Procedures in Submission and Opening of Electronic Bid

1. Upon submission of a duly filled-up LBP Secure File Transfer Facility (LBP SFTF) User Registration Form together with copies of LANDBANK Official Receipt and Payment Acceptance Order for non-refundable bidding fee to the HOBAC Secretariat, the prospective bidder shall receive an email with log-in credentials to access the LBP SFTF.

2. The electronic bid shall be submitted by uploading the same in the LBP SFTF (please refer to the Guide in Accessing LBP Secure File Transfer Facility below). *Electronic bids received after the set deadline basing on the date and time on the electronic folders of bidders shall not be accepted by the HOBAC.* Thus, bidders are requested to upload their electronic bids at least two (2) hours before the set deadline.

3. The electronic bid consisting of two copies/files shall be labelled with bidder's *assigned* short name, last seven (7) digits of the bidding reference number including the parenthesis if there are any, and bid copy number, each separated with a dash sign. Thus, for a project with bidding reference number LBPHOBAC-ITB-GS-20200819-01(2) that XYZ Company wants to bid on, the archived files shall be labelled as XYZ-081901(2)-C1 and XYZ-081901(2)-C2. The archived files shall be generated using either WinZip, 7-zip or WinRAR and password-protected.

   Each of the above mentioned archived files shall contain the Technical Component and Financial Component files. The PDF files shall be labelled as above plus the word "Tech" or "Fin" in the case of the Technical Component and Financial Component, respectively. Thus, using the above example, XYZ-081901(2)-C1 shall contain the PDF files labelled XYZ-081901(2)-C1-Tech and XYZ-081901(2)-C1-Fin while XYZ-081901(2)-C2 shall contain the PDF files labelled XYZ-081901(2)-C2-Tech and XYZ-081901(2)-C2-Fin.

   In case of modification of bid, the qualifier "Mod" and a numeric counter indicating the number of times that the bid had been modified shall be added at the end of the filenames of both the archived and PDF files [e.g. First Modification: XYZ-081901(2)-C1-Mod containing XYZ-081901(2)-C1-Tech-Mod and XYZ-081901(2)-C1-Fin-Mod and Second Modification: XYZ-081901(2)-C2-Mod1, containing XYZ-081901(2)-C2-Tech-Mod1 and XYZ-081901(2)-C2-Fin-Mod1].

   All the required documents for each component of the bid shall be in one (1) PDF file and sequentially arranged as indicated in the Checklist of Bidding Documents. The documents must be signed by the authorized signatory/ies when required in the form.

Each of the archived files and the PDF files shall be assigned with a different password and these passwords shall be disclosed by the bidder only upon the instruction of HOBAC during the actual bid opening.

Electronic bids that are not assembled, labelled and password-protected in accordance with these procedures shall not be rejected/disqualified but the Bidder or its duly authorized representative shall acknowledge such condition of the bid as submitted. The HOBAC/LANDBANK shall assume no responsibility for the non-opening or premature opening of the contents of the improperly assembled, labelled and password-protected electronic bid.

4. The prospective bidder shall receive an acknowledgement receipt via email *after* successful uploading of its/his electronic bid. If no email is received within one (1) hour after successful uploading, the bidder shall call the HOBAC Secretariat at (02) 8522- 0000 local 2609 to confirm whether the submission has been received, and if so, request for the acknowledgment of receipt of the electronic bid.

5. On the bid opening date, the bidder shall confirm its/his participation in the online meeting with the HOBAC Secretariat at least one (1) hour before the scheduled meeting. The bidder shall be able to log in into MS Teams and join the Waiting Room of the HOBAC meeting. Only one account/connection per participating bidder shall be allowed to join the meeting. If the bidder has more than one (1) representatives, the said representatives may take turns in using the allowed account/connection.

6. Projects with participating bidders in attendance shall be given priority in the queuing.

7. Upon the instruction of the HOBAC Chairperson to start the bid opening activity, the HOBAC Secretariat connects the participating bidder/s to the videoconferencing/group calling session. The HOBAC Secretariat shall record the session and act as Moderator of the meeting all throughout.

8. Once the connections are in place, the HOBAC, with the assistance of the HOBAC Secretariat, retrieves the archived file from the LBP SFTF and opens the same. The Technical Proposal shall be opened first. Upon instruction from the HOBAC, the bidder concerned shall disclose the passwords for the archived file and the PDF file of the Technical Component.

In case an archived/PDF file fails to open due to a wrong password, the specific bidder shall be allowed to provide the HOBAC with passwords up to five (5) times only. The same number of attempts shall apply to Copy 2 of the bid, in case there is a need to open it. If the archived/PDF file still could not be opened after the maximum allowable attempts, the bidder concerned shall be disqualified from further participating in the bidding process.

9. The HOBAC then determines the eligibility and compliance with the technical requirements of the specific bidder using a nondiscretionary "pass/fail" criterion. Only bidders that have been rated "Passed" shall be allowed to participate in the succeeding stages of the bidding process.

10. The HOBAC, with the assistance of the HOBAC Secretariat, shall then open the Financial Components of those bidders that have been rated "Passed". Upon instruction from the HOBAC, the bidder concerned shall disclose the password for its/his Financial Component.

11. The HOBAC, with the assistance of the HOBAC Secretariat, conducts bid evaluation and ranking of the bids. The results of bid evaluation and ranking shall be recorded in the Abstract of Bids, which shall be signed by the HOBAC Members and Observers. The result of evaluation and ranking shall also be announced to the participants.

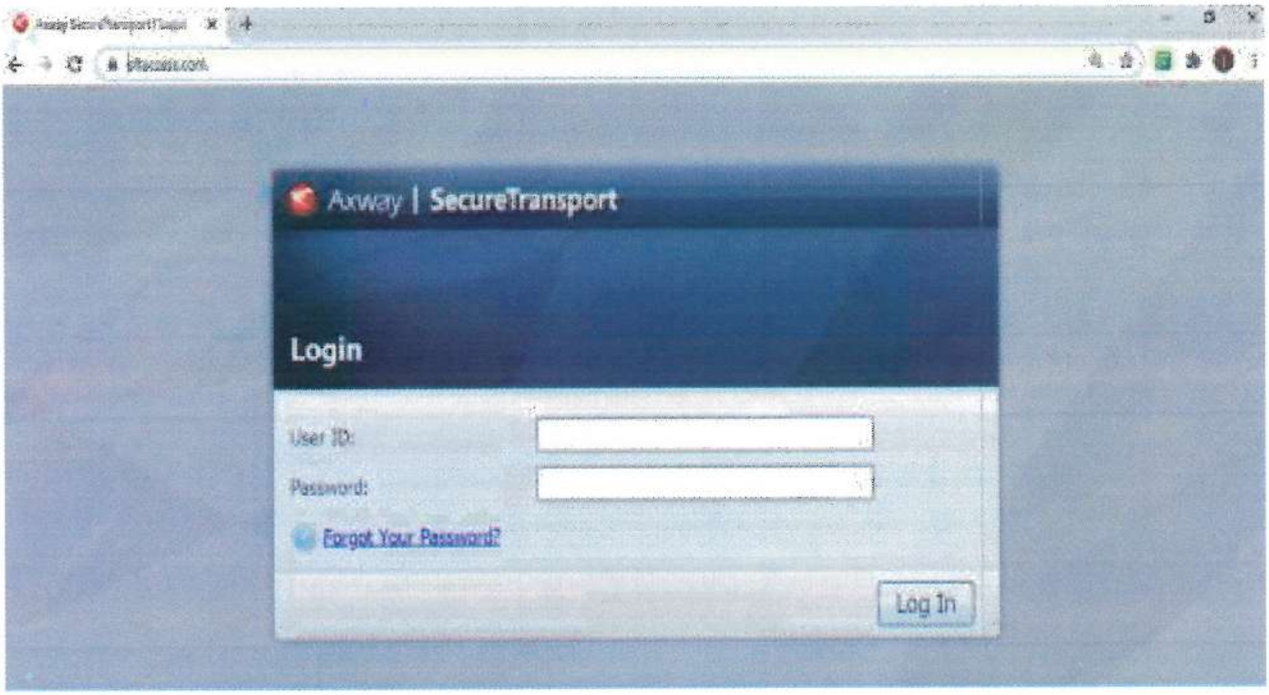
12. The retrieval and opening of the electronic bids, page-by-page review of documents and the results of the bid evaluation and ranking shall be shown to the participants through the screen sharing feature of MS Teams.

13. The access of the bidders to the videoconferencing/calling session shall be terminated once the Chairperson has declared that the bid opening activity for a specific project has been finished.

14. MS Teams Application shall be used in the conduct of online bidding. In the event that it is not available, other videoconferencing/group calling applications may be used as an alternative in conducting the meeting.

Guide in Accessing LBP Secure File Transfer Facility

1. Open browser and type the url: **https://www.sftaccess.com**



2. Log-in with the credentials provided via email. (Note: Log-in credentials will be received upon submission of a duly filled-up LBP SFTF User Registration Form together with copies of LANDBANK Official Receipt and Payment Acceptance Order for non-refundable bidding fee)

   Username: **[E-mail Address] e.g. bidder1@bidder.com**

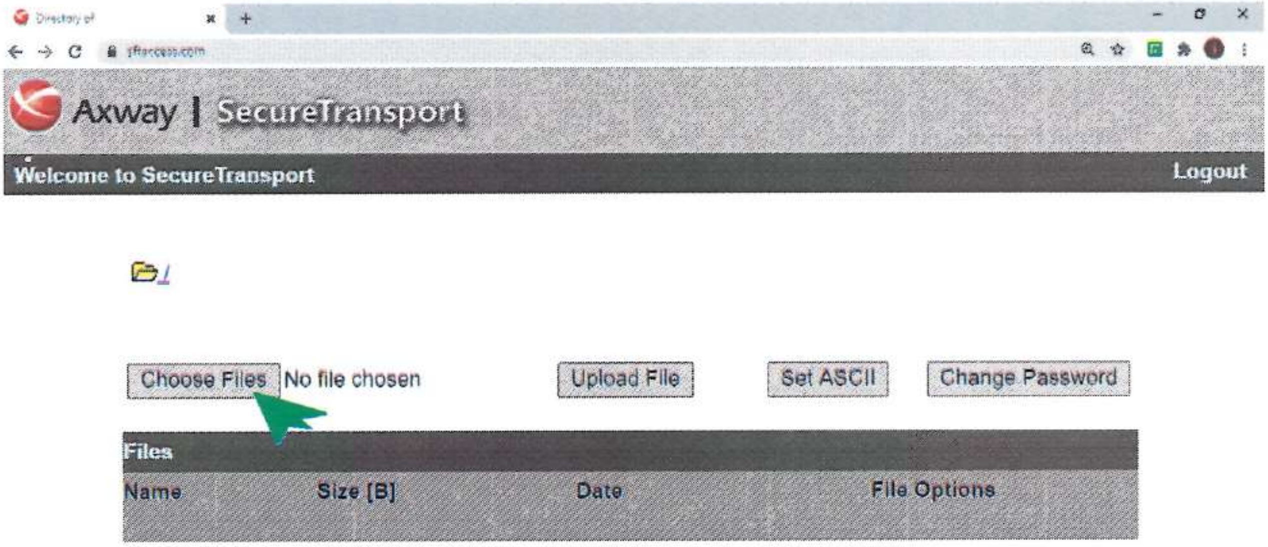
   Password: **[Landbank-provided password]**

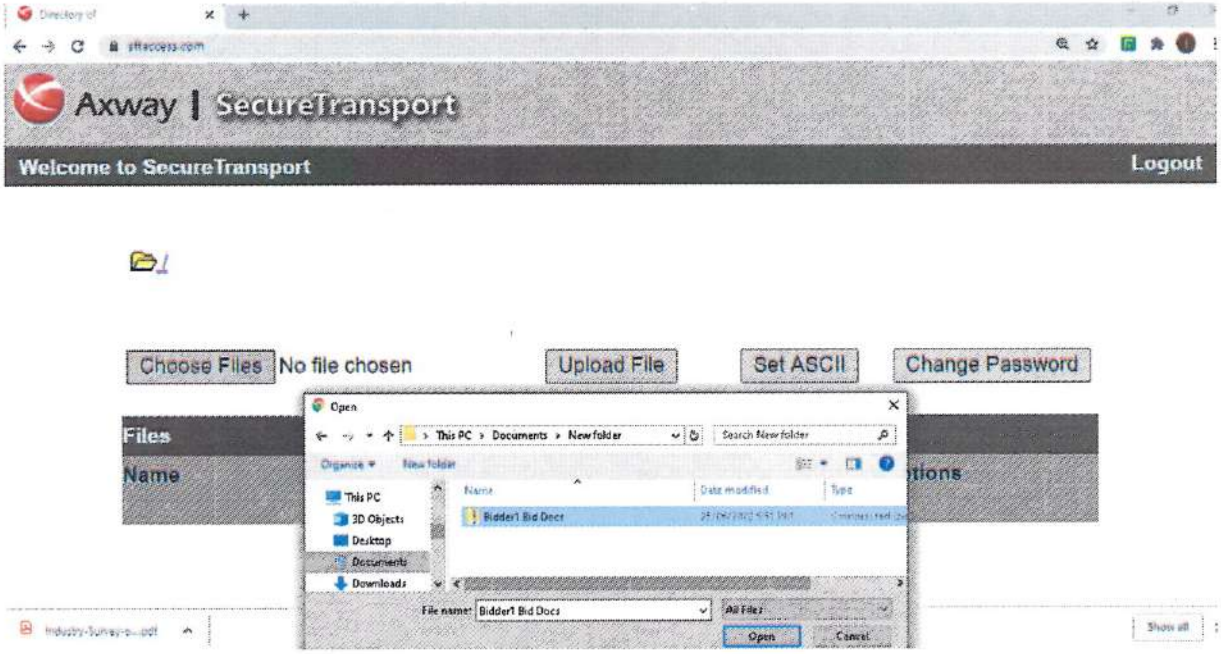
3. Upon successful login, click '**Choose Files**' to upload file/s.

Notes:

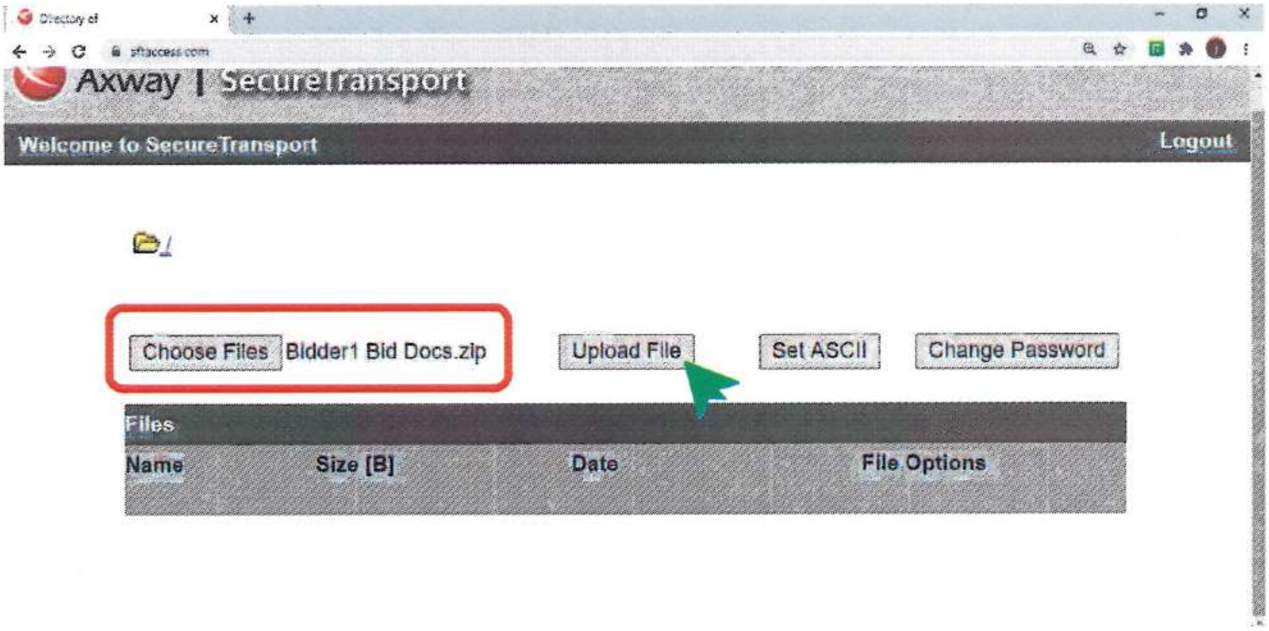
1. Files should be encrypted/password-protected.

2. Please follow the instructions in Item 2 of the above Procedures in Submission and Opening of Electronic Bids.

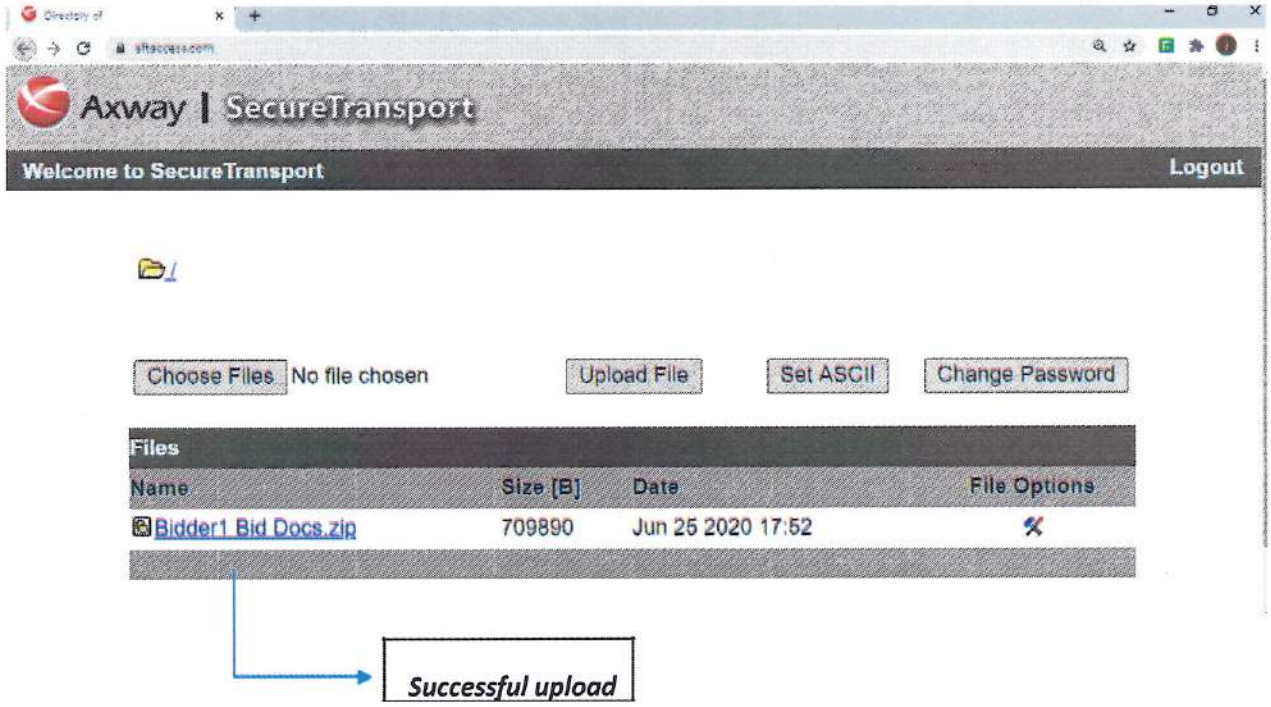




4. Click **'Upload File'** to upload the selected file/s.



5. Once a successful upload is completed, the files cannot be deleted anymore. The bidder will also receive a system-generated acknowledgement receipt in its registered e-mail address. A screenshot of the uploaded Bid/s should be taken by the bidder for record purposes.



Files

Name	Size [B]	Date	File Options
Bidder1 Bid Docs.zip	709890	Jun 25 2020 17:52	⚒

Successful upload

File Repository of Bid Documents

All uploaded bid documents will be stored in the dedicated SFTF directory of a particular bidder and will be accessible by the assigned ProcD personnel.

No revisions as of September 08, 2020

Supply, Delivery, Installation and Configuration of Security Information & Events Management (SIEM) Solution Term of Reference

Item	Description	Comply (Yes/No)
System Architecture and Hardware Requirements		
1	The solution must be delivered together with a Hyperconverged Infrastructure (HCI) with at-least 4 Nodes configuration.	
2	The hardware infrastructure must have a minimum of 24 Cores per Node	
3	The hardware infrastructure must have a minimum of 192GB of memory per Node	
4	The hardware infrastructure must have a minimum hybrid storage configuration of 10 x 12Tb SAS and 2 x 7.68Tb Solid State Drive (SSD) Hard Drives	
5	The hardware infrastructure must support 2 x 10GbE, 2port SFP+ Network Adapter with 10Gb SFP Transceivers and Fiber Patch Cords	
6	The solution must provide a unified browser-based platform that facilitates investigating, reporting, alerting, and administration.	
7	The solution must allow the flexibility to change the default communication ports.	
8	The solution must support multi-nodes design	
9	The solution must create indexes and meta data on the captured network traffic for fast searching and retrieval. Capturing and storing of network packets will be on a different appliance from the indexing appliance.	
10	The solution must use a purpose built internal data store that does not rely on external systems.	
11	The solution must be able to operate in out-of-band mode.	
12	The solution must support IPv6.	
13	The solution must provide redundancy to prevent any single component failure.	
14	The solution must provide support for usage of 3rd party storage	
15	The solution must support the full deployment (entire SIEM Stack) on Amazon Web Service (AWS).	
16	The solution must support up to 10G real time ingestion of Network Packets and 30K real time ingestion of logs via a single server (1 server for network packets and 1 server for logs)	
Hardware Technology and General Requirements		
17	The proposed Hyperconverged Infrastructure shall include the following sub-systems: a) Commodity off-the-shelf Combined Network, Storage, and Compute infrastructure with the following technical requirements: b) Network operating system combining software-defined storage, and built-in virtualization c) Professional Services for Deployment, User Acceptance Training (UAT) and Systems Documentation	
18	The proposed HCI shall be a high performance, scalable and flexible on premise, cloud platform solution that allows scale out or scale up growth dynamically without any limitation. Standard and advanced functionalities shall be achieved without the need to make architecture changes or without the need to invest in third party devices or software. Systems that requires the use of specialized, dedicated hardware or components will NOT be considered.	
19	The proposed Hyperconverged Infrastructure shall be a Combined Network, Storage, and Compute appliance based solution.	
20	The proposed Hyperconverged Infrastructure shall deliver a combined compute, network, storage, and virtualization platform that is scalable to meet workload demands, without the complexities and limited scalability of siloed systems.	

REVISED ANNEX C-1

21	The HCI must be able to run multiple hypervisors. Support for Vmware and HyperV is Mandatory	
22	The HCI should be able support both hybrid and all flash node models. The mix and match of these models should be supported in the same cluster.	
23	The proposed HCI should have built-in self-service cloud capability that allows customers to define quotas and create template and cataloguing as needed.	
24	The HCI shall provide automated provisioning of infrastructure, applications and custom services through a unified, web-based, multi-tenant self-service IT service catalogue.	
25	Must provide a single platform for running VMs, Block Services for a bare metal workload and File Services (CIFS & SMB Protocol). These services should be natively available in the platform without use of any third party tools.	
26	Should be 100% software defined without dependency on any proprietary hardware device. Hyper converged solution must have Deduplication and Compression features	
27	Should provide the ability to enable / disable data services for specific applications that the company feels are not suitable for compression / de-dupe.	
Deployment Requirements		
28	The proposed HCI shall be deployed using commodity off-the-shelf servers.	
29	The proposed HCI shall be deployed using only Ethernet standard for management and data connectivity.	
30	The proposed HCI shall be configured and deployed using web-based tools for simplicity and ease of deployment.	
31	Proposed HCI should be 100% software defined without dependency on any proprietary hardware device. Hyper converged solution must have Deduplication and Compression features	
Resiliency and Data Protection Requirements		
32	The proposed HCI shall not have a single point of failure in its architecture. It shall meet the following resiliency requirements. a. N+1 redundancy for power supply for ability to run on a single power source b. A distributed file system for resiliency in case of storage module failure. c. Redundant network ports in case of link or port failure.	
33	The proposed HCI shall have a capability for quick remediation of hardware or software problems.	
34	The proposed HCI shall distribute data and workloads on at least 3 servers to avoid overloading remaining servers in case of server failure.	
35	The proposed HCI shall deliver a solution that allows applications to move from one server to another in case of server failure, or need for more resources. This capability shall be either automatic or manually controlled.	
36	The proposed HCI shall have a self-healing file system during server failure and replacement, to ensure continuous data availability.	
37	The proposed HCI shall be able to create local and remote copies of applications for data protection and availability. These copies can be on a similar Combined Network, Storage, and Compute appliance, a backup server, or cloud platform for flexibility and choice. These copies can be created on schedule or manually.	
38	The proposed HCI shall be able to replicate data from one hypervisor type to another.	
Hardware Performance Requirements		
39	The proposed HCI shall deliver a simple setup of combined performance and capacity storage modules, treated as a single pool of storage resource, for consistent and predictable performance.	
40	Ability to use a combination of high performance and low performance storage media (Flash / SAS / SATA / NL SAS)	
41	The proposed HCI shall distribute data and workloads on at least three servers to ensure consistent and predictable performance, in case of server failure.	

42	The proposed HCI shall deliver a solution that increases performance in terms of compute, storage, and network through seamless server upgrades.	
HCI Scalability and Efficiency Requirements		
43	The proposed HCI shall be upgradeable through scale up or scale out options. These upgrade options can be done online and are non-disruptive.	
44	The proposed HCI shall be able to share its storage resources using standard network storage protocols for lower operational cost. This ability should not require add on hardware or software to the platform.	
45	The proposed HCI shall be able to provision storage without fully provisioning the required capacity. This "grow as you use" capability will prevent wasteful overprovisioning.	
46	The proposed HCI shall be able provide a choice for upgrading compute and storage resources, or storage resource only. This provides flexibility to scale up only the resource that needs upgrading.	
47	The proposed HCI shall have storage efficiency capability that reduces data footprint and removes duplicate patterns of data. This will reduce storage cost and physical footprint.	
48	The proposed HCI shall have the capability to provide analysis to project the utilization of compute and storage resources. This will provide guidance to acquire additional resources, deallocate unused resources, or resize currently used resources.	
49	The proposed HCI network connectivity shall be upgradeable to 10Gb Ethernet by adding optional NIC module.	
50	Solution should be able to add storage only nodes in same cluster. Such adding of nodes should not result in additional hypervisor license cost	
51	The solution should have both hybrid and all flash node models. The mix and match of these models should be supported in the same cluster.	
HCI Ease of Use Requirements		
52	The proposed HCI shall not use proprietary modules, cables, connectors, or equipment. This will reduce required additional product or technology training and management. This will also provide ease of support in resolving hardware or software issues.	
53	The proposed HCI shall have a single point of support for compute, storage, network, and virtualization. This single point of contact approach provides a holistic and simple support structure.	
54	The proposed HCI shall use a single point of management, not requiring dedicated machines, appliances, or additional software or licenses. Single point of management shall be regardless of solution size or scale. The proposed HCI shall have a single pane of management for compute, storage, and virtualization. This reduces management complexity, training requirements, and allow quick identification and resolution of issues.	
55	The proposed solution shall provide a simple conversion process from one type of hypervisor to another.	
56	Solution should have its build-in self service capability	
57	The proposed solution must provide a single platform for running VMs, Block Services for a bare metal workload and scale-out file services. These services should be natively available in the platform without use of any third party tools.	
58	Solution should provide the ability to enable / disable compression & deduplication for specific applications that the company feels are not suitable for compression / de-dupe	
Analytics Platform		
59	The solution must provide a unified view across both packet data, logs, User & Entity Behaviour Analytics (UEBA) analysis and Endpoint detection and response solution within a single analyst console. The query must return with both network traffic and threat indicators associated to the subject (minimally IP Address, Hostname, Username, Detected threat indicators) in the same investigation view.	

60	The solution must create a complete ontology of searchable metadata across network traffic created at near-real time. It must use lexicon of nouns, verbs and adjectives to represent the captured data, to help analyst easily understand the captured log and traffic data.	
61	The solution must provide a free-form search engine that allows search string to search for events. The text search must provide these capabilities: 1. Use ANDed for Whitespace delimited word (For example, if search is done on Mark, Albert, both Mark and Albert must be found in the session but they need not be together or in specific order 2. Use OR (e.g. if you search Mark OR Albert, either Mark or Albert must be found in the session to match, both are not required) 3. Use ANDs and ORs in a mix and match manner with explicit OR having higher precedence than implicit (Whitespace) AND 4. Use – operator to exclude words from search result 5. Use Regular Expression 6. Search across RAW and META data	
62	The solution must provide a flexible dashboard with chart and summary displays for a complete view of real-time captured data. Dashboard must support geo-location tagging visualization detailing a world map and point of interested reflected on the map	
63	The solution must be able to output reports to remote network destinations via SFTP, Network Share (CIFS/NFS) and URL.	
64	The solution must be able to schedule reports and provide the flexibility to generate on-demand reports, and able to output report, not limiting to CSV and PDF formats	
65	The solution must provide fully customizable queries and report library to define report and alert combinations. The same query must be re-useable to create rule, alert or chart.	
66	The solution must support the following notification output formats to external systems: 1) Common Event Formats (CEF) 2) Simple network management Platform (SNMP) 3) Syslog 4) Simple Mail Transfer Protocol (SMTP)	
67	The solution must support direct drill-down from the reports and charts to the underlying network session, to allow further investigation and pivoting around events of interest.	
68	The solution should support correlation of network packets, logs, netflow and endpoint data (EDR) via a single platform through a common meta-data format	
69	The solution should support the following types of correlation: a) Rule-Based Correlation b) Statistical Based	
70	The solution should provide pre-built correlation rules and allow for modification and import/export of rules	
71	The solution should provide a wizard-based interface for rule creation and the rules should support logical operators for specifying various conditions in rules.	
72	The solution should provide the following regulatory standards reporting templates out-of-the-box: a) Basel II b) Bill 198 c) Family Educational Rights and Privacy Act (FERPA) d) Federal Financial Institutions Examination Council (FFIEC) e) Federal Information Security Management Act (FISMA) f) Gramm-Leach-Bliley Act (GLBA) g) Good Practice Guide 13 (GPG13)	

	h) Health Insurance Portability and Accountability Act of 1996 (HIPAA) i) International Standardization Organization 27002 (ISO 27002) j) North American Electric Reliability Corporation – Critical Infrastructure Protection (NERC CIP) k) National Industrial Security Program Operating Manual (NISPOM) l) Payment Card Industry (PCI) m) Sarbanes-Oxley Act of 2002 (SOX)	
73	The solution must support GeoIP location, name / IP address resolution, Google Earth visualization (or similar) and provide right click menu customization. The GeoIP capability must support both IPV4 and IPV6	
74	The solution must provide visual analytics on captured network data, log data and endpoint via a single user interface	
75	The solution must be able to integrate with Microsoft Active Directory to associate data and activity with a specific user.	
76	The analysis interface must support custom action to launch a 3rd party application or scripts.	
77	The solution must provide an Incident Management module to handle incident journaling, create, assignees, add context, and close incidents. All incidents must be searchable via a filter text box	
78	The solution must present aggregated incident in a nodal graph representation. The nodal graph will show connections in languages easily understood (e.g. belongs to, connecting to). For connections between source and destinations, if the number of connections are higher than other connections in the graph, the 'line' connecting the source and destination should be thicker to represent larger number of connections.	
79	Vendor must provide a complimentary lightweight endpoint EDR solution for collecting host inventories, processes, user activities, and Windows logs and must be installed on Windows, Mac or CENTOS platform.	
80	The vendor must conduct a Capture the Flag (CTF) exercise using the proposed solution or suite of solution from vendor to exhibit required/future added capabilities	
81	For UEBA, minimum of 1000 user licenses is required for the pilot project	
Log Capture and Analysis		
82	The solution must be able to capture logs from event sources and process in real-time.	
83	The solution shall be able to identify and interpret customized or proprietary logs.	
84	The solution must support the following log collection protocols; a) Syslog Event Sources (Syslog) b) File Event Sources (SFTP) c) Windows Event Sources (HTTP/HTTPS) d) ODBC Event Sources (ODBC) e) Checkpoint Event Sources (OPSEC LEA) f) SNMP Event Sources (SNMP) g) SDEE Event Sources (SDEE) h) VMware Event Sources (VMware)	
85	The solution must be able ingest of Netflow messages.	
86	The solution must be able to collect from older Windows versions such as Windows 2000 and Window 2003.	
87	The solution must be able to collect from Windows servers in multiple domains.	
88	The solution must include remote virtualized log collectors to create a lightweight, distributed, log collection infrastructure. Virtualized log collectors must be provided at no additional costs.	
89	The data transport between the remote log collectors and log processing facility must be encrypted. The events must be compressed before forwarding to the correlation/storage facility to maximize the bandwidth.	

90	The remote log collectors must be able to cache the events locally and deliver the events when the communication with the log processing facility resumes. The events must be compressed and encrypted when cached locally.	
91	The remote log collectors must support filtering or discarding of syslog events based on keywords or regex patterns.	
92	The solution must support both push and pull methods between the log collectors and the correlation/storage facility.	
93	The solution must support exporting of logs in the following formats; raw, csv, xml, json.	
94	The solution must support Amazon Web Service (AWS) log collection.	
95	The solution must provide a context lookup menu whereby within 3 clicks on an IP address will display all the incidents/security associated with the IP address	
96	The solution must provide the capability to selectively retain logs based meta-data	
97	The solution must support log collection for AWS and Azure	
98	The solution must support log collection plugin framework allowing support for new protocol or API, the plugin should be built in python	
99	The solution must support event source discovery that automatically detect mis-parsing of logs or logs that are parsed to multiple different log parsers. User must be able to correct the mis-parsing via the SIEM GUI	
100	The solution must provide User Entity Behavior Analysis (UEBA) capabilities as part of the solution (As optional add-ons). The UEBA solution must be from the same vendor providing logs analysis (SIEM) and packet analysis (DPI) capabilities	
101	The solution must support dynamic editing of logs parsers, add custom log parsers and update log parser rules via the solution's user interface	
102	Solution must provide the capability to for user to manually map a log source to a specific parser(Logs normalizer) directly from the solution User Interface (e.g. If Product A is mapped to Parser B, solution must provide the capability to manually map Product A to Parser A)	
103	The solution must retrofit virtually any application with logging capability that may not already be available, even custom applications	
Log Retention and Archiving		
104	The solution must provide the ability to define multiple retention policies based on time periods with a minimum of logs must be stored Three (3) Months On-line and One (1) Year Off-Line Retention, available in an easily accessible storage and immediate available for analysis (eg. Online, archived or restorable from backup), storage allocation, device type, governance, etc.	
105	The solution must enforce data retention policies automatically without necessitating manual data disposition or clean-up efforts.	
106	The solution must provide the ability to suspend the retention policy manually and allow administrators to increase the retention period dynamically for the purposes of evidence preservation in the event of pending litigation.	
107	The solution must integrate with existing NAS environment for storing log archives in a secure, easily retrievable manner. Logs must easily be restored for investigations.	
108	The solution must provide a simple interface to schedule the compression and archiving of log data to a NAS system	
109	The solution must provide a simple interface to manually archiving log data to a NAS system	
110	The solution must provide a simple interface to manually restore log data from a NAS system back to the log management system for historical analysis and reporting.	
Reporting and Visualization		
111	The solution must provide pre-defined, out-of-the-box reports for Operations, Security and Compliance that can easily be modified by customers.	
112	The solution must provide additional modules that can be added to the log management	

	platform to provide compliance auditing, alerting and reporting for governances such as SOX, PCI-DSS, NIST 800-53 and ISO 27002.	
113	The solution must provide the ability for customers to create their own reports and generate it manually or create schedule reports to run hourly, daily, weekly or monthly. There must be numerous output formats and delivery options for scheduled reports. templates, reporting wizard as well as an advanced interface for power users to create their own custom report queries.	
114	The solution reporting function must be capable of exporting reports in various formats. At a minimum, the report formats should be Excel Spreadsheet (.xls), Adobe Acrobat (.pdf), Word document (.doc), Web page (.html) and Comma-Separated Values (.csv). The reporting function should also allow the reports to be run and viewed ad-hoc by user as well.	
115	The solution must provide the ability for customers to schedule and email reports as either an attachment or a URL path for users who have log management system access.	
116	The solution reporting engine must provide the ability to generate linked reports with a master report that allows customers to drilldown into the data within the reports dynamically.	
117	The solution must provide a level of confidence that reporting will continue to work and not have to be modified if a particular technology, such as a Firewall or IPS product, is replaced with a newer product or vendor. The reports should continue to run and include the new technology into the report criteria automatically.	
118	The solution system reporting engine must provide the ability to filter, highlight, and modify various report functions at runtime. This should include the ability to selectively define which device group or storage partition to report upon.	
Alerting		
119	The solution must be capable of generating alerts based on filter pattern matches for operational health monitoring.	
120	In addition, the solution system must provide historical, threshold alerts, configured from saved search queries.	
121	The solution must provide pre-defined alerts and provide the ability to re-use pre-defined filters and customer created filters as alert criteria	
122	The solution must provide options of how alerts are delivered to Security Operation Center (SOC) team operations or security personnel. At a minimum the options must include reporting to the web console, send an email or generate an SNMP trap to an external management system. The solution must be capable of doing all three concurrently for each alert.	
123	The solution must be able to generate alerts based on below best practices Used Cases to various type of threats: • Brute force attempt • Domain Name Server (DNS) Reconnaissance • Denial of Service/ Distributed Denial of Service (DOS/DDOS): DoS/DDoS attacks 10,000 in 15 minutes • Anti-virus failed to clean or quarantine • Email with Malicious attachment • Database connections: unsuccessful connection attempts. • Device out of compliance (antivirus, patching, etc.). • Excessive SMTP traffic outbound • Excessive traffic inbound (streaming, web, etc.). • Excessive port blocking attempts from anti-virus or other monitoring systems • Excessive scan timeouts from anti-virus • Known Exploit Payload detected • Malicious Website	

	• Logs deleted from source • Suspicious traffic to known vulnerable host • Unauthorized subnet access to confidential data • Port Scan IPS from External to Internal • Ransomware Infection • Sinkhole Attack • System Compromise: Command and Control (CnC) communication • System Compromise: Suspicious Behavior • Waterhole attack • IRC Connections proceeded by Server Initiated Connection to Dynamic Hosts • Login to sleeping account: Login attempt to account that was unused for last • Admin Login Fail: Admin 3 Failed logins to any system within 24 hours • Freq. Account Locked: Frequent account locked 3 in 7 days [3/7d] • Login 1 to many: Login attempt from 1 station to more than 2 accounts • Login at off hours Night: Admin login in non-working hours 22:00-06:00 Sunday • Login more than 2 to 1: Login attempt from 3 stations to 1 account • Login Root: Login Directly to Root and not via "SU" • Malware Infections • Multiple Account Locking: Multiple locked accounts from same source IP • Multiple changes from administrative accounts • Same account different countries access attempt within 5 days (user traveled abroad) • SMTP traffic from an unauthorized host. • Privilege Elevation: Permissions were changes from user to Admin • Threat Intel Feed: IOCs detection • Trojan Infection • Virus Found • Vulnerable Software Version Detected	
Network Traffic Capture and Analysis		
124	The solution must be able to capture network traffic via network SPAN port of network tap and analyze it at real time	
125	The solution must be able to correlate collected network traffic with logs for analysis via a single unified user interface	
126	The solution must be able to capture, extract metadata, fully reassembles and globally normalizes network traffic at layers 2-7 of the OSI model	
127	The solution must ingest network packets with real-time capture and analysis capabilities	
128	The solution must support extraction of Packet Capture (PCAPs) for further investigation. The solution must also support Application Programming Interface/Software Development Kit (API/SDK) commands for interfacing with 3rd party solution	
129	The solution must support event reconstruction in the following representation: . Details . Text . Hex . Packets . Web . Mail . IM	
130	The solution must provide out of the box SSL decryption capabilities for incoming or lateral network traffic	
131	The solution must support the ability to decode base64 encoded network traffic natively on the UI	

132	The solution must provide ability to detect statistical variation in network session by using of Entropy calculation. The Entropy value must be represented as a meta data in the platform	
133	To provide an open database format, the solution must support pcapng-formatted database as an option (apart from vendor's proprietary database) for network traffic collection data	
134	The solution must have a 7 days Online RAW Data Packet Retention and 30 days Offline META DATA Packet Retention.	
Event Stream Analysis		
135	The solution must provide advanced event stream analytics such as correlation and complex event processing at high throughputs and low latency.	
136	The solution must support the use of Event Processing Language (EPL) to express filtering, aggregation, and joins, possibly over sliding windows of multiple event series. It also includes pattern semantics to express complex temporal causality among events (followed-by relationship).	
137	The proposed event stream analysis platform must support a scale-out architecture based on performance demands, with single node processing rate of 100,000 events per second (EPS).	
138	The proposed event stream analysis platform must provide both wizard-based creation of logic expressions, as well as the declarative based programming-like syntax language for greater flexibility and advanced capabilities.	
139	The proposed event stream analysis platform must be able to send out Email, SNMP and Syslog alerts when the streaming of log events matches predefined logic expressions.	
140	The proposed event stream analysis platform must be able to send notifications in the format customized using templates.	
141	The proposed event stream analysis platform must provide data science techniques to identify new and unknown C2 domains by focusing on behavior through packets and logs analysis and providing an aggregated score based on minimally the following behavior: - Beaconing behavior - Rare domains - Rare agent string - Missing referrers - Domain age	
Integration		
142	The solution must allow the automatic transmission of asset information and criticality rating from Governance Risk and Compliance (GRC) solutions into the analytics platform, and to make use of these enriched data to define alerts and build dashboards or reports.	
143	The solution must be able to send data feed from DLP to the analytics platform. Data feed should include Source host name, source IP address, type of data resides on the host, severity of sensitivity of the data and information.	
144	The solution must be able populate/update the Asset Database in the GRC solution with the heat maps of assets with sensitive information discovered by DLP, thus providing and facilitating data sensitivity factor into determining asset prioritization in the GRC solution. The updating/populating should be natively provided and can be automated or scheduled.	
145	Versions of the solution (existing and 1 version before existing) must be performed fully via the GUI and not via command line	
146	The solution must be able to integrate to LandBank's existing Security Orchestration, Automation and Response (SOAR) solution.	
Threat Intelligence		
147	The solution must have a bundled Threat Intelligence Feed of the same brand of the	

	SIEM Software.	
148	The solution must provide advance threat intelligence content from multiple threat sources to enrich both captured network traffic for contextual analysis.	
149	The solution must have dedicated research team to directly input threat intelligence into the analytics platform.	
150	The solution must allow customized feeds to label internal network segments for additional contextual information during pivoting of investigation data.	
151	The solution must allow customized feeds to label the functionality of internal servers for additional contextual information during pivoting of investigation data.	
152	The solution must allow customized feeds to label the criticality of internal servers for additional contextual information during pivoting of investigation data.	
153	The solution shall allow participation of intelligence sharing within a closed community.	
154	The solution must come with live cyber security feed that the following information: · New/Updated Correlation Rules · New/Updated Event Source Parsers · Dynamic DNS Domains · File Upload Sites · High Risk File · Hijacked · IDefense Threat Indicators Domain · Malware Domain List · Malware Domains · Malware IP List · MaxMind ASN · Palevo Tracker Domains · Palevo Tracker IPs · Third Party IOC IPs · Tor Exit Nodes · Tor Nodes · url-shortening-services.zip · WikiLeaks Domains · Zeus Domain Tracker · Zeus Tracker	
155	The solution must allow the ingestion of internal/custom threat intelligence feeds and support Structured Threat Information Expression/Trusted Automated Exchange of Intelligence Information (STIX/TAXII) format.	
156	The solution must be able to automatically map external IP addresses with external threat intel platform and automatically makes risk assessment containing risk indicators information such as if the IP address is blacklisted by third party vendors or by community (other customers)	
Endpoint Detection and Response License and Integration		
157	The solution must have a bundled a COMPLIMENTARY End Point Detection and Response license for 1000 users. The EDR license (1000 users) bundle should be the same brand of the SIEM Software.	
158	The Solution must be able to integrate to LandBank's existing Endpoint Detection and Response solution.	
159	The Solution must be able to provide a complementary end point solution part of the same user interface and platform that perform behavioral based analytics on endpoints that does not solely rely on signatures for threat detection.	
160	The solution must provide an intelligent risk-level scoring system that is determined by behavior/characteristic of the artifact being analyzed and also leverage on machine learning capabilities to establish risk score	

161	The solution must provide endpoint monitoring capabilities that does not only analyses and detect threats when scans are triggered. The solution should provide capabilities that monitors processes as they are loaded into endpoint's memory	
162	The solution endpoint agents will operate on kernel-level of the endpoint and monitor the following to detect threats	
163	The solution must support file/applications whitelisting	
164	Delivery of whitelisted signatures to perform hash comparison (determine malicious modules) must be provided via a live feed provided through a cloud-based threat-intel deployment model	
165	The solution must support the ability to perform full scan. In each scan, it must perform an inventory of all files loaded in memory (executable, DLLs, Drivers etc) as well as all files configured to run automatically (Tasks, services, autoruns).	
166	The solution must support agent deployments on Windows, Linux and Mac Operating System	
Scalability		
167	The solution must be able to scale when the monitored network throughput increases by adding more capturing nodes.	
168	The solution must be able to scale when the captured network or the retention requirement increases by adding capacity to the data store.	
169	The solution must be able to scale when the event sources throughput increases by adding more capturing nodes.	
170	The solution must be able to scale when the log events or the retention requirement increases by adding capacity to the data store.	
171	When scaling the solution when in operation, it must not cause any downtime or periods where the network traffic not being captured or monitored.	
System Health and Maintenance		
172	The data store must use First In First Out (FIFO) method to rotate stale captured traffic out of the system. It should be automatic and self-staining; do not require an operator to routinely manage the data store.	
173	The solution must be able to provide dashboard view on the performance of the systems.	
174	The solution must support centralized remote patching or updating of the components, and across geographically distributed setups.	
Security		
175	The solution must support secure communication between the components.	
176	The solution must be able to ensure the integrity of the captured network traffic and to detect any modification on the stored data.	
177	The solution shall support audit trail logging of users and system activities.	
178	The solution shall be able to retain the audit trails for at least 90 days.	
179	The solution must be able to support role based access control.	
180	The solution must support 2-factor authentication.	
181	The solution must allow the configuration of customized login banner.	
182	The solution must support data obfuscation on the meta data to allow data privacy officer or administrator to identify and restrict access using roles and permissions to personally identified data (Ability to choose meta to designate as sensitive and obfuscate it)	
183	The solution must provide capability to limit exposure of meta data and raw content using a combination of techniques as shown below: . Data obfuscation (obfuscation of meta values for privacy-sensitive meta keys with an optional salt) . Data retention enforcement	

	. Auditing logging	
Maintenance and Ongoing Support		
184	The supplier must provide follow the sun support structure offering 24/7 customer support via email or phone call	
185	All support call must be directly supported by the supplier. There must be a local support (Non-Partner) that can converse using Filipino language.	
186	Provide flexibility for customer to choose between 2 maintenance structure	
187	a. Basic Support – For non-mission-critical environments where business-hours support meets your needs (8am-5pm customer local time, Monday through Friday).	
188	b. Enhance Support – 24x7 around-the-clock remote support and access to product's global network of support centers for troubleshooting	
189	The supplier must have support team physically in-country and local office with in-country representative from product vendor (Excluding partners and distributors)	
Collaboration		
190	The Supplier must provide a physical visit to reference customer's production Security Operations Center using vendor's solution	
191	The Supplier must make available training for customized network parsers training (e.g. If a specific Network Protocol for network packets collection is not available out-of-the-box, vendor should have training on creation of network parsers)	
Supplier's Eligibility Requirements		
192	The supplier must be at least five (5) Years of existence in the IT Industry. Information should be based from SEC (Security and Exchange Commission) incorporation information, that the vendor is at least five (5) years. The bidder must submit a notarize certification from them with reference to SEC documents.	
193	The supplier must be an authorized reseller or distributor of the brand being offered. Must submit certification from distributor or principal.	
194	The principal represented by the supplier must have a local Technical manager or Information Technology (IT) support engineers to support the installations, configurations and 24x7 uptime services within the warranty period. Must submit Certificate of employment and Resume/Curriculum Vitae (that the local IT support engineers has at-least 5 years work experience in handling of the product being offered or other related security devices, include list of trainings and seminars attended)	
195	Three (3) years warranty on hardware and software. Warranty shall also cover any reconfiguration/integration after successful implementation. (The warranty certificate will be submitted by the winning bidder)	
196	The supplier must have a local helpdesk to provide 24x7 technical assistance. Must provide detailed escalation procedure and support including contact numbers and email addresses.	
197	The supplier must have a dedicated Project Manager (PM) to oversee the project. Must submit Certificate of Employment and Resume/Curriculum Vitae (that the PM has at-least 5 years work experience and handled at least One (1) Commercial or Universal bank and one (1) non-bank clients as proof of his/her experience on how to handle projects.)	
198	The supplier must have at-least three (3) installed base of same solution or complex technology like Application Programming Interface (API) Management, Security Information and Event Management (SIEM) wherein one (1) is a Universal or Commercial Philippine Bank. Must submit list of installed base with client name, contact person, address, telephone number and email address.	
Delivery Terms and Condition		
191	Delivery after receipt of NTP: 60 calendar days	
192	Installation will start 7 calendar days after delivery and will end 90 calendar days after.	

LBP SECURE FILE TRANSFER FACILITY
REGISTRATION FORM

Name of Participating Bidder/"Company"	
Complete Address of the Company:	**Contact Number/s:**

AUTHORIZED LBP SECURE FILE TRANSFER USER/S:

Name of Authorized Representative:	**Official Email Address:**	**Contact Number/s:**

TERMS AND CONDITIONS:

The Company, through its Authorized User/s, shall:

1. Use LBP's Secure File Transfer Facility to securely transmit files to LBP Procurement Department only for the purpose of online submission of bidding documents.
2. Be responsible for the confidentiality of its assigned log-in credentials. (i.e. assigned user ID)
3. Only upload agreed upon file formats and shall not upload any file/s containing inappropriate content, material that violates or infringes in any manner on the intellectual or proprietary rights of others, and any malwares, software virus, "Trojan Horse" program, "worm" or other harmful or damaging software or software component.
4. Agree and ensure that the computing devices to be used for LBP's Secure File Transfer Facility have the updated anti-virus software and operating system security patches, as minimum requirements in order to establish connectivity, to maintain and ensure the security, integrity and availability of the LBP Secure File Transfer Facility.
5. Agree not to use a public wi-fi/hotspot such as but not limited to those offered in coffee shops, malls, restaurant or hotels to access into the LBP Secure File Transfer Facility.
6. Agree that LANDBANK may revoke, block, or permanently disallow the use of this facility without prior notice due to reasons that may compromise the Bank's security.

AGREEMENT:

As an Authorized User, I hereby agree:

To the above terms and conditions
Not to disclose any confidential information regarding the LBP Secure File Transfer Facility.
To avoid using unauthorized users/computers to input credentials; and
That unauthorized dissemination of information about the LBP Secure File transfer Facility shall be considered a security breach and is ground for the immediate termination of the account.

____

Authorized User
(Signature over Printed Name)

Please print N/A in blank spaces

Annex E

Questronix Clarification	LBP Response
1. Does the vendor should also provide Top of Rack Switches? a. If yes, what is the connectivity of the existing switch for the downlink connection to ToR? b. Do we have to provide a transceiver for the existing ToR/Core switches? If yes, may we know the exact model of the switch? c. What is the network speed from the ToR to existing ToR/Core Switches? d. What is the port of the existing ToR/Core Switches to connect to the ToR that the vendor will provide? BaseT or SFP+? e. How long is the required cable from the ToR to existing ToR/Core Switches? f. What is the distance between the existing core switch and TOR switch? g. Do we need to provide PDU? if no, what is the existing PDU	1. Yes. vendor to provide Top of Rack switches ● (2) units of Top of Rack switch of at-least 24Fixed Ports 1GbE/10GbE SFP+ Ports and 4 Fixed 40GbE QSFP+ Ports with at-least 2 Expansion Slots. ● The TOR Switch configuration should already include the required Optical/Copper Transceivers to connect the HCI Infra to the Landbank Local Area Network (LAN). ● Each TOR Switch should be configured with Redundant Power Supply, Supports both IPv4 and IPv6 and Virtual Chassis Technology. Other details to be provided once declared as the lowest complying bidders
2.What is the machine type and model of your core switch? Is this 10GB or 1Gb? Do you have spear transceivers on it? If none, can you provide the details of the transceivers?	To be provided once declared as the lowest complying bidders
3.Do we need to provide Rack Cabinet and peripherals?	3. No need to provide
4.Are there are required cabling for data and power?	4. Yes. Atleast for the patch cord and power cords.
5.May we know the location of the 4 HCI Nodes to be delivered? Is this Prod only?	5. LBP Head Office. Production only
6.Is this fresh installed or there are physical data/VMs to be migrated? If there are migration can you provide the list of it? will this be VM-to-VM or physical to Virtual Migration? How many VMs do we need to migrate?	6. Fresh installation.
7.Do you have requirement on the raid level for the SSD's and HDD's?	Replication Factor 2 (RF2) or equivalent to RAID 10
8.In item no. 14, what this means provide support usage of 3rd party storage? Do you need to connect on a external storage? Or internal HDC ’	8. Yes. We have an existing NAS storage to be use for archiving.
9.For Training, is this knowledge transfer or do we need to provide formal training? If formal training, do you need to be certified and how many attendees from LBP? Can we do the training remotely if formal training due to pandemic?	9. Formal Training. We can do online training if still in the Pandemic.

MDI Inc. Clarification	LBP Response
1. **Raised during last Friday pre-bid:** In the HCI TOR document, kindly confirm again if the four (4) HCI nodes need to be configured with the required Hypervisor Licenses? And is the preferred Hypervisor is vMware?	1. The HCI Infra to support the SIEM Software Solution should already include the VMware Hypervisor licenses for all 4 HCI Nodes as the recommended Hypervisor platform for the SIEM Software.
2. **Raised during last Friday pre-bid:** In the HCI TOR document, kindly confirm if the Top of Rack (TOR) switches should also be included in the HCI Infra, where in all required Optical Transceivers and Cables are included? Are the two (2) units TOR Switch is configured with redundant power supply	2. The HCI Infra should also include two (2) units of Top of Rack switch of at-least 24Fixed Ports 1GbE/10GbE SFP+ Ports and 4 Fixed 40GbE QSFP+ Ports with at-least 2 Expansion Slots. The TOR Switch configuration should already include the required Optical/Copper Transceivers to connect the HCI Infra to the Landbank Local Area Network (LAN). Each TOR Switch should be configured with Redundant Power Supply, Supports both IPv4 and IPv6 and Virtual Chassis Technology.
3. **Raised during last Friday pre-bid**: In reference to the Section VI: Schedule of Requirements, what is the equivalent Events Per Seconds (EPS) capacity of the given 350Gb Log capacity per day? Kindly confirm the 7.5k eps response of Sir Archie.	3. For Log or EPS Capacity, The 350G per day log capacity is equivalent to 7,500 eps
4. **Additional Inquiry:** In the TOR, specifically for Analytics Platform (item 59-80) may we know the required number of UEBA licenses/agents needed to be bundled in the SIEM software?	4. For UEBA, minimum 1000 user licenses is required for pilot project (Item No. 59-80 of the TOR)
5. **Additional Inquiry:** In the TOR, specifically for the SIEM Log Retention (item 103-105), aside from the three (3) months On-line retention period requirements, may we know the number of retention period (months) for the Off-line data?	5. On Log Retention, the complete requirement should be 3 Months On-line and 1 Year Off-Line Retention (item No. 103 of the TOR)
6. **Additional Inquiry:** In the TOR, specifically for Network Traffic Capture and Analysis (item 119 - 128), what is your required retention period same as my item#5 question for On-line raw packet retention and Offline meta-data retention for Packet Capture?	6. On Packet Retention, the complete requirement should be 7 days Online RAW Data Packet Retention and 30 days Offline META DATA Packet Retention. (Item No. 119-128 of the TOR)
7. **Additional Inquiry:** In the TOR, specifically for Threat Intelligence (item 141 - 149), may we confirm if the SIEM requirement needs to include a Threat Intelligence Feed license/subscription for the same SIEM brand being offered, aside from Landbank's current Threat Intel platform that will be integrated to the SIEM?	7. In reference to the Threat Intel Section of the TOR, must bundled Threat Intelligence Feed of the same brand of the SIEM Software, (Item No. 141 - 249 of the TOR)
8 **Additional Inquiry:** In the TOR, specifically for Endpoint Detection and Response License and Integration (item 150-158), may we know the exact number of EDR agents to be included with the SIEM Software as complimentary EDR license.	8.In reference to the EDR License and Integration Section of the TOR, must bundled a COMPLIMENTARY End Point Detection and Response license for 1000 users. The EDR license (1000 users) bundle should be the same brand of the SIEM Software. (Item #150-158 of the TOR,)