LANDBANK
WE HELP YOU GROW.

SUPPLEMENTAL BID BULLETIN NO. 6
For LBP-HOBAC-ITB-GS-20200407-01

PROJECT	:	**Supply, Delivery, Installation & Configuration of Privileged Access Management (PAM) Solution with Hardware Appliance with Three (3) Years Warranty**
IMPLEMENTOR	:	**Procurement Department**
DATE	:	**September 18, 2020**

This Supplemental Bid Bulletin is issued to modify, amend and/or clarify certain items in the Bid Documents. This shall form an integral part of the Bid Documents.

Modifications, amendments and/or clarifications:

1)

Bidder's Queries/Clarifications	**LANDBANK Responses**
1) The bidder clarified on the following:	
➢ Total number of physical administrators for the PAM solution?	➢ There are fifty (50) users for the PAM solution.
➢ Total number of system/ device/appliances to be enrolled in PAM solution?	➢ There are 2,000 target assets to be enrolled for the PAM solution.
➢ List of systems/devices/ appliances which will be supported by the PAM solution?	➢ The PAM solution must support various assets, as follows: • Microsoft Windows • AIX • Redhat Linux • Unix Systems • Solaris • Oracle • MS SQL/DB2/MYSQL • Network Devices (e.g. Router, Switches, etc.) • Security Devices (e.g. Firewall, IPS, etc.) • Generic Target Systems Connectors
➢ Site location for the deployment of PAM solution?	➢ The PAM solution will be deployed at LANDBANK Head Office and Disaster Recovery site.

2) The prospective bidder/s who would like to participate in the bidding for the above project must send a duly filled-up LBP Secure File Transfer Facility (SFTF) User Registration Form to **lbphobac@mail.landbank.com** on or before **2:00 PM** of **September 23, 2020**. The LBP SFTF User Registration Form can be obtained from Procurement Department by sending a request to the aforementioned e-mail address quoting "SFTF – ITB-GS-20200407-01" as subject.

3) The prospective bidder/s who have submitted 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 to the HOBAC Secretariat shall receive an e-mail with log-in credentials to access the LBP SFTF.

4) The prospective bidder/s who will participate in the bidding for the above project are encouraged to use the Bid Securing Declaration as Bid Security.

5) The Terms of Reference (Annex A), Item Nos. 5 & 7 of the Invitation to Bid, ITB Clauses 9.1, 21 & 24 of the Bid Data Sheet (Section III), Schedule of Requirements (Section VI), Specifications (Section VII), and Checklist of the Bidding Documents (Item Nos. 7, 8, 12, 18, 19 & 21 of the Eligibility and Technical Components) have been revised. Please see attached revised Annexes A-1 to A-9 and specific sections of the Bidding Documents.

6) The deadline for the submission of electronic bids for the above project is re-scheduled on **September 25, 2020** at **10:00 A.M.** Submission of physical bids (hard copy) shall **not** be accepted.

Original Signed
ALWIN I. REYES
Assistant Vice President
Head, Procurement Department and
HOBAC Secretariat

LBP-HOBAC-ITB-GS-20200407-01
Revised 09.18.20

Land Bank of the Philippines

Invitation to Bid For

Supply, Delivery, Installation and Configuration of Privileged Access Management (PAM) Solution with Hardware Appliance with Three (3) Years Warranty

1. The LAND BANK OF THE PHILIPPINES (LANDBANK), through its Corporate Budget for the contract approved by the Board of Directors for 2020 intends to apply the total sum of Twenty Seven Million Three Hundred Fifty Five Thousand Pesos Only (PhP 27,355,000.00) being the Approved Budget for the Contract to payments under the contract for Supply, Delivery, Installation and Configuration of Privileged Access Management (PAM) Solution with Hardware Appliance with Three (3) Years Warranty / ITB No. LBP-HOBAC-ITB-GS-20200407-01. Bids received in excess of the above ABC shall be automatically rejected at bid opening.

2. The LANDBANK now invites bids for the Supply, Delivery, Installation and Configuration of Privileged Access Management (PAM) Solution with Hardware Appliance with Three (3) Years Warranty. Delivery period is indicated in Section VI, Schedule of Requirements. Bidders should have completed, within the last five (5) years from the date of submission and receipt of bids, a contract similar to the Project. The description of an eligible bidder is contained in the Bidding Documents, particularly, in Section II. Instructions to Bidders.

3. Bidding will be conducted through open competitive bidding procedures using a non-discretionary "pass/fail" criterion as specified in the Implementing Rules and Regulations (IRR) of Republic Act (RA) 9184, otherwise known as the "Government Procurement Reform Act".

   Bidding is restricted to Filipino citizens/sole proprietorships, partnerships, or organizations with at least sixty percent (60%) interest or outstanding capital stock belonging to citizens of the Philippines, and to citizens or organizations of a country the laws or regulations of which grant similar rights or privileges to Filipino citizens, pursuant to R.A. 5183.

4. Interested bidders may obtain further information from LANDBANK and inspect the Bidding Documents at the address given below during banking days, from 8:00 A.M. to 5:00 P.M.:

   Procurement Department
   Land Bank of the Philippines
   25th Floor LANDBANK Plaza Building
   1598 M.H. Del Pilar cor. Dr. J. Quintos Sts.
   1004 Malate, Manila
   lbphobac@mail.landbank.com

5. A complete set of Bidding Documents may be acquired by interested Bidders on **June 2, 2020 to September 25, 2020** from the address indicated above and upon payment of the cost of Bidding Documents, pursuant to the latest Guidelines issued by the GPPB, in the amount of Thirteen Thousand Seven Hundred Pesos Only (P 13,700.00).

   It may also be downloaded free of charge from the website of the Philippine Government Electronic Procurement System (PhilGEPS) and the LANDBANK website, provided that Bidders shall pay the corresponding Bidding Documents Fee not later than the submission of their bids.

6. The LANDBANK will hold a Pre-Bid Conference on August 28, 2020 – 1:50 PM through videoconferencing using Microsoft (MS) Teams Application.

   Bidders who would like to participate in the said conference must send a duly filled-up Pre-Bid Conference Registration (PBCR) Form to lbphobac@mail.landbank.com on or before 12:00 PM of August 27, 2020. The PBCR Form can also be downloaded at the PhilGEPS website or requested from MS. MA. ANGELA Q. EMETERIO at MEMETERIO@mail.landbank.com **and** MQEMETERIO@gmail.com. Bidders shall quote "PBCR-ITB-GS-20200407-01" as the email's subject.

   Bidders who have registered for the videoconferencing shall be provided with an e-mail invitation containing a link that would enable them to access the designated Microsoft Teams channel for the detailed procedures in the conduct of Pre-Bid Conference through videoconferencing, post messages therein and join the online meeting.

   For new bidders, a briefing through video conferencing on salient provisions of the 2016 Revised Implementing Rules and Regulations of R.A. 9184 and pointers in the preparation of bid proposals will be conducted on August 27, 2020 – 2:00 P.M. through video conferencing using MS Teams application.

7. **All bids shall be submitted electronically on or before the 10:00 A.M. deadline on September 25, 2020.** All Bids must be accompanied by a bid security in any of the acceptable forms and in the amount stated in ITB Clause 18. Only electronic bids that are successfully uploaded to the Secure File Transfer Facility of LANDBANK on or before the deadline shall be accepted. Submission of physical bid (hard copy) shall not

be accepted. The procedures that will be followed in the submission and opening of electronic bids are described in the Detailed Procedures in Submission and Opening of Electronic Bids per attached Annexes D-1 to D-8.

8. The LANDBANK reserves the right to (a) reject any and all bids at any time prior to the award of the contract; (b) waive any minor formal requirements in the bid documents; (c) accept such bids it may consider to be advantageous and beneficial to the Bank, without thereby incurring any liability to the affected bidder or bidders.

9. For further information, please refer to:

   Mr. Alwin I. Reyes, CSSP
   Assistant Vice President
   Head, Procurement Department
   1598 M.H. Del Pilar cor. Dr. J. Quintos Sts.
   1004 Malate, Manila
   Tel. (+632) 8-522-0000 or 8-551-2200 local 7370
   Fax (+632) 8-528-8587
   Email lbphobac@mail.landbank.com

Original Signed
ALEX A. LORAYES
Senior Vice President
Chairman, Bids and Awards Committee

Bid Data Sheet

ITB Clause	
1.1	The Procuring Entity is LAND BANK OF THE PHILIPPINES (LANDBANK). The name of the Contract is Supply, Delivery, Installation and Configuration of Privileged Access Management (PAM) Solution with Hardware Appliance with Three (3) Years Warranty The identification number of the Contract is LBP-HOBAC-ITB-GS-20200407-01
1.2	The lots and references are: Supply, Delivery, Installation and Configuration of Privileged Access Management (PAM) Solution with Hardware Appliance with Three (3) Years Warranty
2	The Funding Source is: The Government of the Philippines (GOP) through the Corporate Budget for the contract approved by the LANDBANK Board of Directors for 2020 in the total amount of Twenty Seven Million Three Hundred Fifty Five Thousand Pesos Only (PhP 27,355,000.00). Project: Supply, Delivery, Installation and Configuration of Privileged Access Management (PAM) Solution with Hardware Appliance with Three (3) Years Warranty
3.1	No further instructions.
5.1	Bidders should have no negative dealings with LANDBANK or its subsidiaries.
5.2	Foreign bidders, falling under **ITB** Clause 5.2 (b) and/or doing business in the Philippines may participate in this Project provided they meet the requirements under Section 23.4.1.2 of the Revised IRR of RA 9184.
5.4	The Bidder must have completed, within the last five (5) years from the date of submission and receipt of bids, a single contract that is similar to this Project, equivalent to at least fifty percent (50%) of the ABC. For this purpose, similar contracts shall refer to contracts involving

	Information Technology hardware and/or software. Bidders must submit proof of their respective Single Largest Completed Contract. Proofs shall be: • Copy of the contract or purchase order; or • Copy of official receipt/collection receipt or Certificate of Satisfactory Performance from bidder's client.
7	No further instructions.
8.1	Subcontracting is not allowed.
8.2	Not applicable.
9.1	**The LANDBANK will hold a Pre-Bid Conference on August 28, 2020 – 1:50 PM through videoconferencing using Microsoft (MS) Teams Application.** **Bidders who would like to participate in the said conference must send a duly filled-up Pre-Bid Conference Registration (PBCR) Form to** lbphobac@mail.landbank.com **on or before 12:00 PM of August 27, 2020. The PBCR Form can also be downloaded at the PhilGEPS website or requested from MS. MA. ANGELA Q. EMETERIO at** MEMETERIO@mail.landbank.com **and** MQEMETERIO@gmail.com. **Bidders shall quote "PBCR-ITB-GS-20200407-01" as the email's subject.** **Bidders who have registered for the videoconferencing shall be provided with an e-mail invitation containing a link that would enable them to access the designated Microsoft Teams channel for the detailed procedures in the conduct of Pre-Bid Conference through videoconferencing, post messages therein and join the online meeting.** **For new bidders, a briefing through video conferencing on salient provisions of the 2016 Revised Implementing Rules and Regulations of R.A. 9184 and pointers in the preparation of bid proposals will be conducted on August 27, 2020 – 2:00 P.M. through video conferencing using MS Teams application.**
10.1	The Procuring Entity's address is: Land Bank of the Philippines 25th Floor, LANDBANK Plaza Building 1598 M.H. Del Pilar corner Dr. J. Quintos Streets 1004 Malate, Manila www.landbank.com Contact person :

	Mr. Alwin I. Reyes, CSSP Assistant Vice President Head, Procurement Department 1598 M.H. Del Pilar cor. Dr. J. Quintos Sts. 1004 Malate, Manila Tel. (+632) 8-522-0000 or 8-551-2200 local 7370 Fax (+632) 8-528-8587 lbphobac@mail.landbank.com
1.21 (a)	Bidders may still submit their Class "A" Eligibility Documents required to be uploaded and maintained current and updated in the PhilGEPS pursuant to Section 8.5.2 of the same IRR, or if already registered in the PhilGEPS under Platinum category, their Certificate of Registration and Membership in lieu of their uploaded file of Class "A" Documents, or a combination thereof. In case the bidder opted to submit their Class "A" Documents, the Certificate of PhilGEPS Registration (Platinum Membership) shall remain as a post-qualification requirement to be submitted in accordance with Section 34.2 of the 2016 Revised IRR of RA 9184.
12.1(a)(ii)	The statement of all ongoing government and private contracts (use Form No. 3) and Single Largest Completed Contract (use Form No. 4) similar to the contract to be bid shall include all such contracts within five (5) years prior to the deadline for the submission and receipt of bids.
13.1	Bidders are required to use the Bid Form provided in Section VIII. Bid Form (use Form Nos.1 and 2).
13.1(b)	No further instructions.
13.1(c)	No further instructions.
13.2	The Approved Budget for the Contract (ABC) Twenty Seven Million Three Hundred Fifty Five Thousand Pesos Only (PhP 27,355,000.00). Any bid with a financial component exceeding this amount shall not be accepted.
15.4(a)(iv)	Please refer to Clause 6.2 of the Special Conditions of the Contract for the incidental services required.
15.4(b)	Please refer to Clause 6.2 of the Special Conditions of the Contract for the incidental services required. The price of the Goods shall be quoted DDP specified delivery site/s.
16.1(b)	The Bid Prices for the Goods supplied from outside of the Philippines shall be quoted in Philippine Pesos.
16.3	Not applicable.

17.1 Bids will be valid until 120 calendar days from date of opening of bids.

18.1 The bid security shall be limited to Bid Securing Declaration or any other form in accordance with the following minimum amount:

Form of Bid Security	Minimum Amount of Bid Security
(a) Cash or cashier's/ manager's check issued by a Universal or Commercial Bank;	P 547,100.00
(b) Bank draft/guarantee or irrevocable letter of credit issued by a Universal or Commercial Bank; Provided, however, that it shall be confirmed or authenticated by a Universal or Commercial Bank, if issued by a foreign bank; and	
(c) Surety bond callable upon demand issued by a surety or insurance company duly certified by the Insurance Commission as authorized to issue such security.	P 1,367,750.00

1. If bid security is in the form of cash, a bidder is required to secure an electronic Payment Acceptance Order (PAO) from LANDBANK Procurement Department. The electronic PAO shall then be printed and presented to the Teller at any of the LANDBANK Branches together with the corresponding cash. The LANDBANK Teller shall issue a machine validated Official Receipt (OR) evidencing payment of the bid security. A scanned copy of the Official Receipt shall be included in the Eligibility and Technical Proposal/Documents.
2. If bid security is in the form of cashier's/manager's check, the check should be payable to LAND BANK OF THE PHILIPPINES. The physical check must be delivered to and received by LANDBANK-Procurement Department not later than the following banking day after the opening of bids.
3. If in the form of bank draft/guarantee, the bidder may use the standard format of the issuing Bank, provided the ITB No. and Name of the Project are indicated.

	4. If in the form of Standby Letter of Credit, it may be secured through LANDBANK Corporate Banking Department 2 (CBD 2) and Small and Medium Enterprises – Market Lending Department 2 (SME-MLD 2) with the following contact details: a) CBD 2 – 18th Floor, LANDBANK Plaza Building Telephone No. 8-405-7345 local 2117 (For Assets 1 Billion and up) b) SME-MLD 2 - 18th Floor, LANDBANK Plaza Building Telephone No. 8-405-7431 local 7431 (For Assets below 1 Billion) 5. If in the form of surety bond, it should be issued by a surety or insurance company duly accredited by the Insurance Commission (IC) and has not been issued a cease and desist order by the IC or is currently not included in the list of blacklisted firms. The surety bond may be secured through LANDBANK Insurance Brokerage, Inc. (LIBI) with the following contact details: (a) LIBI-Forex 14th Floor, LANDBANK Plaza Building Telephone 8-710-7114 (Every Tuesday and Thursday) (b) 12th Floor, SSHG Law Center Bldg. 105 Paseo de Roxas, Legaspi Village Makati City Telephones 8-812-4911 and 867-1064 Surety bonds with the following or similar conditions/phrases shall not be accepted: (a) "In case of default by the Principal, this bond shall only answer for the difference in the bid price of the winning bidder and that of the next lowest complying bidder or that of the new winning bidder in case of re-bidding plus necessary expenses incurred by the Obligee in the re-bidding which liability shall in no case exceed the amount of the bond"; or (b) "That the amount of liability of the Surety under this bond is limited to the actual loss or damage sustained and duly proven by the Obligee." 6. If in the form of Bid Securing Declaration, the attached form (Form No. 8) must be used.
18.2	The bid security shall be valid until 120 calendar days from date of opening bids.

20	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 per attached Annexes D-4 to D-6. *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. 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. *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. 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.
20.3	Each Bidder shall submit two (2) sets of electronic bids (archived files) labeled in accordance with the instructions described in ITB Clause 20 above.
21	**All bids shall be submitted electronically on or before the 10:00 A.M. deadline on September 25, 2020.** All Bids must be accompanied by a bid security in any of the acceptable forms and in the amount stated in ITB Clause 18. Only electronic bids that are successfully uploaded to the Secure File Transfer Facility of LANDBANK on or before the deadline shall be accepted. Submission of physical bid (hard copy) shall not be accepted. The procedures that will be followed in the submission and opening of electronic bids are described in the Detailed Procedures in Submission and Opening of Electronic Bids per attached Annexes D-1 to D-8.
23	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]
24	**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) representative, the said representative may take turns in using the allowed account/connection.** **Projects with participating bidders in attendance shall be given priority in the queuing.** **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.** **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.** **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.** **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.** **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.** **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.** **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.**
24.2	No further instructions.
24.3	No further instructions.

27.1	No further instructions.
28.3	The goods are grouped in a single lot and the lot shall not be divided further into sub-lots for the purpose of bidding, evaluation and contract award.
28.4	No further instructions.
29.2	Certified true copy of Value Added Tax (VAT) or Percentage Tax (PT) Returns for the last two (2) quarters filed manually or through the BIR Electronic Filing and Payment System (EFPS). Only tax returns filed manually or through EFPS and taxes paid shall be accepted.
32.4(f)	No additional requirement.
33.2	If in the form of Standby Letter of Credit, it may be secured through LANDBANK Corporate Banking Department 2 (CBD 2) and Small and Medium Enterprises – Market Lending Department 2 (SME-MLD 2) with the following contact details: 1. CBD 2 – 18th Floor, LANDBANK Plaza Building Telephone No. 8-405-7345 local 2117 (For Assets 1 Billion and up) (b) SME-MLD 2 - 18th Floor, LANDBANK Plaza Building Telephone No. 8-405-7431 local 7431 (For Assets below 1 Billion)

Section VI. Schedule of Requirements

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

Item Description	Quantity	Delivery Period and Site
Supply, Delivery, Installation and Configuration of Privileged Access Management (PAM) Solution with Hardware Appliance with Three (3) Years Warranty		**Delivery Period:** **Within sixty (60) calendar days after receipt by the supplier of the Notice to Proceed** **Installation Period:** Ninety (90) calendar days to start seven (7) calendar days after delivery **Delivery Site:** Network Operations Department LANDBANK Plaza Building 1598 M.H. del Pilar corner Dr. J. Quintos Streets, Malate, Manila **Contact Person:** VP Enrique L. Sazon, Jr. Head, Network Operations Department **Contact Number:** 8405-7168
1. Hardware Server Appliance for both Production and Disaster Recovery Site, 3 Years Warranty	7 units	
1.1 Gateway Server	3 units	
1.2 Application Server	2 units	
1.3 Database Server	2 units	
2. Client Manager Licenses for Target Devices (Windows, AIX, Linux, Security and Network Devices), 3 Years License Key	2,000 licenses	
3. Client Manager Licenses for Privileged Users, 3 Years License Key	50 licenses	

Conforme:

____
Name of Bidder

____
Signature Over Printed Name of
Authorized Representative

____
Position

Section VII. Specifications

Specifications	Statement of Compliance
	Bidders must state here either "Comply" or "Not Comply" against each of the individual parameters of each Specification stating the corresponding performance parameter of the equipment offered. Statements of "Comply" or "Not Comply" must be supported by evidence in a Bidders Bid and cross-referenced to that evidence. Evidence shall be in the form of manufacturer's un-amended sales literature, unconditional statements of specification and compliance issued by the manufacturer, samples, independent test data etc., as appropriate. A statement that is not supported by evidence or is subsequently found to be contradicted by the evidence presented will render the Bid under evaluation liable for rejection. A statement either in the Bidders statement of compliance or the supporting evidence that is found to be false either during Bid evaluation, post-qualification or the execution of the Contract may be regarded as fraudulent and render the Bidder or supplier liable for prosecution subject to the provisions of **ITB** Clause 3.1(a)(ii) and/or **GCC** Clause 2.1(a)(ii).
Supply, Delivery, Installation and Configuration of Privileged Access Management (PAM) Solution with Hardware Appliance with Three (3) Years Warranty **For current and past suppliers of Supply, Delivery, Installation and Configuration of Privileged Access Management (PAM) Solution with Hardware Appliance for LANDBANK, they must have satisfactory performance in their dealings with LANDBANK for the past twelve (12) months (reckoned from the date of issuance of the Certificate of Satisfactory Performance).** **Terms of Reference (TOR) and other requirements per attached revised Annexes A-1 to A-9.**	**Please state here either "Comply" or "Not Comply"**

The following documents/requirements shall be included in the Eligibility and Technical Component PDF File:

1. **Duly accomplished revised Terms of Reference signed in all pages by the authorized representative/s of the bidder.**

2. Notarized self-certification based on Security and Exchange Commission (SEC) document that the bidder has been existing in the IT industry for at least five (5) years.

3. Certification from the distributor or principal that the bidder is an authorized reseller or distributor of the brand being offered.

4. Certificate of Employment, resume/curriculum vitae and list of trainings and seminars attended of the assigned local Technical Manager or IT support engineers as proof that they have at least five (5) years work experience in handling of the IT product being offered or other related security devices.

5. Detailed escalation procedure and support including contact numbers and email addresses.

6. Certificate of Employment and resume/curriculum vitae of the Project Manager with at least five (5) years work experience and handled at least one (1) Commercial or Universal Bank in the Philippines and one (1) non-bank client.

7. **List of at least three (3) installed bases with client's name, contact person, address, telephone number and email address of same or complex technology like Application Programming Interface (API) Management, Security Information and Event Management (SIEM) wherein one (1) is a Commercial or Universal Philippine Bank.**

8. **Certificate of Satisfactory Performance issued by the Head, Network Operations Department (NOD) not earlier than thirty (30) calendar days prior to the deadline of submission of bid (applicable only for current and past suppliers of Supply, Delivery, Installation and Configuration of Privileged Access Management (PAM) Solution with Hardware Appliance). The Certificate shall still be subject to verification during post-qualification of bid.**

   NOTE: Certificate of Satisfactory Performance shall be requested in writing from the Head of NOD at 16h floor, LANDBANK Plaza Building (Tel. No.: 8405-7168), at least five (5) working days prior to the submission of bid.

Non-submission of the above-mentioned documents may result in bidder's disqualification.

Conforme:

____

Name of Bidder

____

Signature Over Printed Name of
Authorized Representative

____

Position

LBP-HOBAC-ITB-GS-20200407-01
Revised 09.18.20

Checklist of Bidding Documents for Procurement of Goods and Services

Documents should be arranged as per this Checklist. Kindly provide guides or dividers with appropriate labels.

Eligibility and Technical Component (PDF File)

- **The Eligibility and Technical Component shall contain documents sequentially arranged as follows:**

  - **Eligibility Documents – Class "A"**

    Legal Eligibility Documents

    1. PhilGEPS Certificate of Registration under Platinum Membership (all documents enumerated in its Annex A must be updated); or all of the following:

       - Registration Certificate from SEC, Department of Trade and Industry (DTI) for sole proprietorship, or CDA for cooperatives, or any proof of such registration as stated in the Bidding Documents;

       - Valid and current mayor's/business permit issued by the city or municipality where the principal place of business of the prospective bidder is located, or equivalent document for Exclusive Economic Zones or Areas; and

       - Tax Clearance per Executive Order 398, Series of 2005, as finally reviewed and approved by the BIR.

    Technical Eligibility Documents

    2. Duly notarized Secretary's Certificate attesting that the signatory is the duly authorized representative of the prospective bidder, and granted full power and authority to do, execute and perform any and all acts necessary and/or to represent the prospective bidder in the bidding, if the prospective bidder is a corporation, partnership, cooperative, or joint venture (sample form - Form No. 7).

    3. Duly notarized Omnibus Sworn Statement (sample form - Form No.6)

    4. Statement of the prospective bidder of all its ongoing government and private contracts, including contracts awarded but not yet started, if any, whether similar or not similar in nature and complexity to the contract to be bid, within the last five (5) years from the date of submission and receipt of bids. The statement shall include all information required in the sample form (Form No. 3).

    5. Statement of the prospective bidder identifying its single largest completed contract similar to the contract to be bid, equivalent to at least fifty percent (50%) of the ABC supported with contract/purchase order, end-user's acceptance or official receipt(s)

issued for the contract, within the relevant period as provided in the Bidding Documents. The statement shall include all information required in the sample form (Form No. 4).

6. Bid security in the prescribed form, amount and validity period (ITB Clause 18.1 of the Bid Data Sheet).

7. **Revised Section VI - Schedule of Requirements with signature of bidder's authorized representative.**

8. **Revised Section VII - Specifications with response on compliance and signature of bidder's authorized representative.**

Financial Eligibility Documents

9. The prospective bidder's audited financial statements, showing, among others, the prospective bidder's total and current assets and liabilities, stamped "received" by the BIR or its duly accredited and authorized institutions, for the preceding calendar year which should not be earlier than two (2) years from the date of bid submission.

10. The prospective bidder's computation for its Net Financial Contracting Capacity (NFCC) following the sample form (Form No. 5), or in the case of Procurement of Goods, a committed Line of Credit from a Universal or Commercial Bank.

- **Eligibility Documents – Class "B"**

11. Valid joint venture agreement (JVA), in case the joint venture is already in existence. In the absence of a JVA, duly notarized statements from all the potential joint venture partners stating that they will enter into and abide by the provisions of the JVA in the instance that the bid is successful shall be included in the bid. Failure to enter into a joint venture in the event of a contract award shall be ground for the forfeiture of the bid security. Each partner of the joint venture shall submit its legal eligibility documents. The submission of technical and financial eligibility documents by any of the joint venture partners constitutes compliance, provided, that the partner responsible to submit the NFCC shall likewise submit the statement of all its ongoing contracts and Audited Financial Statements.

- **Technical Documents**

12. **Duly accomplished revised Terms of Reference signed in all pages by the authorized representative/s of the bidder.**

13. Notarized self-certification based on Security and Exchange Commission (SEC) document that the bidder has been existing in the IT industry for at least five (5) years.

14. Certification from the distributor or principal that the bidder is an authorized reseller or distributor of the brand being offered.

15. Certificate of Employment, resume/curriculum vitae and list of trainings and seminars attended of the assigned local Technical Manager or IT support engineers as proof that they have at least five (5) years work experience in handling of the IT product being offered or other related security devices.

16. Detailed escalation procedure and support including contact numbers and email addresses.

17. Certificate of Employment and resume/curriculum vitae of the Project Manager with at least five (5) years work experience and handled at least one (1) Commercial or Universal Bank in the Philippines and one (1) non-bank client.

18. **List of at least three (3) installed bases with client's name, contact person, address, telephone number and email address of same or complex technology like Application Programming Interface (API) Management, Security Information and Event Management (SIEM) wherein one (1) is a Commercial or Universal Philippine Bank.**

19. **Certificate of Satisfactory Performance issued by the Head, Network Operations Department (NOD) not earlier than thirty (30) calendar days prior to the deadline of submission of bid (applicable only for current and past suppliers of Supply, Delivery, Installation and Configuration of Privileged Access Management (PAM) Solution with Hardware Appliance). The Certificate shall still be subject to verification during post-qualification of bid.**

- **Post-Qualification Documents – [The bidder may submit the following documents within five (5) calendar days after receipt of Notice of Post-Qualification]:**

20. Business Tax Returns per Revenue Regulations 3-2005 (BIR No.2550 Q) VAT or Percentage Tax Returns for the last two (2) quarters filed manually or through EFPS.

21. **Latest Income Tax Return filed manually or through EFPS.**

Financial Component (PDF File)

- **The Financial Component shall contain the documents sequentially arranged as follows:**

1. Duly filled out Bid Form signed by the bidder's authorized representative (sample form - Form No.1)
2. Duly filled out Schedule of Prices signed by the bidder's authorized representative (sample form - Form No.2)
3. Annex B – Breakdown of Cost

Supply, Delivery, Installation and Configuration of Privileged Access Management (PAM) Solution with Hardware Appliance *Term of Reference*

Item	Description	Comply (Yes/No)
	Hardware Infrastructure Requirements	
1	**3 units (2 in HO and 1 in DR) Gateway Servers with minimum specs of the following:** - Single CPU with atleast 8Core, 3Ghz/11M Cache -16Gb Memory -5 x 600Gb SAS Hard Drives, RAID 1 + RAID 5 -Management Controller -Dual 1GbE Network Interface Card -Red Hat Operating System, 3Yrs Premium Subscription -Dual Power Supply -Rack Railing Kit -3Yrs Hardware and Software Warranty	
2	**2 units (1 in HO and 1 in DR) Application Servers with minimum specs of the following:** -Single CPU with atleast 12Core, 2.7Ghz/19.25M Cache -32Gb Memory -5 x 600Gb SAS Hard Drives, RAID 1 + RAID 5 -Management Controller -Dual 1GbE Network Interface Card -Windows Server Operating System -Management Controller -Dual 1GbE Network Interface Card -Windows Server Operating System -Dual Power Supply -Rack Railing Kit -3Yrs Hardware and Software Warranty	
3	**2 units (1 in HO and 1 in DR) Database Servers with minimum specs of the following:** -Single CPU with atleast 8Core, 3Ghz/11M Cache -32Gb Memory -2x 600Gb SAS Hard Drives, RAID 1 for OS -8 x 1.8Tb SAS Hard Drives, RAID 5 fot Data -Management Controller -Dual 1GbE Network Interface Card -Windows Server Operating System -Windows SQL Server Database License -Dual Power Supply -Rack Railing Kit -3Yrs Hardware and Software Warranty	
	Single - Sign On and Authentication Models	
4	**The solution should be able to create seamless single sign-on for** a. Microsoft Windows 2003/2008/2013/2012/2016 b. AIX c. Redhat Linux d. Unix Systems e. Solaris Systems f. Oracle g. MS SQL Server / DB2 / MYSQL	

REVISED

	h. Network Devices (e.g. Router, Switches, etc)) i. Security Devices (e.g. Firewalls, IPS, etc) i. Generic Target System Connectors	
5	The solution should be agentless in nature	
6	The solution should support transparent connection to the target device, without seeing the password or typing it in as part of the connection	
7	The solution should support direct connections to windows, ssh, databases and other managed devices without having to use a jump server	
8	The solution shall also include an option of biometric based authentication and/or hardware-less strong authentication (eg Mobile OTP). Further the solution should be able to integrate out of the box with leading dual factor authentication products.	
9	The solution should have an inbuilt dual factor authentication for soft token, mobile OTP etc. Also it should have an inbuilt authentication for Bio-Metrics without having to acquire another biometric authentication server.	
10	The solution shall also include an option of hardware-based tokens. Further the solution should be able to integrate out of the box with leading dual factor authentication products.	
11	The solution should be able to integrate with enterprise authentication methods e.g. multiple 3rd party authentication methods including LDAP, RADIUS and a built-in authentication mechanism	
12	The solution should also provide local authentication and all the security features as per best standards	
13	The solution should provide flexibility user/device wise for local authentication or enterprise authentication	
14	The solution should support an application integration framework for web based as well as .exe based applications. There should be strong out of the box support including ease of integration with any third party connectors.	
15	The solution should provide multi-tenancy feature whereby the entire operations can be carried out within a tenant or line of business.	
16	The solution should provide multi-domain feature whereby the entire operations can operate in an distributed environment	
17	The solution can restrict end-user entitlements to target accounts by location; that is, allow access only from a specified PC or range or class of PCs.	
18	The solution should provide an inbuilt PCI-DSS compliant MFA tool/solution	
19	Ability to allow self-registration of MFA solution for authenticating user	
20	The solution should be able to handle multi-location architecture or distributed architecture with seamless integration at the User Level. For example: Multiple datacenter can be handled with just one installation.	
Shared Account Password Management		
21	The solution shall perform password change options which is parameter driven	
22	The solution should set password options every x days, months, years and compliance options via the use of a policy	
23	Ability to create exception policies for selected systems, applications and devices	
24	The solution should enable an administrator to define different password formation rules for target accounts on different target systems and supports the full character set that can be used for passwords on each target system.	
25	The solution enables an administrator to change a target-account password to a random value based on a manual trigger or automatic schedule.	
26	Allow single baseline policy across all systems, applications and devices (eg one single update to enforce baseline policy	
27	The solution should support changing a password or group of passwords according to a	

REVISED

	policy (time based or 'on-demand')	
28	Ability to generate 'One-time' passwords as an optional workflow	
29	Ability to send notifications via email or other delivery methods triggered by any type of activity	
30	Ability to send notification via email to the user requesting the password that checkout is complete	
31	Flexibility that allows exclusivity for password retrieval or multiple users checking out the same password for the same device in the same time period.	
32	The solution generates an alert if the password change fails after an administrator-specified number of retries.	
33	The solution should identify pending password changes to any target system that was unavailable at the time the change was initiated	
34	All locally stored target-account passwords should encrypted using AES or similar encryption with at least 256 bit keys.	
35	The solution should automatically reconcile passwords that are detected 'out of sync' or lost without using external restore utilities	
36	The solution should have the ability to reconcile passwords manually, upon demand	
37	The solution should automatically verify , notify and report all passwords which are not in sync with PIM	
38	The solution should have the ability to automatically "check-out" after a specific time and "check-in" within a specified time.	
39	The solution should set unique random value anytime a password is changed. The password generated should be strong and should not generate a similar value for a long iteration.	
40	**The tool allows secure printing of passwords in Pin Mailers or a secured printing form. Lifecycle of printing and labelling of envelopes should be part of the module.**	
41	The solution should be able to control re-prints with adequate authorization	
42	Secured platform - main password storage repository should be highly secured (built-in firewall, hardened machine, limited and controlled remote access etc.)	
43	The proposed solution should restrict the solution administrators from accessing or viewing passwords or approve password requests	
44	The solution should have the capability to seamlessly change the passwords for the large number of desktops.	
45	Ability to manage privileged passwords for multi-lingual servers	
46	Provision to prompt for a password change immediately after onboarding/vaulting a privileged account	
47	Provision to configure/define custom commands for password change without OEM's intervention.	
Access Control		
48	The solution should be able to restrict usage of critical commands over a SSH based console based on any combination of target account, group or target system and end-user.	
49	The solution should restrict privileged activities on a windows server (e.g. host to host jumps, cmd/telnet access, application access, tab restrictions) from session initiated with PIM	
50	The solution should be able to restrict usage of critical commands on command line through SSH clients on any combination of target account, group or target system and end-user.	
51	The solution should be able to restrict usage of critical commands on tables for database access through SSH, SQL+(client/), front-end database utilities on any combination of	

REVISED

	target account, group or target system and end-user.	
52	The solution enables an administrator to restrict a group of commands using a library and define custom commands for any combination of target account, group or target system and end user.	
53	The solution should provide secure mechanism for blacklisting/whitelisting of commands for any combination of target account, group or target system and end user.	
54	The solution can restrict user-specific entitlements of administrators individually or by group or role.	
55	The solution should have worklfow control built-in for critical administrative functions over SSH including databases (example user creation, password change etc) and should be able to request for approval on the fly for those commands which are critical.	
56	The solution can restrict target-account-specific entitlements of end users individually or by group or role.	
57	The solution can restrict end-user entitlements to target accounts through a workflow by days and times of day including critical command that can be fired.	
58	System should be able to define critical commands for alerting & monitoring purpose and also ensure user confirmation (YES or NO) for critical commands over SSH.	
Privileged Session Management and Log Management		
59	The solution should be able to support any session recording on any session initiated via PIM solution including servers, network devices, databases and virtualized environments.	
60	The solution should be able to **log commands** for all commands fired over SSH Session and for database access through ssh, sql+	
61	The solution should be able to log/search text commands for all sessions of database even through the third party utilities	
62	The solution should be able to log/search text commands for all sessions on RDP	
63	The solutions should support selective option for enabling session based recording on any combination of target account, group or target system and end-user.	
64	All logs created by the solution should be tamper proof and should have legal hold	
65	The solution logs all administrator and end-user activity, including successful and failed access attempts and associated session data (date, time, IP address. Machine address, BIOS No and so on). The tool can generate — on-demand or according to an administrator-defined schedule — reports showing user activity filtered by an administrator, end user or user group.	
66	The tool can restrict access to different reports by administrator, group or role.	
67	The tool generates reports in at least the following formats: HTML, CSV and PDF	
68	System should be able to define critical commands for alerting & monitoring purpose through SMS or Email alerts	
69	The solution should provide separate logs for commands and session recordings. Session recordings should be available in image/ video based formats	
70	The session recording should be SMART to help jump to the right session through the text logs	
71	Secure and tamper-proof storage for audit records, policies, entitlements, privileged credentials, recordings etc.	
72	The proposed solution shall cater for live monitoring of sessions and manual termination of sessions when necessary	
73	The proposed solution shall allow a blacklist of SQL commands that will be excluded from audit records during the session recording. All other commands will be included.	
74	The proposed solution shall enable users to connect securely to remote machines through the tool from their own workstations using all types of accounts, including accounts that are not managed by the privileged account management solution.	

REVICED

75	The proposed solution shall allow configuration at platform level to allow selective recording of specific device.	
76	The proposed solution shall allow specific commands to be executed for RDP connections (e.g. Start the connection by launching a dedicated program on the target machine without exposing the desktop or any other executables).	
77	The proposed solution shall support correlated and unified auditing for shared and privileged account management and activity.	
78	The proposed system shall support full colour and resolution video recording.	
79	The proposed system shall support video session compression with no impact on video quality.	
80	Ability to capture text logs for all privileged sessions	
81	Ability to perform text based search on video logs	
82	Ability to identify direct access to managed devices (bypass PAM) and alert/block access	
PIM Security		
83	The solutions should use minimum FIPS 140-2 validated cryptography for all data encryption.	
84	All communication between system components, including components residing on the same server should be encrypted.	
85	All communication between the client PC and the target server should be completely encrypted using secured gateway. (Example: a telnet session is encrypted from the client PC through the secured gateway)	
86	The Administrator user cannot see the data (passwords) that are controlled by the solution.	
87	Secured platform - main password storage repository/Vault should be highly secured (hardened machine, limited and controlled remote access etc.).	
88	The solution should secure master data, records, entitlement, policy data and other credentials in tamper proof storage container.	
PIM Administration		
89	The solution should have central administration web based console for unified administration.	
90	The tool uses Active Directory/LDAP as an identity store for administrators and end users.	
91	The tool enables an administrator to define groups (or similar container objects) of administrators and end users.	
92	The tool enables an administrator to add an administrator or end user to more than one group or to add a group to more than one supergroup.	
93	The tool enables an administrator to define a hierarchy of roles without limit.	
94	Administrative configurations (e.g. configuration of user matrix) shall be accessible via a separate client where client access is controlled by IP address.	
95	Important configuration changes in the solutions (example changes to masters) should be based on at least 5 level workflow approval process and logged accordingly	
96	Segregation of Duties - The Administrator user cannot view the data (passwords) that are controlled by other teams/working groups (UNIX, Oracle etc.).	
97	All administrative task should be done LOB wise i.e. Line of Business Wise	
98	Provision for User Creation approval/rejection via E-mail	
99	Provision for User self-registration in PAM	
100	Provision for bulk operation for management of devices inside PAM	
101	Provision for scheduling user access review inside PAM	
System Architecture		
102	The solution architecture should be highly scalable.	
103	The proposed solution shall provide multi-tier architecture where the database and	

REVICED

	application level is separated.	
104	The proposed solution shall provide scalability where it is not limited by the hardware. Also the solution shall provide modular design for capacity planning and scalability metrics.	
105	The proposed solution shall have the ability to support multiple mirrored systems at offsite Disaster Recovery Facilities across different data centre locations.	
106	The proposed solution shall have built-in options for backup or integration with existing backup solutions	
107	The proposed solution shall handle loss of connectivity to the centralized password management solution automatically.	
108	The proposed solution shall not require any network topology changes in order to ensure all privileged sessions are controlled by the solution.	
109	The proposed solution shall support distributed network architecture where different segments need to be supported from a central location.	
110	The proposed solution shall support both client based (in the case where browser is not available) as well as browser based administration	
111	The proposed solution should be 100% agentless that includes password storage, password management and session recording features.	
112	The solution must support parallel execution of password resets for multiple concurrent requests.	
113	The solution should provide fully automatic failover from a single active instance to a backup/standby instance with a fully replicated repository	
114	The solution should support multiple active instances with load balancing and fully automatic failover to another active instance	
115	The solution provides automatic detection of failure of the single/multiple active instance(s), and fully automatic failover to a backup/standby instance on a DR site.	
116	The solution if required should be available to install on a virtual sever	
117	The system should be highly available (24x7x365) and redundant from a hardware failure, application failure, data failure, and or catastrophic failure. Please elaborate	
118	The solution should have an ability to have direct connection to target device as well as using secured gateway channel	
119	Provision to deploy the solution on-premise, cloud or hybrid environment.	
120	Ability to run multiple PAM instances locally in case of connectivity failure (for multi-site setup)	
121	Zero downtime for performing upgrades/planned activities	
Out of box Integration		
122	Ability to integrate with enterprise authentication methods e.g. multiple 3rd party authentication methods including AD, LDAP, Windows SSO, PKI, RADIUS and a built-in authentication mechanism.	
123	Ability to integrate with Bio-Metric Solutions	
124	Ability to integrate with Hard and Soft token solutions	
125	Ability to integrate with ticketing systems.	
126	Ability to integrate with Automation softwares for enhancing productivity in the data center	
127	The proposed solution supports integration with the Hardware Security Module (HSM) devices to store the encryption keys.	
Ticketing System integration		
128	The solution can force the requestor of password / session to provide a reason, including a service desk incident ticket number, for the request.	

REVISED

129	The solution can communicate with a workflow engine to verify an incident ticket number cited in the end user's request.	
130	The solution provides the capability to enable end users to retrieve (or reset) a target-system password only after approval by a designated approver (to allow dual control). Approval criteria can be based on any combination of target account, group or target system and end-user identity, group or role, as well as contextual information such as day of the week or time of day.	
131	Ability to enforce ticketing integration as well as approval workflow for specific ticket types (e.g. change/incident ticket)	
132	Inbuilt ticketing system with 5 level workflow approval with ticket level validation, risk and impact assessments as per LOB wise, Service type and user type. This ticketing system to help in creating a work order on an executer, who will then request for the access through the request workflow with this valid ticket	
SIEM Integration		
133	The solution should be able to integrate with the bank SIEM and other leading SIEM Solutions.	
134	The solution should be able to integrated with applications like VA Systems, performance monitoring applications to eliminate hard coded passwords	
Application Password Management (Hard-Coded Password Management)		
135	The solution should have an ability to eliminate, manage and protect privileged credentials in applications, scripts, configuration files etc.	
136	The solution should be able to authenticate and trust the application requesting the privileged password based on various authentication methods	
137	Application Servers Support - The product should support removing static hard coded passwords from Data Sources in Application Servers. Please elaborate.	
Auto Discovery of Privileged Accounts		
138	The solution should be able to perform auto discovery of privileged accounts on target systems and perform two way reconciliation.	
139	The solution should provide feature for user governance on the target devices i.e autodetect users and schedule a governance workflow and user certification process with adequate review process.	
140	Ability to easily discover and flag accounts that do not adhere to the corporate password policy without having to implement a PAS solution	
141	Map privileged and personal accounts on various target systems	
142	Ability to quickly identify all non-built-in local administrator accounts in your environment (flag possible 'backdoor' accounts)	
143	Ability to quickly identify private and public SSH keys, including orphaned SSH keys, on Unix/Linux machines, extracts key related data and ascertain the status of each key.	
Notification Engine		
144	The solution should have capability to provide alerts and notification for critical PIM events over SMS & Email	
145	The solution should have capability to provide alerts and notification for all administration/configuration activities over SMS & Email	
146	Customizable notification for command executed on SSH and Telnet based devices	
147	Customizable notification for command/Process executed on Windows	
148	Notification on target being access on criteria like Line of Business or Groups	
Solution Workflow		
149	The solution should have inbuilt workflow to manage a. Electronic Approval based Password Retrieval	

REVICED

	b. Onetime access / Time Based / Permanent Access c. 5 level approval workflow with E-mail and SMS notification with delegation rules	
150	Ability to provide for delegation at all levels in the workflow	
151	Mobile device support - ability to send a request to access a password, approve the request and retrieve the password, all from a hand-held mobile device e.g. smart phones	
152	Supports a workflow approval process that is flexible to assign multiple level of approvers based on product or model (i.e. require 2 or more approvals before access is allowed).	
153	Supports a workflow approval process that requires approvers to be in sequence before final approval is granted.	
154	Ability to log workflow processes and/or have the ability to be reported or audited.	
Dashboard & Reporting		
155	Dashboard Capabilities should included real-time view of activities performed by the administrators	
156	The system shall have the ability to run all reports by frequency, on-demand and schedule.	
157	The solution should provide detailed and scheduled reporting with the following basic report sets Entitlements Reports, User's activities, Privileged Accounts inventory and Activities log	
158	The solution should have ability to report on all system administrative changes performed by PIM Administrators with relevant auditable records	
159	The solution should be able to report password lockouts (failure logon attempts)	
160	Ability to report password checkouts on systems and users requesting passwords	
161	Ability to report password lockouts (failure logon attempts)	
162	Ability to report on password change following verification process	
163	Ability to report on password status	
164	Reports should be customizable	
165	Audit data can be exported for use for any BI Tool	
166	Reports shall be automatically distributed by email	
167	Access to audit reports (and report configuration) shall be restricted to "auditor" end-users	
168	Ability to replay actual session recordings for forensic analysis	
169	Dashboard - for at a glance critical events and password policies.	
Risk & Threat Assessment		
170	Ability to analyze user behavior and predict unusual activity inside PAM	
End-Point Privilege Management		
171	Ability to manage passwords of privileged accounts on user workstations	
172	Ability to facilitate remote access of workstations with administrative rights to system administrators locally (over LAN) as well as over the internet	
Additional Features		
173	PAM Users to have a personal vault for secure storage of confidential files	
174	Provision to select file types that a PAM user can secure using the personal vault	
175	Ability to share files uploaded in personal vault with other PAM users	
176	Ability to authenticate Linux/Unix servers against Windows Active Directory (AD Bridging)	
177	The solution should provide multi-browser support	
178	The solution should bundle utilities for easy access to target devices incase of absence of native clients	
179	The solution must support integration with target devices for Single Sign On (SSO) using native client (e.g. NMS, IAM)	
Supplier's Eligibility Requirements		

REVISED

180	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.	
181	The supplier must be an authorized reseller or distributor of the brand being offered. Must submit certification from distributor or principal.	
182	The principall 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)	
183	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)	
184	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.	
185	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.)	
186	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		
187	Delivery after receipt of NTP: 60 calendar days	
188	Installation will start 7 calendar days after delivery and will end 90 calendar days after.	

REVISED