, 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.

7. Other Considerations

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.

	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. 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 book binding) and electronic formats. **7.4** Provide the list of hardware, network resources and application to be provided which will be used for the project.	
	IMPLEMENTATION REQUIREMENTS To safeguard the interests of the PPA, the winning bidder must comply with the conditions for implementation specified in this section. 1. Integration 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. 1.2 The system must be capable of interfacing with PPA's computerized accounting system for the reporting of collection and remittance. 1.3 The system must be capable of interfacing with PPA's existing application used in port operations to capture relevant data. 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 prior to tests.	

	3. Duration: The total duration of the Technical Implementation Phase of the project must not exceed twelve (12) months from the issuance of the Notice to Proceed (NTP). 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. 5. Ownership and Confidentiality of Data 5.1 All data/information related to the TOP-CRMS Project shall be owned by the Philippine Ports Authority (PPA). 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. 5.3 All required database licenses purchased for the on-premise storage equipment / appliances of the solution shall be named under the Philippine Ports Authority. 5.4 The Winning bidder shall ensure that personal information recorded in the system shall be treated with confidentiality through a non-disclosure agreement. 5.5 The Winning bidder shall abide by the provisions stipulated in the Data Privacy Act.	
	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.	

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:

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.

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.

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.

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.

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.

	6. A fully configured and operational data warehouse and repository that is accessible via a secure standard API web service endpoint. 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. 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. 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. 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.	
	BIDDER'S QAULIFICATIONS: 1. Given the nature of the system and services required by PPA and to ensure the successful delivery and operation of the envisioned Project, the prospective bidder must have the following current ISO certifications: a. ISO 9001:2015 b. ISO 27001:2013 c. ISO 27017:2015 d. ISO 27018:2014 and e. ISO 27701:2019	

	2. All certifications must be current and active at the time of bid submission. 3. To ensure that prospective bidder have the requisite experience and financial capacity to successfully deliver the project, the prospective bidder must: a. Be in continuous operation with combined experience as a service provider, information system provider, systems developer, and systems integrator for at least ten (10) years at the time of bid submission. Have a minimum of 10 hectares of available area, accessible by major roads, within a 50km radius from international container terminals in Manila for use as a secure container staging facility or container depot for re-exporting empty containers.	
	POST QUALIFICATION REQUIREMENTS: **1.** The prospective bidder must already have an available software of a TOP-CRMS inclusive of Cloud-based solution during post qualification. **2.** The prospective bidder must be able to conduct a systems demonstration for technical evaluation to determine if functional requirements are at least 50% fit in accordance with the specifications provided in Annex "A" of this TOR. **3.** The proposed solution is uniquely designed to primarily meet regulatory capabilities of the PPA. As such, the Authority recognizes that the solution in its final form will be a system that integrates several commercial-off-the-shelf and operational software technologies, interfacing a variety of physical devices, and will also consist of multi-protocol/multi-modal network connectivity that will need to be customized or configured to meet the exact specifications of the envisioned PPA system. **4.** To ensure that the solutions proposed by prospective bidders are functional and operational systems, each bidder will be required, as a post-qualification requirement, within five (5) days from being issued a post-qualification notice by the Authority, to demonstrate that components intended	

for full functional/operational integration system demonstrate the following:

a. Demonstrate an operational tracking device with the following out-of-the-box (OOTB) features:

   i. Network connectivity (local network)

   ii. Network reach and successful data transmission within 200km radius from the PPA Headquarters

   iii. Secure tracking and/or telemetry data ingestion and repository

   iv. Secure remote device configuration

   v. Basic tracking data consolidation and report dashboard

b. Demonstrate the following operational mobility features and cloud-native applications:

   i. Basic User Identification (KYC) and Persona Management

   ii. Basic Service Registration for Shipping Lines, Forwarders, Brokers, Truckers, and Drivers

   iii. Basic Service Acceptance and Dispatch

   iv. Trucking/Trucker Location Monitoring

   v. Container Insurance Policy Coverage Availment

   vi. Delivery and Fulfillment Confirmation

   vii. Standards-based Payment Settlement Interface / Electronic Purse and Payment Services

c. Demonstrate the availability and accessibility of the following data registries:

   i. UN/LOCODE Registry

   ii. Country Registry

d. Proposed locations accompanied with a location map of available 10 hectare that is within the specified 50 km radius from the Port of Manila to house the empty container staging facility. TCT for owned / lease agreement/conditional lease agreement for leased area should also be submitted during bid opening.

DEPLOYMENT PERIOD:

The system must be deployed within the specified duration from the receipt of the Notice to Proceed (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-Boarding and 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 (refer to the policy development specifics under the performance target section of this document.	4	NTP+6
8. Deployment, Go-Live,and Operationalization	▪ Network Testing ▪ System Usability Testing ▪ Systems Integration Testing ▪ Stress Testing ▪ Vulnerability and Penetration Security Testing ▪ 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 device tagged containers ▪ Deployed field personnel for device attachment/detachment in PPA designated areas	7	NTP+9

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)	
	WARRANTY 1. The project contractor shall provide, 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 government. 2. The project contractor shall ensure that all hardware equipment is covered by a replacement/maintenance agreement throughout the term of the contract. **3.** The project contractor shall ensure that all subscriptions, licenses, and support agreement remain active throughout the duration of the contract.	
	All other provisions stated in the Terms of Reference not included herein.	

TERMS OF REFERENCE

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

BACKGROUND:

The Philippine Ports Authority (PPA) is the frontline agency mandated to regulate the port transactions, facilities, and operations that cover the movement of all persons, vehicles, and assets (whether private or public) that use the port under its administrative jurisdiction.

Section 6(a) of Presidential Decree (PD) 857, as amended, states that PPA shall have the corporate duty to supervise, control, regulate, construct, maintain, operate and provide such facilities or services as are necessary for the ports vested in, or belonging to PPA.

Further, Section 26(a) states that PPA may, after consultation with relevant government agencies and stakeholders, make rules or regulations for planning, development, construction, maintenance, control, supervision, and management of any port or port district and the services to be provided therein, and for the maintenance of good order therein, and generally for carrying out the purposes of the PD.

PPA is in the best position to take advantage of the first instance of disclosure as vessels are already required to submit detailed information for port entry giving PPA first access to data in establishing a reference baseline from the first disclosure of data. This enables PPA to establish provenance as it is technically, the first government agency that has full access to fully disclosed data.

With provenance established, PPA is then able to provide important contextual information that is useful to other regulatory, revenue collection, and law enforcement agencies in building necessary correlations that will strengthen its profiling capabilities. The PPA is the logical source of actionable intelligence for all things and persons entering Philippine territory via seaports.

In recognition of the mandate of PPA and the need to establish an explicit registry of containers entering the Philippine ports, PPA Administrative Order (AO) No. 04-2021 entitled, "Policy on the Registration and Monitoring of Containers" was issued on September 22, 2021 and took effect on October 19, 2021.

Section 5.1 thereat states that PPA shall acquire the necessary technology solution for the implementation of the registration and monitoring system that will have the following features:

- Facility to record all containers passing in and out from the port terminals;
- Provide a real-time monitoring facility of the location, status, and movements of containers from the time the container is discharged from the vessel up to the time the same container is loaded for export; and

- Easily interfaced with the existing container monitoring or tracking system of other concerned government agencies as well as port terminal operators, as may be necessary.

In line with the provisions of AO No. 04-2021, PPA intends to procure a Trusted Operator Program - Container Registry Monitoring System (TOP-CRMS) that will introduce rational, cohesive, and integrated solutions which will solve persisting systemic problems affecting the overall performance and efficiencies of the PPA in areas related to its frontline and regulatory services, third-party managed services, monitoring, and enforcement services, and inter-agency services.

The TOP-CRMS is intended to establish a "high-trust" foundation between government and private economic operators to optimize procedural efficiencies through the establishment of transactional transparency that international and local private operators (that constitute what is referred to as the "port community") extend or share with regulatory authorities to reduce procedural delays arising from the need of the regulator to have every transaction subjected to scrutiny and re- validation.

1. GENERAL OBJECTIVES:

The objectives of the TOP-CRMS program are as follows:

a. To create and institutionalize a sustainable trust framework that establishes the foundation for the PPA to a) improve its operational efficiencies b) improve its public-facing services, and c) enhance and continually improve levels of customer satisfaction by providing the necessary systems.

b. To implement and institutionalize the PPA Container Registry and Monitoring System that aims to streamline transactions in support of the trade facilitation, ease of doing business, border protection programs of the national government.

c. To acquire, implement, and manage a complete, full-stack, turnkey system that will equip the PPA with the capability to implement, manage, and sustain a credible and non-repudiable registry of all inbound shipping containers, its utilization, movement, and location within the Philippine jurisdiction, the identities of customers that use inbound shipping containers and the identities of the service providers that handle and transport shipping containers.

d. To provide a credible record to enable the PPA to accurately collect all required regulatory storage fees, and/or penalties as may be required by the PPA and other revenue collection agencies of government.

To provide a credible data service that promotes transactional transparency, enhanced security, while promoting the proper and proportionate use of data to provide regulatory agencies with credible information and to objectively help lower the cost of doing business on the part of local importers.

e. To establish and institutionalize a system of empty container storage shared services facilities to alleviate storage problems for laden containers and augment the capabilities of the PPA.

f. To streamline the payment process and collection of port fees and harmonize it with the existing e-payment system of the PPA.

g. To have an integrated system that can generate credible, immutable, and highly available data which can be used for analytics, reporting, and decision support purposes of the PPA.

2. GENERAL DESCRIPTION OF THE PROJECT

The supply, delivery of the full technology stack, the financing, technical implementation services, and managed services to successfully implement TOP-CRMS of PPA.

The TOP-CRMS program will be launched and rolled out covering two (2) pilot ports that house 98% of all container traffic. These are at the Port of Manila (POM): Manila International Container Terminal (MICT); and Manila South Harbor (MSH), inclusive of three (3) PEZA locations (for detachment and re-attachment of tagging devices of containers entering/leaving PEZA zones), as defined/required by the PPA.

The TOP-CRMS consists of the following, inter-related program components: the Trusted Operator Program, the Container Identification, and Control Program, the Container Tracking Program, the Container Accountability, and Insurance Protection Program. Each of these sub-programs targets specific functional contexts and form the collective whole.

3. BUDGET FOR THE CONTRACT

PPA intends to apply the sum of **Nine Hundred Eighty Million Pesos Only (Php980,000,000.00)**, exclusive of 12% VAT.

The service fee shall be the basis for the financial bid and shall not exceed the amount of **Four Thousand Nine Hundred Pesos (Php4,900.00)**, exclusive of 12% VAT, per tagged container.

Item Description	Cost per Tagged/Serviced Container (Upper Threshold)	Total
TOP-CRMS Turnkey Managed Services	Php 4,900.00	Php 980,000,000.00

4. BIDDER'S QUALIFICATION

1. Given the nature of the system and services required by PPA and to ensure the successful delivery and operation of the envisioned Project, the prospective bidder must have the following current ISO certifications:

    a. ISO 9001:2015
    b. ISO 27001:2013
    c. ISO 27017:2015
    d. ISO 27018:2014 and
    e. ISO 27701:2019

2. All certifications must be current and active at the time of bid submission.

3. To ensure that the prospective bidder has the requisite experience and financial capacity to successfully deliver the project, the prospective bidder must:

    a. Be in continuous operation with combined experience as a service provider, information system provider, systems developer, and systems integrator for at least ten (10) years at the time of bid submission.

    Have a minimum of 10 hectares of available area, accessible by major roads, within a 50km radius from international container terminals in Manila for use as a secure container staging facility or container depot for re-exporting empty containers.

    b. Delivered projects (local or international) for either a government agency or private sector company with a value of not less than Four Hundred Ninety Million Pesos (PHP490,000,000.00) within seven (7) years at the time of bid submission.

    c. Similar project refers to a contract that involves designing, implementing, deploying, and operating the managed services of a comprehensive managed services operations and technology solution for a government agency or private company that includes transactional applications that produce official issuances or provide location and identification management, issuance of permits, tickets, identification card processing, identification matching, KYC, or implementing and monitoring location-locked systems, machines, or devices.

5. POST QUALIFICATION REQUIREMENTS

5.1 The prospective bidder must already have an available software of a TOP-CRMS inclusive of a Cloud-based solution during post qualification.

5.2 The prospective bidder must be able to conduct a systems demonstration for technical evaluation to determine if functional requirements are at least 50% fit in accordance with the specifications provided in Annex A of this TOR.

5.3 The proposed solution is uniquely designed to primarily meet the regulatory capabilities of the PPA. As such, the Authority recognizes that the solution in its final form will be a system that integrates several commercial-off-the-shelf and operational software technologies, interfacing a variety of physical devices, and will also consist of multi-protocol/multi-modal network connectivity that will need to be customized or configured to meet the exact specifications of the envisioned PPA system.

5.4. To ensure that the solutions proposed by prospective bidders are functional and operational systems, each bidder will be required, as a post-qualification requirement, within five (5) days from being issued a post-qualification notice by the Authority, to demonstrate that components intended for full functional/operational integration system demonstrate the following:

a. Demonstrate an operational tracking device with the following out-of-the-box (OOTB) features:

   i. Network connectivity (local network)
   ii. Network reach and successful data transmission within 200km radius from the PPA Headquarters
   iii. Secure tracking and/or telemetry data ingestion and repository
   iv. Secure remote device configuration
   v. Basic tracking data consolidation and report dashboard

b. Demonstrate the following operational mobility features and cloud-native applications:

   i. Basic User Identification (KYC) and Persona Management
   ii. Basic Service Registration for Shipping Lines, Forwarders, Brokers, Truckers, and Drivers
   iii. Basic Service Acceptance and Dispatch
   iv. Trucking/Trucker Location Monitoring
   v. Container Insurance Policy Coverage Availment
   vi. Delivery and Fulfillment Confirmation
   vii. Standards-based Payment Settlement Interface / Electronic Purse and Payment Services

c. Demonstrate the availability and accessibility of the following data registries:

   i. UN/LOCODE Registry
   ii. Country Registry

d. Proposed locations accompanied with a location map of available 10 hectares that is within the specified 50 km radius from the Port of Manila to house the empty container staging facility. TCT for owned / lease agreement/conditional lease agreement for the leased area should also be submitted during the bid opening. Multiple TCT is acceptable, however, the area should be contiguous.

6. SCOPE OF WORK

6.1 Physically tag and monitor a minimum of 200,000 containers

6.2 Deliver, install, customize, configure, deploy, and implement a TOP-CRMS for the Philippine Ports Authority.

6.3 Set up and operationalize 24/7 field operations for the attachment and detachment of tagging devices in the following locations, namely: The Port of Manila: MICT and MSH; and three (3) PEZA locations, as defined/required by the PPA.

6.4 Provide support services necessary to ensure the exchange of information as well as hardware, software, network, databases, and information systems/application systems that are fully integrated and operational.

6.5 Provide the following implementation services:

6.4.1 Functional / Procedural Engineering, Re-Engineering, and Change Management

6.4.2 Policy Evaluation, Design, and Development

6.4.3 Technology Implementation

6.4.4 Business Development, Marketing, and Communications

6.4.5 10-hectare Area for Empty Container Re-Export Staging and Tagging Device Detachment

6.5 Include in its Operations, Maintenance, and Support Plan, among others, the following information:

6.5.1 Staffing plan and Number of Support Staff

6.5.2 Location and Operational Processes

6.5.3 Minimum Service Levels, such as:

6.5.3.1 Immediate Help desk response time for various classes of problems.

6.5.3.2 On-site support within 4 hours of the reported incident

6.5.4 Usage statistics

6.6 Provide a risk management plan detailing the strategies and appropriate measures to be undertaken. The plan should detail the following:

6.6.1 Risk Management Organization and Responsibilities

6.6.2 Risk Management Structure and Procedures for planning, identification, assessment, handling, and monitoring.

6.7 Provide a Disaster Recovery Plan which must contain the comprehensive procedures necessary to resume business to its normal operation in the least possible time for emergency response, backup, and recovery.

6.8 Provide complete documentation for every deliverable. PPA shall own all documents and shall reserve the right to reproduce at no additional cost.

6.9 Provide sufficient area for the staging of containers and detachment of tracking devices.

7. RESPONSIBILITY OF THE WINNING BIDDER

The winning bidder shall be responsible for the provision of the following components for the entire duration of the contract:

7.1 Technology

7.1.1 TOP-CRMS with perpetual licensing and annual support and maintenance included for the whole duration of the Contract.

7.1.2 Hybrid and/or Multi-Cloud Infrastructure (Compute and Storage)

7.1.3 Cloud-Based High-Performance Computing Server

7.1.4 On-Premise Backup and Enterprise Storage System

7.1.5 Network, and Application Security Appliance

7.1.6 Trusted Operator System

7.1.7 Container Identification and Control System

7.1.8 Container Accountability and Insurance Protection System

7.1.9 Tracking Device, Communications Network, and Monitoring Systems

7.1.10 Computing and Storage, Cloud Infrastructure, and Connectivity Systems

7.1.11 Frontline and Mobile Transactional Applications Systems

7.1.12 Enterprise Applications, Middleware, Data Processing, Data Management, and Reports and Analytics Systems

7.1.13 Data Protection and Security Systems

7.1.14 Account and Profile Management System

7.1.15 Development and Deployment Platform

7.1.16 Turnkey Environment for Tracking Devices and Communications Network

7.1.17 Payment Aggregator and secure API connector services to standard, local, and international payment gateway systems, and/or electronic money issuers

7.1.18 Cloud security and Threat Analytics

7.2 Services

7.2.1 Supply, Delivery, Installation and Commissioning of the TOP-CRMS System, Engineering, Implementation, and Support Services

7.2.2 Project and Technical Implementation Services

7.2.3 Systems Administration Services

7.2.4 Dedicated Technical and Helpdesk Support Staff

7.2.5 Operations Management Services

7.3 Network Connectivity

7.4 Courseware Materials and Training Conducts

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

7.5 Post- Production Container Operator On-Boarding Support

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

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

7.6 Post-Production Software and Equipment Support and Maintenance

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

The winning bidder shall also provide a replacement for all damaged parts and equipment that are covered under the prescribed warranty period, within 24-hours of being reported as inoperable or at the time the same has come to the knowledge of the service provider, whichever comes first.

7.7 Technical Support and Customer Help Desk

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

.

8. OPERATIONAL AND FUNCTIONAL REQUIREMENTS, DESCRIPTIONS, AND SPECIFICATIONS

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

Functional Components

Trusted Operator System	This functional program sub-group will provide the required conventional and mobility systems and technology infrastructure to capture, store, and process subscription and transactional activities and integrated services made availableto trusted operators.
Container Identification and Control System	This functional program sub-group will provide the required conventional systems, mobility systems, and technology infrastructure to enable the PPA to digitally capture using industry-accepted data interchange formats, through secure and encrypted channels, all inbound shipping containers in advance or before its entry in any port of the country.
Container Tracking System	This functional program sub-group will provide the conventional systems, devices, and technology infrastructure (hardware, software, data management) to enable the PPA to digitally tag all inbound shipping containers witha tracking device (attached to the container asset while remaining in the country) giving the PPA full visibility of the utilization, movement, and location of every foreign-ownedcontainer.
Container Accountability andInsurance Protection System	This functional program sub-group will provide local importers access to container insurance services, and will also provide the PPA the ability to monitor financial transactions required by shipping lines for all inbound shipping containers to safeguard the revenue interests ofthe government.

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

Software-Based Components	
System Group	System Module / Feature Components
Tracking Device, Communications Network, and Monitoring Systems Group	The solution must have the following minimum devices, standard turnkey capabilities, and services: ▪ IP67 Certified Tracking Devices ▪ Network Gateways ▪ Receiver Base Stations ▪ High-speed Broadband Network Interconnectivity ▪ Tracking Device Management System ▪ Cloud Data Repository ▪ Device Monitoring Service ▪ API Web Service Endpoint Services
Frontline and Mobile Transactional Applications Systems Group	The solution must have the following minimum standard turnkey capabilities andservices: ▪ Program Portal CMS ▪ System Account Registration and SecureLogin
Software-Based Components	
System Group	System Module / Feature Components
	▪ Enrollment and Registration Services

	(Shipping Line, Vessel and Voyage, Driver, and Vehicle) ▪ User Profile and Account Management Services ▪ Container, Driver, and Transport Management Services Mobile Application(Transaction Dispatch, Driver Acceptance, Delivery Confirmation, Yard Entry/Exit Tagging, Road Emergency Report Service) ▪ Shipping Container Registry ▪ Vehicle Mapping Service ▪ Container Protection Disclosures ▪ Container Insurance Enrollment Services ▪ FAQs, User Help Desk and Online Support ▪ API Web Service Endpoint Services
Enterprise Applications, Middleware, Data Management, Data Processing, Reports, and Analytics Systems Group	The solution must have the following minimum standard turnkey capabilities and services: ▪ Enterprise Applications o Systems and User Administration Management o System Access and Permissions Management o Subscriber Profile Records Management o Subscription Management o Subscriber Benefits Administration and Management o User Transactions Monitoring o Risk Exceptions Processing o Case Management o Invoicing and Billing ▪ Middleware and Integration o Application Registry / Catalog Service o API Web Service Endpoints Catalog Service o Business Orchestration Service (Business Process and Rules Management, Workflow and Route Management Engine) o Operations Management Platform o API Gateway Management ▪ Service

	▪ Data Management o Open Standards-based Databases (Relational DatabaseManagement System (RDBMS),NoSQL Database Management,Flat-file Storage System) o Big Data Repositories (Data Lake System, Data Warehousing, DataMart) o Data Management (Data Management and Administration, ETL Management Tool, ReferenceData Registries) ▪ Analytics and Visualization: o Executive Dashboard o Data Streaming Engine o Risk and Compliance Profiling Reports Visualization
Data Protection and Security SystemsGroup	The solution must have the following minimum standard turnkey capabilities and services: ▪ Data Encryption and Protection (encryption-in-flight / encryption-at-rest) ▪ Network Security (Edge Protection, CDN, Optimization) ▪ Cloud Security and Workload Protection ▪ Malware Scanning, Detection, Detonation, Inoculation, Attribution, andReporting ▪ Vulnerability and Penetration Testing ▪ Cybersecurity Threat Monitoring

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

System Group	Frontline Transactional Application Systems
Business Requirement	**Functional Specification**
Program Portal and Unified CMS	▪ The Unified Portal must provide an open standards-based Content Management System (CMS) that will serve as the unified access service or portal service for public and agency users to centrally access the system. ▪ The CMS must be based on current web-responsive technologies ▪ The CMS must provide features that allowcontent creators, designers, copywriters to securely publish both static and dynamic content. ▪ The CMS must provide features that allowend-users to extend and scale functionalities to meet current and emerging content publication needs. ▪ The CMS must provide features that consolidate the library of end-user applications accessible via a single portalwith a cohesive, end-user configurable, user experience ▪ The CMS must provide end-users accessto a rich library of web templates ▪ The CMS must provide features for personalization. ▪ The CMS must provide features to seamlessly integrate with current SAMLor OAuth-based Single Sign-On (SSO) capabilities. The CMS must provide a native API web service endpoint (JSON, XML) for modulesecurity, integration, and accessibility
System User Registration Service	▪ The System User Registration service must provide features and functions forthe public to register online to create an account. ▪ The service must provide provenance-enabled features that allow new registrants to: o Create their initial login credentials (username andpasswords) o Define the number of applicable system personas o Define organizationalaffiliations o Provide basic user data (name, DoB, address, primaryand secondary email address, mobile number, etc.) ▪ Upon successful access registration, theservice must be able to generate a standard user identity QR code that will be readable and usable throughout the entire system. ▪ The module must provide a native API web

	service endpoint (JSON, XML) for module security, integration, and accessibility.

System Group	Frontline Transactional Application Systems
Program Enrollment Service	▪ The program enrollment service is the primary application for existing registered system users to enroll in the Trusted Operator Program of the CRMS. ▪ It must provide features that enable enrollees to: o Complete the program enrollment using an online application form o Submit a current digital photo o Submit digital copies of required program documentation o Provide digital references to other government identification, permits/license, or accreditation systems ▪ It must provide native digital workflow routing features for application processing, disposition, and approval ▪ It must provide enrollees with a visual process map showing the details and status of their application, indicating who is handling their application and when it was received by the processor. ▪ Upon successful access enrollment, the service must be able to generate a standard QR code that will be readable and usable throughout the entire system. ▪ The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.
Shipping Container Registration and Identification Service	The shipping container registration and identification service enable all foreign shipping lines to submit a complete inventory of all foreign-owned containers that enter Philippine ports. ▪ The service must allow foreign shipping lines the ability to perform secure bulk uploads (*.csv, *.xlsx, *.odt formats) submission of their container inventory that enters Philippine ports ▪ The service must comply with UN/CEFACT standards for shipping container data exchange format. ▪ The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.
Advanced In-Bound ContainerDeclaration	▪ The in-bound container declaration service is an online bulk submission service to enable shipping lines to transmit data on all inbound containers in

	advance or before arrival. ▪ The service must allow foreign shipping lines the ability to perform secure bulk uploads/submission (*.csv, *.xlsx, *.odt formats) of their in-bound container inventory in advance. ▪ The service must provide a downloadable spreadsheet template that users can use to bulk upload all in-bound containers in advance. ▪ The service must comply with UN/CEFACT standards for shipping container data exchange format. The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.
Advanced Port Services Booking	▪ The advanced port services booking is a service available only to registered and subscribed Trusted Operators of the CRMS enabling subscribers to schedule berth entry, unloading and unloading, schedule with the TABS system of the PPA, and reserve storage. ▪ The service must integrate with current PPA container handling, discharge, transport, and storage services. ▪ The service must integrate with the following current PPA services: o Berth Scheduling

System Group	Frontline Transactional Application Systems
Business Requirement	Functional Specification
	o Unloading and Loading Scheduling o Trucker Advanced Booking System o Returns Scheduling and Storage ▪ The service must allow Trusted Operators to pay for all required fees for all services availed by the Trusted Operator via services of banks, registered EMV's, or online payment gateway services. ▪ Upon successful access enrollment, the service must be able to generate a standard QR code that will be readable and usable throughout the entire system ▪ The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.
Container Protection Disclosures	▪ The container protection disclosures service enables both shipping lines and local importers the ability to disclose financial transactions made

	against the use of foreign-owned shipping containers. ▪ The service must provide the functionality to enable *shipping lines* or their local representatives with the ability to disclose container protection options (container deposit, container maintenance, containerinsurance) and values paid by local importers either in bulk or per unit for the use of the shipping container. ▪ The service must provide the functionality to enable *local importers* or their designated brokers with the ability to directly associate the container protectionoption and the corresponding value or the amount paid for the use of a shipping container (per unit or in bulk). ▪ The system must be able to dynamically reference the foreign shipping line owner of a container ID number referenced by a local importer. ▪ The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.

System Group	Frontline Transactional Application Systems
Business Requirement	**Functional Specification**
Container Insurance Service Provider Registration	▪ The container insurance service provider registration enables private insurance providers to register to make their services accessible to importers or service subscribers via the online CRMS. ▪ Insurance providers must be enrolled and registered as subscribers to the Trusted Operator Program. ▪ The service must provide features forinsurance providers to: o Detail different insurance product offerings, the scope of coverage, value, and premiumamount, additional riders (if orwhen applicable) o Payment settlement options o Detail claims processing requirements ▪ The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.

Container Insurance Enrollment and Claims	▪ The container insurance enrollment service enables local importers the option to avail of container insurance coverage instead of paying for container deposit or container maintenance fees ▪ The service must: o Allow the local importer to electronically avail of insurance coverage for one or many shipping containers across one or multiple shipping transactions between one or many shipping lines o Enable insurance providers to electronically issue the insurance policy document covering one or multiple shipping transactions across one or multiple shipping lines ▪ The service must enable importers todirectly pay for insurance coverage. ▪ The service must provide features for local importers to electronically file for insurance claims. ▪ The service must also provide features that enable both the claimant (local importer) and beneficiary (shipping lines)to monitor the progress of claims submitted and in process The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.

System Group	Frontline Transactional Application Systems
Business Requirement	**Functional Specification**
Electronic Purse and Payment Services	▪ The electronic purse and payment services are the payment aggregation service of the system that enables the system and its subscribers to manage their payment transactions and connect tocurrent payment gateways, banks, or electronic wallets. ▪ The service must provide features that provide subscribers with a digital expense wallet with the native feature toconnect to one or several payment gateways and/or banks. ▪ The service must provide features that enable users to track and monitor payments as well as detailed ledgers ofhistorical payment transactions. ▪ The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.

Online Support and Chat	▪ The online support and chat service enables users and subscribers to accessonline help via live chat (regular business hours) or using guided/scripted chatbots 24x7 for the most common questions or help items. ▪ The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.

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

System Group	Account and Profile Management System
Business Requirement	**Functional Specification**
User Account Profile and Persona Management	▪ The user account profile and personal management service enable registered users to detail their personal information and detail the different personas (importer, broker, shipper, logistics provider, trucker, driver, etc.) that apply inthe use of the system. ▪ The system must allow users to managepersonal details, add, update, or modify personal details. ▪ The system must provide features thatgenerate a secure QR Code unique toeach user. ▪ The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.

System Group	Mobile Transactional Application Systems (Android)
Business Requirement	**Functional Specification**

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

System Group	Mobile Transactional Application Systems (Android)
Business Requirement	**Functional Specification**
Driver and Truck Dispatch Service	▪ The driver and truck dispatch service enable the service provider to managethe assigning of a driver or drivers to a specific truck or trucks and dispatch thesame to fulfill a work order. ▪ The module must provide native API webservice endpoints (JSON, XML) for module security, integration, and accessibility.

Job Acceptance, Delivery, and Fulfillment Confirmation	▪ The service must provide features that enable the driver to tag the actual time acontainer is hitched to a truck for transport and the time it completes a delivery. ▪ The module must provide native API webservice endpoints (JSON, XML) for module security, integration, and accessibility.

System Group	Mobile Transactional Application Systems (Android)
Business Requirement	**Functional Specification**
Container Tagging and Recording System	▪ The container tagging and recording service enable designated personnel to physically tag a container with a trackingdevice and associate the container reference identification with the tracking device. ▪ This service must-have features that enable it to directly exchange data with the Trucker Advanced Booking Systems and the gate management systems of each container port/yard. ▪ The module must provide native API webservice endpoints (JSON, XML) for module security, integration, and accessibility.
Container Release, Receiving, and Device Detachment	▪ The service must provide a gate management system (RFID or QR Code) to monitor the discharge and return of allshipping containers to and from the container yard. ▪ The application must also provide features that enable the management of device detachment before the re-exportof shipping containers. ▪ The service must provide four status options about the container, namely: discharged, returned, in-storage, and re-exported. ▪ The module must provide native API webservice endpoints (JSON, XML) for module security, integration, and accessibility.

Road Emergency Reporting	▪ The emergency reporting service enablesdrivers to report roadside incidents and communicate directly with the customer. ▪ The service must provide features that directly message all involved parties via the in-app messaging service, and electronic mail. ▪ The module must provide native API webservice endpoints (JSON, XML) for module security, integration, and accessibility.

System Group	Mobile Transactional Application Systems (Android)
Business Requirement	**Functional Specification**
Advanced Port Services Booking	▪ The advanced port services booking, is a concierge-type, red-carpet service available only to users subscribed under the Trusted Operator Program of CRMS. ▪ The service must provide features that enable users to schedule port services inadvance, that include the following: o Advanced Port EntryClearance o Advanced Berthing Appointment and Booking o Prioritized Unloading andLoading o Advanced Port ServicesPayment o Advanced TABS Appointmentand Booking ▪ The module must provide native API webservice endpoints (JSON, XML) for module security, integration, and accessibility.
Container Insurance Enrollment	▪ The container insurance enrollment service enables local importers the option to avail of container insurance coverage instead of paying for container deposit or container maintenance fees using a mobile application. ▪ The service must: o Allow the local importer to electronically avail of insurance coverage for one or many shipping containers across one or multiple shipping transactions between one or many shipping lines o Enable insurance providers to electronically issue the insurance policy document covering one or multiple

	shipping transactions across one or multiple shipping lines ▪ The service must enable importers todirectly pay for insurance coverage. ▪ The service must provide features for local importers to electronically file forinsurance claims.

System Group	Mobile Transactional Application Systems (Android)
Business Requirement	**Functional Specification**
	▪ The service must also provide features that enable both the claimant (local importer) and beneficiary (shipping lines)to monitor the progress of claims submitted and in process ▪ The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.
Electronic Purse and Payment Services	▪ The electronic purse and payment services are the payment aggregation service of the system that enables the system and its subscribers to manage their payment transactions and connect tocurrent payment gateways, banks, or electronic wallets using a mobile application. ▪ The service must provide features that provide subscribers with a digital expense wallet with the native feature to connect to one or several payment gateways and/or banks. ▪ The service must provide features that enable users to track and monitor payments as well as detailed ledgers of historical payment transactions. ▪ The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.
Online Support and Chat	▪ The online support and chat service enables users and subscribers to accessonline help via live chat (regular business hours) ▪ The online support must provide guided/scripted chatbots 24x7 for the most common questions or help itemsusing a browser or mobile application. ▪ The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.

Vehicle Mapping Services	▪ The vehicle mapping is a software-basedservice that enables parties involved in atransaction to track the location of a vehicle using a mobile application.

System Group	Mobile Transactional Application Systems (Android)
Business Requirement	Functional Specification
	▪ The service must-have features that couldsend or stream the location of the user to a designated analytics and reporting system. ▪ The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.

System Group	Enterprise Application Systems
Business Requirement	Functional Specification
Systems Access and Permissions Management	▪ The systems access and permissions management enable system administrators to define, assign, modify, revoke, or terminate end-user permissions at defined levels of granularity. ▪ The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.
Systems and User Administration Management	▪ The systems and user administration management enables systems administrators to define, assign, modify, revoke, or terminate systems users or designated functional administrators. ▪ The service must provide centralized administrative features that enable systems administrators to manage everycomponent of the deployed system, inclusive of the CMS, web forms, cloud infrastructure, orchestration, middlewareand integration, API management, database management, big data, and analytics system. ▪ The module must provide a native API web service endpoint (JSON, XML) for module security, integration, and accessibility.
Subscriber Administration and Management	▪ The subscriber administration and management enable the systems administrator to define and configuresubscriber programs. ▪ The service must provide functions that enable systems administrators to define requirements, define permissions, define and configure allowed functions (such aspersonalization and messaging). ▪ The service must provide functions that enable systems administrators to define and configure features available to functional users.