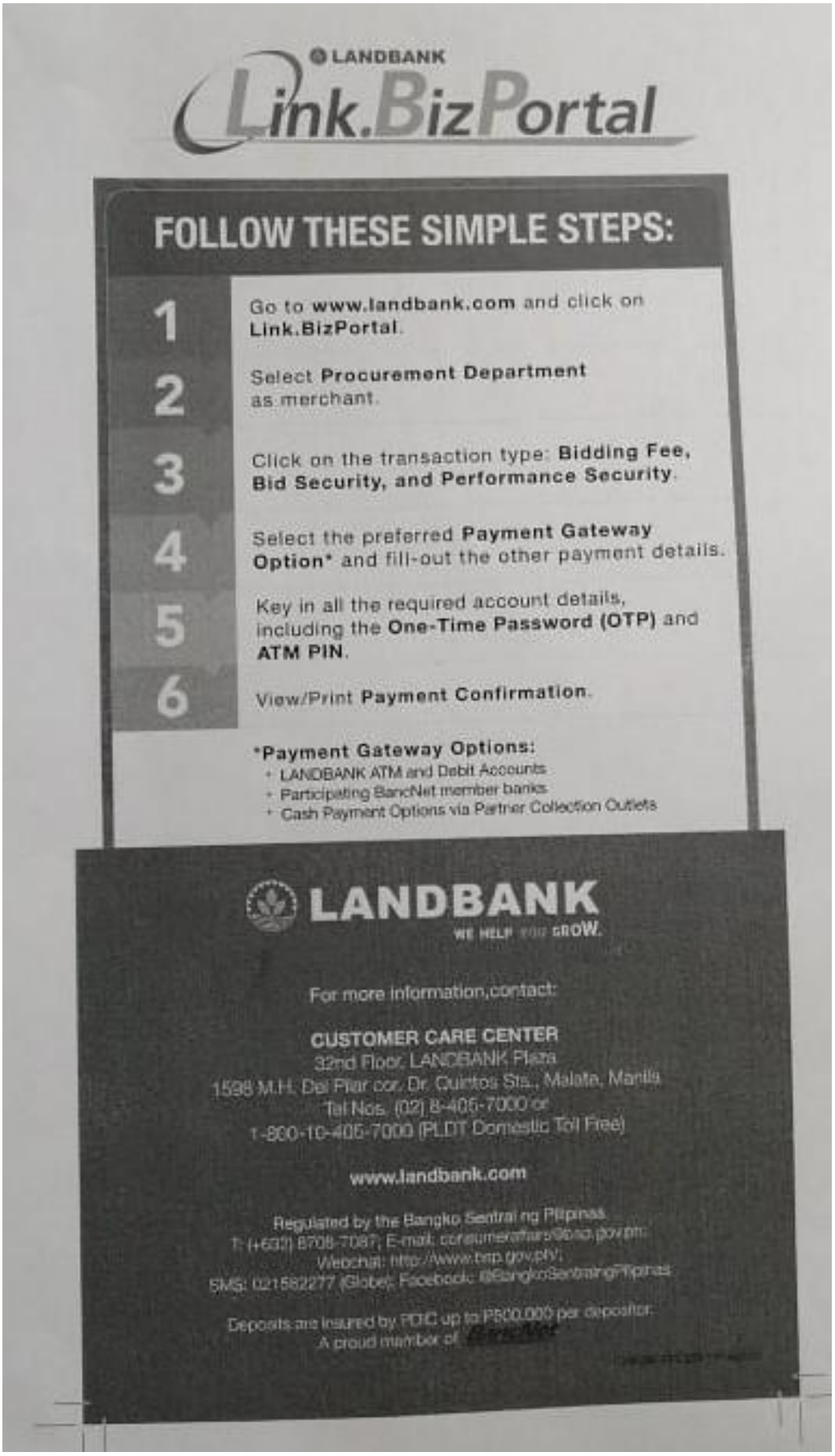

LANDBANK
Link.BizPortal
FOLLOW THESE SIMPLE STEPS:
1 Go to www.landbank.com and click on Link.BizPortal.
2 Select Procurement Department as merchant.
3 Click on the transaction type: Bidding Fee, Bid Security, and Performance Security.
4 Select the preferred Payment Gateway Option* and fill-out the other payment details.
5 Key in all the required account details, including the One-Time Password (OTP) and ATM PIN.
6 View/Print Payment Confirmation.
*Payment Gateway Options:
• LANDBANK ATM and Debit Accounts
• Participating BancNet member banks
• Cash Payment Options via Partner Collection Outlets
LANDBANK
WE HELP YOU GROW.
For more information,contact:
CUSTOMER CARE CENTER
32nd Floor, LANDBANK Plaza
1598 M.H. Del Pilar cor. Dr. Quintos Sts., Malate, Manila
Tel Nos. (02) 8-405-7000 or
1-800-10-405-7000 (PLDT Domestic Toll Free)
www.landbank.com
Regulated by the Bangko Sentral ng Pilipinas
T: (+632) 8708-7087; E-mail: consumeraffairs@bsp.gov.ph;
Webchat: http://www.bsp.gov.ph/;
SMS: 021582277 (Globe); Facebook: @BangkoSentralngPilipinas
Deposits are insured by PDIC up to P500,000 per depositor
A proud member of BancNet

Annex A

LAND BANK OF THE PHILIPPINES
PROCUREMENT DEPARTMENT

PRE-BID CONFERENCE REGISTRATION

Project Identification Number	**LBP-HOBAC-ITB-GS-20230725-01**
Project Name	**Two (2) Years Shared Cyber Defense Solution for the Insurance Cluster**
Company Name	
Address	
Name of Authorized Representative	
Contact Number	
eMail Address	
Please list down request for clarification/s, if any:	

Note: Please print or type all entries.

Annex B

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 consist of two identical copies of archived/compressed files (Copy 1 and Copy 2). The archived/compressed 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/compressed files shall be labelled as XYZ-081901(2)-C1 (for Copy 1) and XYZ-081901(2)-C2 (for Copy 2). Copy 1 shall serve as the primary file while Copy 2 shall be the backup file. The archived/compressed files shall be generated using either WinZip, 7-zip or WinRAR and password-protected.

   The above mentioned archived/compressed files shall contain the Technical Component and Financial Component files in PDF format. These PDF 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 the word "Tech" or "Fin" in the case of the Technical Component and Financial Component, respectively, each separated with a dash sign. Thus, using the above example, the archived/compressed files XYZ-081901(2)-C1 and XYZ-081901(2)-C2 shall both contain the PDF files labelled XYZ-081901(2)-Tech and XYZ-081901(2)-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.

   The archived file 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. The passwords for Copy 1 and Copy 2 shall be the same.

   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.

   In case of modification of bid, a modified version of Copy 1 and Copy 2 of the bid (archived/compressed) files shall be uploaded to the SFTF. 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. Using again the earlier example, the sample labels and contents of the modified bid shall be as follows: a) First Modification: XYZ-081901(2)-C1-Mod1 and XYZ-081901(2)-C2-Mod1 containing XYZ-

081901(2)-Tech-Mod1 and XYZ-081901(2)-Fin-Mod1, and b) Second Modification: XYZ-081901(2)-C1-Mod2 and XYZ-081901(2)-C2-Mod2, containing XYZ-081901(2)-Tech-Mod2 and XYZ-081901(2)-Fin-Mod2]. Only the latest modified bid shall be opened while the rest of the superseded bids will be rejected.

3. All bids shall be submitted electronically on or before the 10:00 A.M. deadline. All Bids must be accompanied by a bid security in any of the acceptable forms and in the amount stated in ITB Clause 14.1. Only electronic bids that are successfully uploaded to the Secure File Transfer Facility of LANDBANK on or before the deadline shall be accepted. 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.

   The prospective bidder shall receive an acknowledgement receipt via email *after* successful uploading of its/his/her 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.

4. On the bid opening date, the bidder shall confirm its/his/her 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. A maximum of two (2) accounts/connections per participating interested bidder shall be allowed to join the meetings.

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

6. 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.

   In case a bidder cannot connect to the videoconferencing via MS Teams application, the HOBAC Secretariat shall contact the bidder concerned through its registered mobile phone/landline telephone up to a maximum of three (3) call attempts with five (5) minutes interval after each call attempt. A text message advising the bidder that the public bidding has already started will also be sent by the HOBAC Secretariat. If the HOBAC Secretariat still cannot contact the bidder after the said allowable call attempts or the bidder is unable to contact the HOBAC Secretariat to provide the passwords needed to open its electronic bids when required by the HOBAC, the bidder concerned shall be disqualified from further participating in the bidding process.

7. 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.

8. 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.

9. 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/her Financial 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 or due to technical issues, the bidder concerned shall be disqualified from further participating in the bidding process. Thus, the bidders are encouraged to test their electronic bids and ensure that they are free from technical errors prior to uploading of the same to the SFTF.

10. 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.

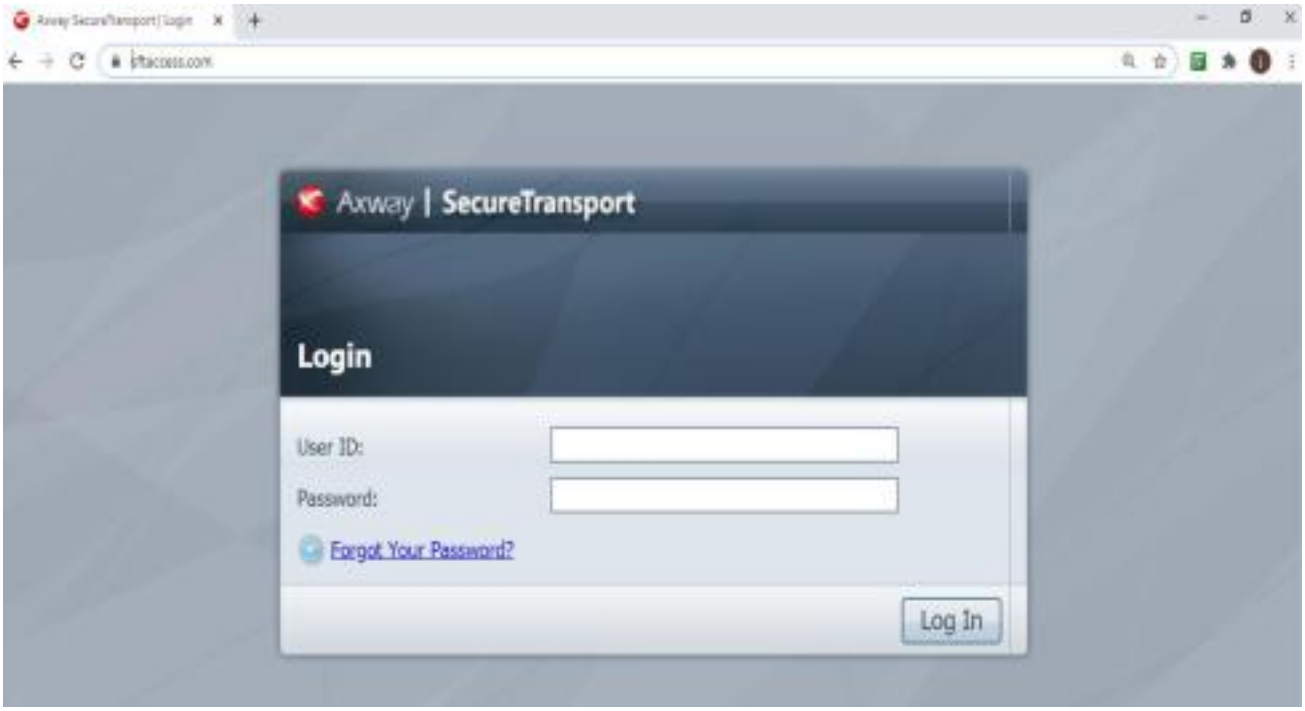
11. The retrieval and opening of the electronic bids, page-by-page review of documents and the results of the bid evaluation and ranking shall be shown to the participants through the screen sharing feature of MS Teams.

12. 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.

13. MS Teams Application shall be used in the conduct of online bidding through videoconferencing. 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**

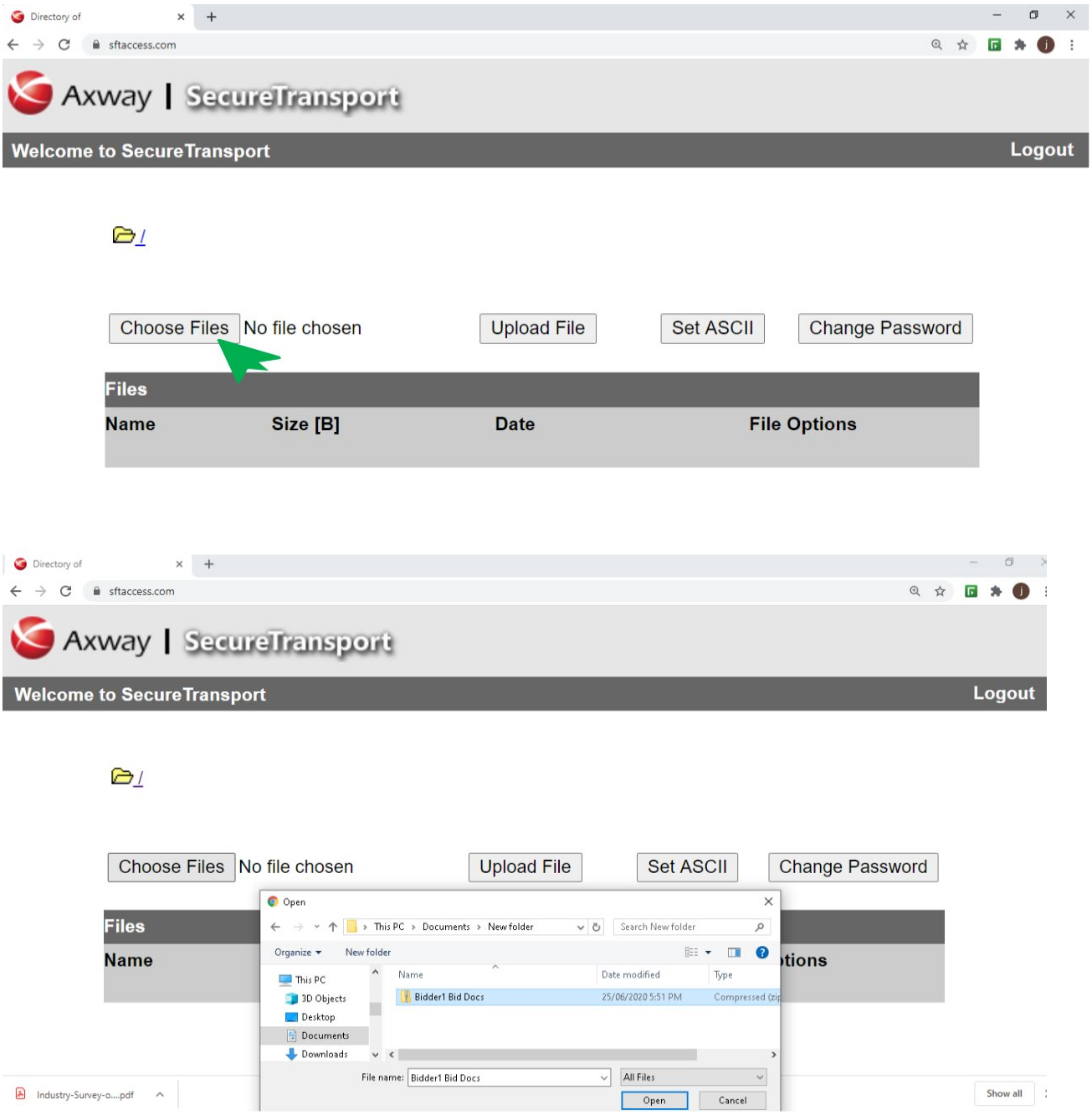
   Password: **[Landbank-provided password]**

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

   Notes:

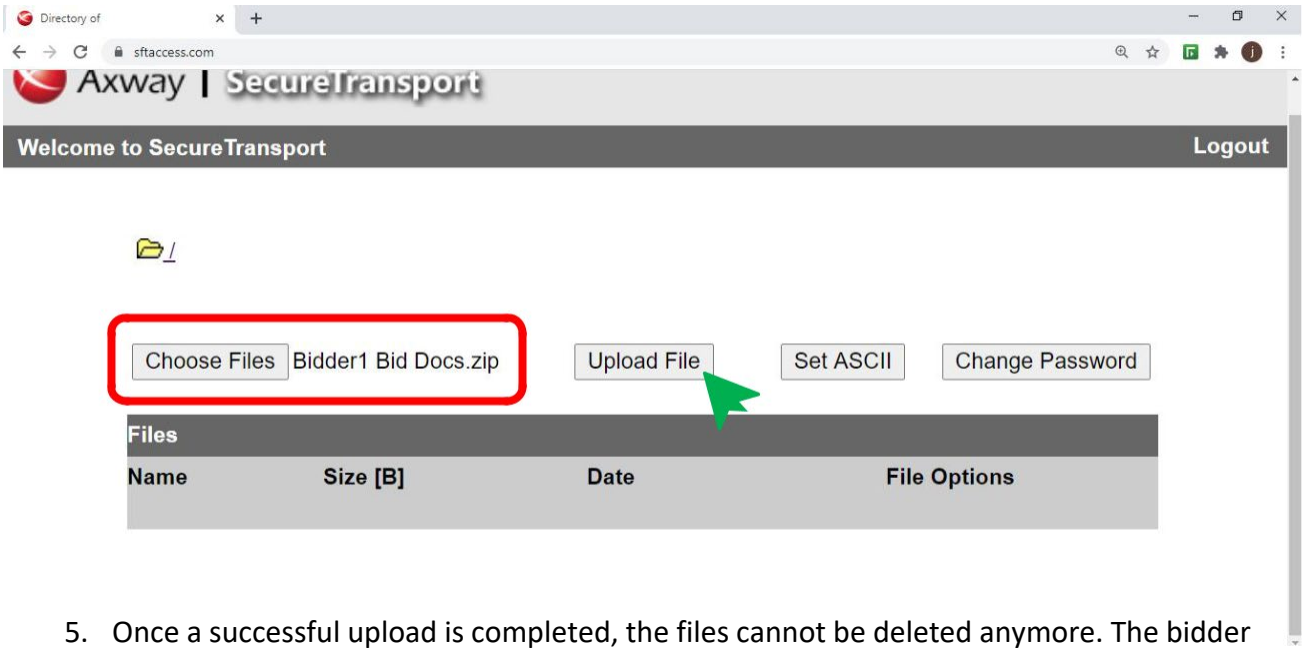
   1. Files should be encrypted/password-protected.

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

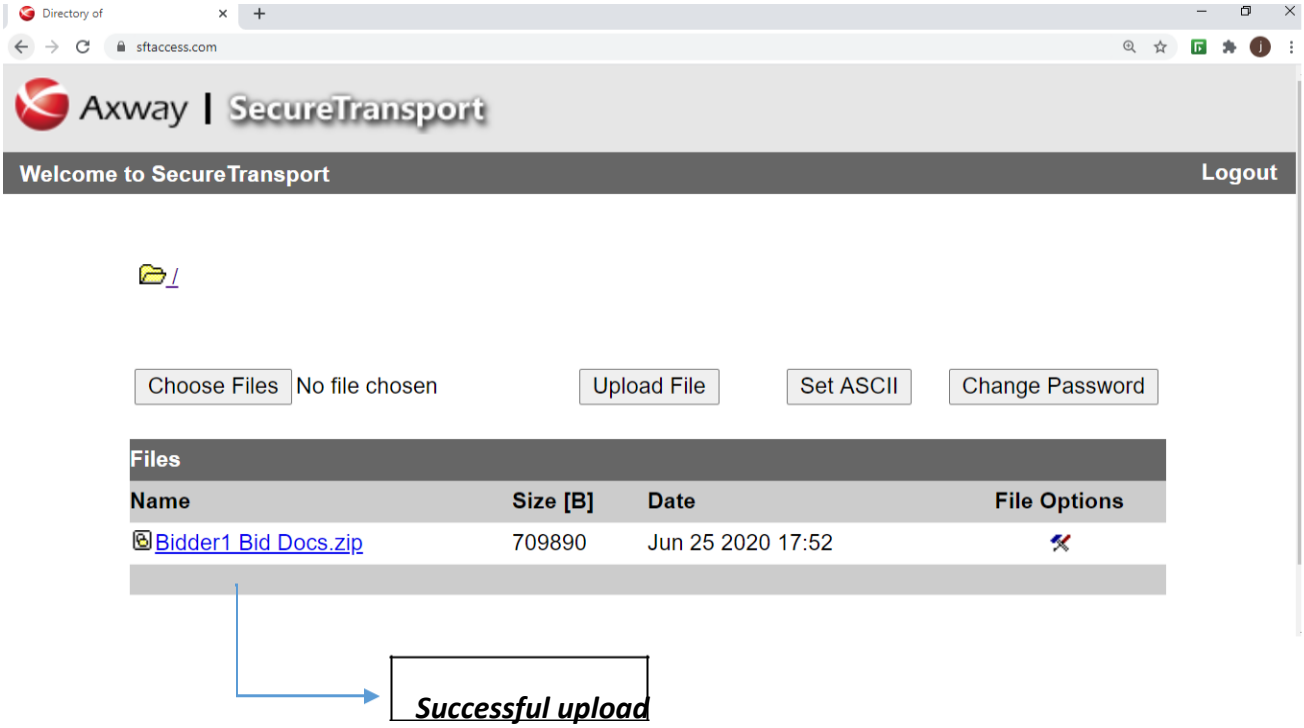

Directory of
sftaccess.com
Axway | SecureTransport
Welcome to SecureTransport
Logout
/
Choose Files
No file chosen
Upload File
Set ASCII
Change Password
Files
Name
Size [B]
Date
File Options
Directory of
sftaccess.com
Axway | SecureTransport
Welcome to SecureTransport
Logout
/
Choose Files
No file chosen
Upload File
Set ASCII
Change Password
Files
Name
Open
This PC
Documents
New folder
Search New folder
Organize
New folder
This PC
3D Objects
Desktop
Documents
Downloads
Name
Date modified
Type
Bidder1 Bid Docs
25/06/2020 5:51 PM
File name:
Bidder1 Bid Docs
All Files
Open
Cancel
Industry-Survey-o....pdf
Show all

Annex C-5

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.



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.

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

List of LANDBANK Officers, Employees and Consultant(s)

A. Board of Directors

Ex-Officio Chairman:	Sec. Benjamin E. Diokno, Department of Finance (DOF)
	Ms. Rosalia V. De Leon, Treasurer, Primary Alternate – DOF
	Mr. Erwin D. Sta. Ana, Deputy Treasurer, Secondary Alternate – DOF
Vice Chairperson:	Ms. Ma. Lynette V. Ortiz, President and CEO
Members:	Pres. Ferdinand R. Marcos Jr., Department of Agriculture (DA)
	Mr. Domingo F. Panganiban, Senior Undersecretary, DA
	Ms. Mercedita A. Sombilla, Undersecretary, Alternate Member – DA
	Sec. Bienvenido E. Laguesma, Department of Labor and Employment (DOLE)
	Mr. Benedicto Ernesto R. Bitonio, Jr., Undersecretary, Alternate Member – DOLE
	Sec. Conrado M. Estrella III, Department of Agrarian Reform (DAR)
	Mr. Napoleon U. Galit, Undersecretary, Alternate Member – DAR
	Ms. Nancy D. Irlanda, Representative - Private Sector
	Atty. David D. Erro, Representative - Agrarian Reform Beneficiaries Sector
	Ms. Virginia N. Orogo, Representative - Agrarian Reform Beneficiaries Sector

B. President and CEO: Ms. Ma. Lynette V. Ortiz

C. Bids and Awards Committee (HOBAC)

Chairman:	Mr. Reynaldo C. Capa, Senior Vice President – Banking Services Group
Vice Chairman:	Mr. Alwin I. Reyes, Vice President – Procurement Department
Regular Members:	Ms. Adelfa R. Masacupan, First Vice President – Asset and Liability Management Group
	Mr. Emmanuel G. Hio, Jr., First Vice President – Facilities Engineering Services Group
	Ms. Marife Lynn O. Pascua, Vice President – Agrarian Services Group
	Mr. Reo S. Andarino, Vice President – Digital Banking Support Department
Provisional Member:	Atty. Joseph Dennis C. Castro, Legal Manager - Legal Services Group

D. Technical Working Group

Mr. Archieval Tolentino (Land Bank of the Philippines)
Mr. David Andrei P. De Mesa (Bureau of the Treasury)
Mr. Jonathan Pineda (Government Security Insurance System)
Ms. Jocelyn Dela Peña (Social Security System)
Ms. Maria Belinda San Jose (Philippine Deposit Insurance Corp.)

E. HOBAC Secretariat

Head:	Atty. Honorio T. Diaz Jr.
Officers and Staff:	Ms. Remedios S. Lacaden, Senior Management Associate
	Ms. Ruby S. Cortez, Procurement Specialist III
	Ms. Farah Eva B. Esguerra, Administrative Specialist II
	Ms. Maribel J. Paredes, Procurement Specialist I
	Mr. Mark Anthony C. Pantalla, Procurement Analyst
	Ms. Jenica V. De Vicente, Procurement Assistant
	Mr. Jerome C. Relucio, ASO I

F. Procurement Department

Head:	Mr. Alwin I. Reyes, Vice President
Officers and Staff:	Ms. Ma. Victoria C. Viray, Senior Procurement Officer/Team Leader
	Ms. Rosemarie SJ. Mirando, Senior Procurement Officer/Team Leader
	Ms. Leonor F. Santos, Acting Senior Procurement Specialist/Team Leader
	Mr. Joel R. Perez, Senior Procurement Specialist/Team Leader
	Ms. Helen S. Purificacion, Senior Procurement Specialist/Team Leader

Mr. Donato DR. Cariaga, Senior Procurement Specialist/Team Leader
Ms. Kristi Ann P. Rutab, Procurement Officer/Team Leader
Atty. Karla May M. Temporosa, Administrative Officer
Mr. Rommel C. Pascua, Procurement Specialist III
Ms. Cathrina Marie A. Garcia, Procurement Specialist III
Mr. Rosalino V. Cruz, Procurement Specialist II
Ms. Lubelle B. Lumabas, Procurement Specialist II
Mr. Jerome V. Bueno, Procurement Specialist II
Ms. Nadia G. Ileto, Procurement Specialist I
Ms. Ma. Angela Q. Emeterio, Procurement Analyst
Ms. Jeramae F. Concepcion, Procurement Analyst
Ms. Kimberly Joy A. Sto. Tomas, Procurement Analyst
Mr. Jollianz Jenkin G. Dy, Procurement Analyst
Ms. Charmaine F. Mangilit, Procurement Analyst
Ms. Jeah Chrysel L. Escalona, Procurement Analyst
Mr. Marlon R. Faraon, Procurement Analyst
Mr. Aaron V. Sedanto, Procurement Analyst
Mr. Rudyrick B. Silva, Procurement Analyst
Ms. Fretch Camille J. Japole, Procurement Assistant
Mr. Mark Anthony M. Abad, Procurement Assistant
Ms. Almay Joyce B. Ruz, Procurement Assistant
Ms. Vinna Mariella T. Custodio, Procurement Assistant
Ms. Ma. Theresa N. Cruz, Acting Executive Assistant
Ms. Julieta S. Rabino, ASO I
Ms. Joy L. Gabay, ASO I
Mr. Jesus David, SCW
Mr. Emil Dela Cruz, SCW
Mr. Erikson Guani, SCW
Mr. Vicente Gutierez, Jr, SCW
Mr. Andrew Palma, SCW
Mr. Dexter Naguit, SCW
Mr. Ramil Pendilla, SCW
Mr. Frederick Reyes, SCW
Mr. Pablo Tenoria, SCW

SHARED CYBERDEFENSE SOLUTION (REBIDDING)

Terms of Reference (Insurance Cluster)

Version Number	:	4.3
Date	:	3 August 2023
Author	:	Government Service Insurance System Bureau of the Treasury Social Security System Philippine Deposit Insurance Corporation

1. Name and Description of the Project

With the continued evolving nature of cybersecurity risks, the Secretary of Finance has mandated various agencies under the Department to establish a cost-effective defense strategy that will add a layer of defense for the agencies to shield their respective IT systems from potential cybersecurity threats, along with other possible risks and data breaches in the digital landscape.

For this Terms of Reference (TOR), it will cover the Insurance Cluster composed of the Bureau of the Treasury (BTr), Government Service Insurance System (GSIS), Social Security System (SSS), Philippine Deposit Insurance Corporation (PDIC).

2. Project Objective and Scope

The proposed Common Cyber Defense Solution shall require the vendor to provide a two (2) year subscription for the provision of Security Monitoring and Management, Vulnerability Management, Threat Intelligence, and Incident Response. This is primarily focused on the National Institute of Standards and Technology (NIST) Cybersecurity Framework – Identify, Protect, Detect, Respond and Recover.

The Approved Budget for the Contract (ABC) shall be the upper limit or ceiling for the proposal, and shall cover all project costs, including, but not limited to the following:

- Subscription cost that will be based on the number below:

Agency	Servers	Desktops/Laptops	Total
BTr	150	1450	1600
GSIS	400	4000	4400
SSS	200	7800	8000
PDIC	82	1118	1200

- The project shall include project management, consulting, requirements validation, customization, training, integration, training, production deployment, system integration, change management and other out-of-pocket expenses (e.g., transportation allowance, per diem, etc.);

- The Shared Defense subscription shall commence immediately after the Phase 1 implementation of the project.

- Post Go Live support starting from the implementation date; and

- All applicable taxes, service fees and charges (e.g., fund transfers fees, foreign exchange difference)

The proposed Common Cyber Defense Solution for the Insurance Cluster shall be procured in one lot which shall consist of sublots per agency. Likewise, this shall be the basis for awarding per agency.

The pricing shall be uniform for all agencies in the cluster.

Other Requirements

During procurement, the bidder is required to submit respective proposals for all the agencies concerned.

3. Functional and Non-Functional Requirements

The vendor shall respond to each requirement stated herein. Failure to conform to any of the specifications shall be sufficient grounds for disqualification.

I. Functional Requirements

A. Security Monitoring and Management	COMPLIED	REMARKS
A.1 Security Operations Center (SOC)	**Y/N**	
1. The service provider shall provide a cloud-based SOC for individual agencies with complete Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solution that allows for two-way integration with the agencies data sources, capture of near real-time log data, and must perform correlation between data sources during investigation which shall also be accessible by the individual agencies.		
2. The service provider shall set up a cluster level SOC dashboard to have an integrated and high level overview of the cluster agencies security posture.		
3. The SOC, through the SIEM, shall detect and monitor threats, correlate with threat intelligence sources, generate alerts, conduct investigation, and escalate tickets to the agencies on a 24x7 basis, using the Security Operations Center (SOC) platform, inclusive of the security tools to be provisioned for the agencies.		
4. There must be a proper onboarding and integration period between the service provider and the agencies prior to full SOC operation to ensure completeness of SOC visibility and familiarization with the agencies processes and network behavior.		
5. The SOC solution shall have its own ticketing tool for incident ticket generation.		
6. The SOC solution, through the SIEM, shall classify security events based on the following risk rating matrix containing the following information. The report method shall be thru call and/or e-mail:		

		Impact				
	Response Time	High	Medium	Low	Very Low	**Report Time**
Priority	Within 2 hours	P1	P2	P2	P3	within 15 minutes
	Within 12 hours	P2	P2	P3	P4	within 30 minutes
	Within 24 hours	P2	P3	P3	P4	N/A
	24 hours	P3	P3	P4	P4	N/A

- Impact: Severity of the security event to critical assets

• Priority: Based on the impact and severity • Nature of threat • Potential business impact • Remediation recommendations **Response Time: How soon the security incident must be acknowledged by the service provider* **Report Time: How soon a reference number/ problem ticket must be created by the service provider and received by the agency. The Report Time is included in the Response Time.*		
7. Monthly monitoring service management: The service provider shall conduct regular meetings with the agencies IT stakeholders to review SOC performance and discuss the overall IT security posture of the agencies, including fine-tuning of configurations and provision of best practices advice, to aid in continuous improvement. Regular written reports must also be available to track the status of cases and the assistance needed. Monthly reports shall contain, but not limited to: • SLA Performance • Correlated Events Overview • Correlated Events Graph Distribution Overtime • Correlated Events and Rules Triggered Summary • Summary of Incident Ticket per Use Cases Incident Management		
8. The service provider shall ensure flexibility and scalability of the agencies SOC platform and shall ingest and process all events sent by the agencies for the SIEM and SOAR requirements including its current and future needs.		
9. The service provider shall facilitate SOC security briefing at least once a month for the agencies to present the latest local and international news and updates in Cyber security.		
A.2 Managed Detection and Response	**COMPLIED**	**REMARKS**
A.2.1 Deployment and Management	**Y/N**	
1. The service provider shall supply Managed Detection and Response services, including the Endpoint Protection / Endpoint Detection and Response (EDR) licenses required for supported endpoints. Supported endpoints refer to Windows endpoints, Windows servers, major Unix and Linux distributions, MacOS, Mobile devices, that is still under support or extended support by the manufacturer.		
2. The solutions provider must be capable to deploy the endpoint technology to workstations and servers, including Windows, Mac, Unix and Linux assets, using the agencies or the solutions providers deployment tool, and must support both physical and virtual environments.		
3. For non-supported systems, other means of monitoring must be performed, such as network detection and response (NDR or similar) tool shall be provided.		

4. The solution shall detect and prevent attacks on-premise, for supported and unsupported endpoints, including agency deployments in public clouds, if any, such as, but not limited to Amazon Web Services (AWS), Azure, Oracle Cloud and Google Cloud.		
5. The solution shall be capable to block malicious indicators of compromise (IOCs) and behaviors of compromise (BOCs) automatically with expert review of detections by analysts to ensure there is always human oversight on technology.		
6. The solution shall allow custom enforcement policies to neutralize sophisticated malware and lateral movement utilizing ”living off the land” techniques that can potentially evade standard detections, however, ensuring that these custom policies does not impede business operations.		
7. Update of Indicators of Compromise (IOC) and watchlist repository, whenever applicable		

A.2.2 Prevention and Detection	**COMPLIED Y/N**	**REMARKS**
1. The solution shall have integration with the SIEM for central monitoring and analysis, including the setup of relevant dashboards such as but not limited to, attacks, threats, endpoints at risk.		
2. The solution should utilize signature-based and/or signature-less detection techniques to protect against known and unknown attacks.		
3. The solution should have Machine Learning and Behavioral Pattern Indicator of Attack (IOA) detection capability.		
4. The solution must be able to detect and prevent the following: • exploitation behavior using IOAs and no signatures. • ransomware behavior using Behavior IOA patterns and no signatures. • file-less malware using Behavior IOA patterns. • malware-free tradecraft using Behavior IOA patterns. • BIOS level attacks • Privilege Escalation • Exfiltration • Connection to malicious command and control destinations		
5. The solution must be able to enrich a detected event with its own threat intelligence and not any third-party Intelligence including mapping of the technique, tactic and procedure (TTP) against the MITRE ATT&ACK framework.		
A.2.3 Threat Hunting and Response	**COMPLIED Y/N**	**REMARKS**
1. The service provider must provide 24x7 Managed Threat Hunting Service, supported by experienced and certified analysts or incident responders for the remote response on endpoint incidents/events		

2. The service provider must have pre-built threat hunting applications and queries		
3. The service provider must be able to get context from indicators such as IP's, URL's, domains, or hashes using the tools within the platform, including associated events with unique visibility including account creation, login activity, local firewall modification, service modification, sources of remote operations (including scheduled task creations, registry changes, WMIC execution, among others)		
4. The solution shall be able to isolate "at-risk" endpoints, including the blocking the launching of suspicious or malicious applications.		
5. The solution shall allow blacklisting and whitelisting of hashes manually through the solution.		
6. The solution shall provide remote response by administrators, analysts, or incident responders such as containment, deleting files, killing process among others without the need for additional tools or agents.		
7. The solution shall provide root cause analysis of all identified malicious activity.		
A.3 Security Information and Event Management (SIEM)	**COMPLIED Y/N**	**REMARKS**
1. The solution shall provide individual agency, web-based dashboards for accessing their agency information about alerts, attacks, track remediation on incidents, generate and extract reports which can be presented near real-time or over a time period. The agencies must be able to request customized dashboards and ad-hoc reports from the service provider.		
2. The solution shall be capable to support collection of different types of metadata (e.g., logs, security events, network flows, among others) from data sources and shall include log compression and industry standard encryption at rest and in transit to ensure security of captured data from disclosure to disinterested parties.		
3. The data sources ingested by the solution shall include at least the events from perimeter security tools, active directory logs, endpoint protection, and endpoint detection and response tools, including events from sensors that may be deployed by the solutions provider, if needed.		

4. The maximum aggregate daily data ingestion shall be as follows: Agency / Daily Event Log Aggregate Size in Gigabytes (GB) BTr — 17 GB GSIS — 24 GB SSS — 48 GB PDIC — 15 GB		
5. The service shall have content packs that are prebuilt configurations for common security use cases that provide sets of rules, alarms, baselines, views, reports, variables, and watchlists.		
6. The service shall provide advanced security capabilities, such as User and Entity Behavioral Analytics (UEBA), natively within its own platform.		
7. The solution must integrate with the global threat intelligence subscription service for data enrichment to quickly identify attack paths and past interactions with known bad actors and increase threat detection accuracy while reducing response time.		
8. The solution must be able to generate and send actionable items to the automation and orchestration tool as well as generate and send alerts to both service provider and agency analysts and incident responders.		
9. The service provider shall ensure the availability of the ingested raw logs twelve (12) months with comprehensive searchability. The logs, including evidences of security incidents, should be tamper proof and made available for legal and regulatory purposes, as required. The logs beyond the retention period shall be archived and given monthly to the agencies in an agreed format.		
10. The service provider shall ensure that the data ingested from the insurance cluster is not shared or disclosed to or accessed by parties not mentioned in the contract unless explicitly granted permission by the cluster.		
A.4 Security Orchestration, Automation and Response (SOAR)	**COMPLIED Y/N**	**REMARKS**
1. The solution must be able to integrate with the SIEM and fully orchestrate security operations and provide security teams with case management, automation, and investigation within a single pane of glass		
2. The solution must have visibility into the security operation provided via dashboards, KPIs and customizable reporting		
3. The solution must be able to support machine driven and analyst led response to remediate threats in a consistent and auditable manner		

4. The solution must render alerts, cases, query reports, and events into clustered and contextualized threat storylines with a high degree of visualization		
5. The solution must be an open architecture that allows for easy connectivity and integrations to any existing system, bringing them all together into a single, contextual language. Integration with other solutions can either be out of the box or customized.		
6. The solution must be able to accelerate security incident processes by automating or semi automating workflows		
7. The solution must be include out of the box or customizable playbooks of best practices to scale operations, drive consistency in response and meet compliance requirements. Playbooks deployed shall include at least: • Phishing enrichment and response • Malware endpoint response • Login Anomalies (multiple failed logins, unusual activity such as login attempts outside office hours, etc) • Unusual browsing activity • Web attack profiling and blacklisting		
8. The solution should provide pre-set and customizable KPI metrics to monitor threat response efficacy and team performance.		

B. Vulnerability Management and Penetration Testing		
B.1 Vulnerability Management	**COMPLIED Y/N**	**REMARKS**
1. The solution provided must be a cloud based service, integrated within the SIEM, that shall give immediate global visibility into where the Agency IT system might be vulnerable to the latest Internet threats and how to protect them.		
2. It should be able to continuously identify threats and monitor unexpected changes in the network before they turn into breaches. The solution can be agentless or agent-based if continuous monitoring is required on specific systems.		
3. The solution should be able to scan systems anywhere in the Agency environment, from the same console: whether the asset is on the perimeter, the internal network, or cloud environments (such as Amazon Web Services, Oracle Cloud, Microsoft Azure or Google Cloud) with the ability to create custom reports showing each audience just the level of detail it needs to see.		
4. The solution should be able to identify and prioritize critical vulnerabilities and risks to enable the agencies to prioritize the remediation of the highest business risks using trend analysis, zero-day and patch impact predictions.		
5. The solution should be able to track vulnerability data across hosts and time, to give a better understanding of the agencies security posture. The reports can be changed through existing pre-built templates, without the need to rescan. The reports can be generated on demand or		

scheduled automatically and then shared with the appropriate recipients online, in PDF or CSV		
6. The solution should be able to automatically gather and analyze security and compliance data in a scalable backend, with provisioning additional capabilities as easy as checking a box.		
7. The solution should be able to proactively address potential threats whenever new vulnerabilities appear, with real-time alerts to notify the agencies immediately, without the need to schedule scan windows or manage scanning credentials.		
8. The solution must be able to conduct a continuous compromise assessment, which shall include at the minimum: • Identification of the specific vulnerabilities, at risk, and/or compromised assets • Evaluation of scanned assets and identification of possible vulnerability linkages through a detailed analysis of the results		
B.2 Vulnerability Assessment and Penetration Testing (VAPT)	**COMPLIED Y/N**	**REMARKS**
1. Vulnerability Assessment and Penetration Testing (VAPT) shall be performed annually on an agreed schedule and scope with the agencies. The VAPT scope may include network infrastructure, applications (e.g., public-facing web and mobile applications), Application Programming Interfaces (APIs), endpoints, hosts and databases, including member service systems or kiosks, if any and among others.		
2. The scope of VAPT shall be at least the following:		
3. The service provider shall deliver and maintain a vulnerability database with relevant software version upgrades and security policy update recommendations, inclusive of changes to existing and new vulnerability and threat signatures.		
4. The service provider shall provide online reporting and metrics capability: • VAPT results/data (including risk, remediation status, and data compromised, if any) and access to historical test result and trend analysis delivered via the service provider's portal shall be accessible to the agencies. This would also include handholding with the agencies concerned to properly remediate/mitigate vulnerabilities, findings, and observations.		

Agency	Scope
BTr	7 External resources, up to 80 IP addresses
GSIS	20 External resources, 2 mobile apps, up to 80 IP addresses
SSS	25 External resources, 1 mobile app up to 150 IP addresses
IC	20 External resources, up to 80 IP addresses
PDIC	8 External resources, up to 80 IP addresses

5. The service provider shall have predefined fields/templates for the generation of reports, such as, but not limited to: • VAPT Report (i.e., Executive Summary, Conclusion for Management Area, and Specific Action Plans) • Security Profiling Results (including reports from automated scanning tools) • Detailed observations and recommendations		
6. Common Vulnerability Scoring System values: • The service provider shall use CVSS v3.0 or later for risk ranking and prioritizing security vulnerabilities.		
• The service provider shall be capable to generate multi-format reports, including exporting of report data in PDF, Microsoft Excel, XML, CSV, and HTML.		
7. The service provider shall perform Host discovery and Operating System (OS) fingerprinting functionalities for the following, but not limited to: • Windows (all versions) • Linux and other Unix flavors (all versions) • Network and security related equipment, whether software or hardware-based • User profile settings • Advanced password analysis		
8. The service provider shall perform common service discovery and fingerprinting functionalities for the following, whether on-premise or cloud-based: • Application servers • Authentication servers • Backdoors and remote access services • Backup applications/tools • Database servers • Active Directory, Lightweight Directory Access Protocol (LDAP) • Domain Name Systems (DNS) • Mail servers and Simple Mail Transfer Protocols (SMTP) • Network File Systems (NFS), Network Basic Input/Output System (NetBIOS) and Common Internet File Systems (CIFS) • Network Time Protocols (NTP) • Remote Procedure Calls • Routing protocols • Simple Network Monitoring Protocol (SNMP) • Telecommunications Network (Telnet), Trivial File Transfer Protocol (TFTP), Secure Shell (SSH) • Virtual Private Network (VPN) • Web and mobile applications • Web servers		

C. Threat Intelligence	COMPLIED	REMARKS
1. The solution shall deliver threat intelligence on the following:		
• Brand protection - company names/domain		
• Social media pages		
• External Internet Protocol (IP) addresses		
• Website and mobile application monitoring		
• VIP e-mails		
• Sector monitoring Financial, Government, Insurance, and Healthcare		
• Society for Worldwide Interbank Financial Telecommunication (SWIFT) codes		
• Credit cards		
• GitHub		
• Custom queries		
• 25 Site take downs for each agency during the duration of the contract(i.e., phishing, social media sites, and others) however, should the agency need additional takedowns, this will be provided by the service provider at no additional cost.		
• Scraping databases that contain large amounts of data found in the deep and dark web		
• Third party queries		
• Investigation		
• Threat library		
2. The threat intelligence solution must, at minimally, harvest data from the following open, technical and closed sources types:		
• Mainstream Media (including news, information security sites, vendor research, blogs, vulnerability disclosures)		
• Social Media		
• Forums		
• Paste Sites		
• Code Repositories		
• Threat lists (including spam, malware, malicious infrastructure)		
• Dark Web (including multiple tiers of underground communities and marketplaces)		
• Original research from in-house human intelligence analysts		
3. The solutions provider must be able to:		

• Detect and take down servers launching phishing attacks		
• Take down of fake applications that impersonate legitimate ones from app stores.		
• Take immediate action on the agencies behalf and provide all the context to execute rapid take-down of malicious servers, websites or social media accounts.		
4. The solution shall be capable to detect leaked Personally Identifiable Information (PIIs) and the agencies information from the deep and dark web, social media, and other forms of instant messaging platforms and provide recommended action plan.		
5. The threat intelligence solution must be able to identify fraudulent social media accounts that are impersonating the agencies and its executives		
6. The solution shall monitor the domains and IP addresses that have bad reputation.		
7. The service provider shall consume internal and external threat intelligence into its threat analysis process.		
8. The service provider shall deliver weekly intelligence summary reports on the latest cyber threats, including detected information on the intention to target agencies or other government industries, major activist campaigns, and indications of activism against the agencies, financial and health sector, and the government.		
9. The service provider shall provide a special report or notice to the agencies immediately, should there be any information or detection of targeted attacks against the agencies, the government or the sectors of the concerned agencies.		

D. Incident Response	COMPLIED Y/N	REMARKS
1. The service provider shall review the agencies Incident Response Plan (IRP), which would guide the agencies on the creation, enhancement, and documentation of incident response playbooks, policies, and guidelines, such as, but not limited to: • Escalation process • Incident containment process • Incident eradication process • Incident recovery process • Incident identification process • Process flow		
2. The service provider shall act as the Incident Response (IR) Manager and facilitate the six (6) phases of IR. The service provider must be on-call and will conduct the IR activities onsite, as necessary (i.e., in cases of breach). The IRs per agency shall cover 200 accumulated hours per year. Beyond the required 200 hours, the agencies shall shoulder the cost. In case the 200 hours allotted for IR is not fully or not consumed, it can be converted to other services, such as training among others, that the provider can render for information security.		
3. The service provider shall conduct an annual, or as needed, IR readiness training to the agencies Computer Security Incident Response Teams (CSIRT), including IT security awareness trainings to both technical and non-technical audiences of the agencies. The		

readiness training shall include best practices recommendation in isolation, containment, and remediation activities of the security incident.		
4. The service provider shall conduct an annual, or as needed, incident response drill or simulation exercises with the agencies-CSIRTs to improve detection and internal readiness for cyber security incidents. This will include internal and external incident communications, reduced impact on operation continuity, reporting to regulators (e.g., NPC, DICT), CSIRT readiness, blue team capability, tabletop exercises, among others.		
5. The Service Provider shall map security playbook and runbooks for applicable security use cases to guide client on their incident response.		
6. The service provider shall deliver technical assistance to the agencies CSIRTs during emergency (successful) breach response.		
7. The Service Provider shall have a facility to receive client's reported incident (via authorized point of contact from client) for incidents not captured on the monitoring tool.		
8. The service provider shall deliver network/firewall/web applications breach response.		
9. The service provider shall identify, cleanse or contain malicious code, malware, spyware, and system-file hacks.		
10. The service provider shall deliver root cause analysis to identify the intrusion vector and provide mitigating procedures to address network and system vulnerabilities.		
11. The service provider shall identify indicators of compromise and scan the network to search for other related infected systems.		
12. The service provider shall deliver insider threat investigation, as needed.		
13. The service provider shall deliver employee misconduct investigations, as needed.		
14. The service provider shall deliver incident and investigation reports.		
15. The service provider shall have a certified and recently trained (at least in the past 12 months) in-house cyber security forensics specialist, to support advanced investigation.		
16. The service provider shall assist in the following: • Incident handling preparation and execution • Crisis management • Breach communication • Forensic analysis including preservation of evidence for chain of custody requirements • Remediation		
17. The Service Provider shall rate the prioritization and severity of security incidents and create a service ticket as per agreed Service Level Agreement (SLA).		

Service Level Agreement (SLA)

1. Acknowledgement SLA - The Acknowledgement SLA Percentage shall be computed per month base on the total number of missed hours exceeding the Acknowledgement SLA guarantee of fifteen (15) minutes per incident

Service Level Target	Description
98%	Acknowledgement SLA of 15 minutes from the time incident is detected by SIEM or from the time the Client provides a proof of compromise (POC) incident report, whichever comes first, up to the creation of service ticket.

2. Incident Response SLA - Time to respond or provide request from when incident or request is reported based on severity level.

Priority Level	Incident Response Time	Reference:
P1 - Catastrophic	Within 60 minutes	From the creation of service ticket up to triage. Triage is when the SOC L2 Incident Responder communicates with the client to further investigate and provide recommendation on how to contain, remediate, and recover from the security incident.
P2 - Critical	Within 90 minutes	
P3 – Marginal	Within 120 minutes	
P4 - Negligible	Within 160 minutes	

	Target Response Time % per Month		
Incident Priority	1 and 2	3 and 4	
	>=90%	>=80%	Sum of the number of incidents meeting required Response Time for all days in the month

II. Non-functional Requirements

A. Access Management	COMPLIED Y/N	REMARKS
1. All credentials with the service provider shall be stored in a monitored central management system. These are leased to the agencies once strong authentication has been implemented and for the specific task for which it was authorized.		
2. The service provider's solution shall be accessed through a centralized portal, which enforces session timeouts, mandates the use of multi-factor authentication (MFA), and provides anomaly detection for monitoring user behavior.		
3. The service provider shall maintain logical access controls which are role-based, including principles of least privilege and segregation of duties.		
4. All passwords must have a minimum of fifteen (15) characters. Passwords must be changed every ninety (90) days and cannot be the same as the prior three (3) passwords. The service provider's system must mask passwords when entered and store password files separately from the application system data. Only encrypted hashes of passwords may be stored and transmitted.		
5. All access from the service provider's managed endpoints to sensitive resources shall be done via VPN configured with MFA. Opportunistic Transport Layer Security (TLS) is configured by default for e-mail. Remote hardware is managed by comprehensive enterprise management software that allows for maintenance and access control management.		
6. The service provider shall provide physical and environmental controls at the primary and secondary sites for this project.		
7. The agencies data shall be logically separated by using unique tagging to ensure segregation of data from the other agencies. The agencies should retain as the legal owner of the data processed and managed by the service provider.		

B. Training and Other Requirements	COMPLIED Y/N	REMARKS
1. The service provider should facilitate at least once a year Continual Service Improvement (CSI) workshop with client for possible improvement of service through process, people and technology.		
2. The service provider should provide security advisories with the client for the cybersecurity news and updates like the latest viruses, trojans, worms, or other malicious programs.		
3. The service provider shall conduct an annual cyber security maturity assessment (i.e., people, process, and technology) on each Government Agency based on the NIST or CIS Controls.		

C. Service Provider's Qualification and Requirements *Note: Submission of required documents shall be during the submission of bids.*	COMPLIED Y/N	REMARKS
1. The service provider must be a certified/authorized reseller of the brand(s) being offered and shall submit a valid, certification from the manufacturer(s).		
2. The service provider must submit the following certifications: a. For Cloud based Security Operations Center (SOC), that this is hosted in a provider categorized as a leader either in the latest Forrester Wave™: Public Cloud Development And Infrastructure Platforms report or Gartner Magic Quadrant for Cloud Infrastructure and Platform Services; b. For Endpoint Detection and Response (EDR), that solution is categorized as a leader either in the latest Forrester Wave™ report for Enterprise Detection and Response or Gartner Magic Quadrant for Endpoint Protection Platforms; c. For Security Information and Event Management (SIEM), the solution provided is categorized as a leader in the latest Forrester Wave™ report for Security Analytics Platforms or Gartner Magic Quadrant for Security Information and Event Management (SIEM).		
3. The service provider must have 24 x 7 x 365 local technology operation center (SOC/NOC facilities/infrastructure and service), with a pool of at least 20 IT or Information Security related certified onsite support engineers within Metro Manila. A list of the support engineers shall be provided with their required qualifications, as stated in item D. Personnel Qualifications / Requirements.		
4. The service provider must have sales and technical offices located in the Philippines. The service provider should submit the list of their sales and technical offices in the Philippines, including the complete address and contact details. This is subject for actual site visit to the facility.		
5. The SOC can be provided on the cloud or within the premises of the service provider. Should the Security Operations Center (SOC) with their SOC analysts be on premise, they should be housed in a Data Center with TIA-942 Rated 3 Facility Certification or any equivalent third party assessment indicating the capability of the SOC to provide the required security, scalability, stability and high performance.The proof of compliance shall be submitted. 6. However, if the service provider's SOC will be implemented through a cloud service provider (CSP), the SOC platform must be guaranteed with at least 99.9% uptime or availability. The proof of compliance shall likewise be submitted.		
7. The service provider's SOC Analysts must have at least one or more of the following certifications: Certified Ethical Hacker (CEH), CyberSec First Responder, Information Technology Infrastructure Library (ITIL), or any relevant product certification to the security products of the platform offered by the Service Provider.		
8. The service provider must be at least five (5) years in Security and ICT Industry and must have more than three (3) years of experience in providing SOC services. The Service provider must have a SOC 2 Type II Attestation Report or ISO 27001 certification for		

Managed ICT Services or similar, done at least in 2021, to ensure controls related to security, availability, processing integrity, confidentiality and privacy are in place.		
9. The prospective bidders shall be required during the post qual evaluation to demonstrate the salient features of the proposed Shared Cyber Defense solution at the Project Site or via online.		

D. Personnel Qualifications/Requirements	COMPLIED Y/N	REMARKS
1. The service provider must have at least Two (2) local Certified Engineer on each of the following security tools below: • SOAR • SIEM • Vulnerability Management The certification must be the same with the brand that is being proposed.		
2. The service provider must assign a dedicated local SOC Manager that oversees the SOC and conducts regular monthly service performance review and reporting to client's management. A monthly service performance report shall be submitted and discussed by the SOC Manager. It shall contain the following: • SLA Performance • Correlated Events Overview • Correlated Events Graph Distribution Over Time • Correlated Events and Rules Triggered Summary • Summary of Incident Ticket per Use Cases Incident Management		
3. The service provider must submit the following for all the personnel to be assigned to the cluster, and failure to submit the any of the requirement below is subject for disqualification. • Resume/CV of the Proposed Personnel • Company ID • Certificate of employment		
4. The service provider must have a dedicated 24x7x365 team assigned to the cluster, composed of at least: • 2-Tier 1 analyst who will be responsible for the following tasks: 1. Monitoring via existing SIEM/Analytics Platform 2. Funneling of alerts (noise elimination) 3. Incident Validation 4. Case Management 5. Threat Containment (Using Existing EDR or agreed process) – with guidance from L2 and up 6. General Communication 7. Weekly Summary Reports		

• 1-Tier 2 analyst who will be responsible to conduct further analysis and decides on a strategy for containment. 1. Proactive Searches/ Threat Hunting 2. Qualification of Incident Priority/Severity 3. Investigation via SIEM/Analytics Platform and other accessible sources 4. Rule Tuning 5. Ad hoc Vulnerability Advisory & Research 6. Threat Containment (Using Existing EDR or agreed process) 7. Incident Response/Recommendations • 1-Tier 3 senior analyst who will be responsible to manage critical incidents. Tier 3 analysts are also responsible for actively hunting for threats and assessing the vulnerability of the business. 1. Manage High Severity Triage 2. Incident Response and Forensics Capabilities 3. Threat Containment (Using Existing EDR or agreed process) 4. Reporting and Post Incident Review 5. Use Case Development 6. Threat Searches 7. New Correlation Rules • 1-Tier 4 analyst or the SOC manager, who will be in charge of strategy, priorities and the direct management of SOC staff when major security incidents occur. The SOC manager will also be responsible for the management of the MSOC operations for the agency and cluster.		
5. The service provider should ensure that there will be alternate personnel deployed to the cluster should the primary personnel be unavailable for whatever reason.		
6. Qualifications		
• Project Manager: • Must be with the service provider's organization at least one (1) year before the bid opening • Has handled project management for at least two (2) financial corporations or should have at least two (2) successful project implementations of at least Php 20M in amount in the last two (2) years. • Must provide a list of projects handled in the last 5 years, indicating the Project Name, Project Duration (Start date and end-date) and Contact Person with details for verification. • Must have a valid project management certification • SOC Manager/Tier 4 Analyst: • Must be with the service provider's organization one (1) year before the bid opening		

• Has performed and managed three (3) engagements within the last five (5) years comparable to the proposed engagement • Must have at least five (5) years active IT security experience • Must have at least three (3) years SIEM or system and network administration experience. • Has any two (2) of the following unexpired professional certifications: Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), GIAC Security Essentials (GSEC), GIAC Continuous Monitoring (GMON), GIAC Certified Detection Analyst (GCDA), GIAC Web Application Penetration Tester (GWAPT), GIAC Incident Handler (GCIH), GIAC Certified Forensic Analyst (GCFA), GIAC Certified Intrusion Analyst (GCIA), Cisco Certified Network Associate (CCNA), Information Technology Infrastructure Library (ITIL), Certified Ethical Hacker (CEH), Computer Hacking Forensic Investigator (CHFI), Certified Network Defense Architect (CNDA), CyberSec First Responder (CFR), CompTIA Security+, Certified Vulnerability Assessor (CVA), Offensive Security Certified Professional (OSCP), Certified Information System Security Professional (CISSP), Global Information Assurance Certification (GIAC) Penetration Tester (GPEN), GIAC Exploit Researcher & Advanced Penetration Tester (GXPN), EC-Council Licensed Penetration Tester (LPT) Master, Certified Penetration Tester (CPT), Certified Expert Penetration Tester (CEPT), Certified Mobile and Web Application Penetration Tester (CMWAPT), CompTIA PenTest+, Certified Payment Card Industry Security Implementer (CPISI), or other security-related certifications.		
• Team Lead/Tier 3 Analyst: • Must be with the service provider's organization one (1) year before the bid opening • Has functioned as lead in the performance of three (3) engagements within the last five (5) years comparable to the proposed engagement • Must have at least five (5) years active IT security experience • Must have at least three (3) years SIEM or system and network administration experience • Has any two (2) of the following unexpired professional certifications: CISA, CISM, GSEC, GMON, GCDA, GWAPT, GCIH, GCFA, GCIA, CCNA, ITIL, CEH, CHFI, CNDA, CFR, CompTIA Security+ CVA, OSCP, CISSP, GPEN, GXPN, LPT Master, CPT, CEPT, CMWAPT, CompTIA PenTest+, CPISI, or other security-related certifications.		

• Team Member/Tier 2 or Tier 1 Analyst:
  • Must be with the service provider's organization one (1) year before the bid opening
  • Has performed three (3) engagements within the last five (5) years comparable to the proposed engagement
  • Must have at least three (3) years active IT security experience
  • Must have at least three (3) years SIEM or system and network administration experience
  • Has at least one (1) of the following unexpired professional certifications: CISA, CISM, GSEC, GMON, GCDA, GWAPT, GCIH, GCFA, GCIA, CCNA, ITIL, CEH, CHFI, CNDA, CFR, CompTIA Security+ CVA, OSCP, CISSP, GPEN, GXPN, LPT Master, CPT, CEPT, CMWAPT, CompTIA PenTest+, CPISI, or other security-related certifications.		

4. Delivery Time/Completion Schedule

The Project must be implemented by phases: Phase 1 - Threat Intelligence, Security Monitoring and Management and Incident Response , 120 working days from the issuance of the Notice to Proceed, Phase 2- Vulnerability Management, 90 working days from the issuance of the Notice to Proceed . Commencement date will be from the receipt of Notice To Proceed (NTP) by the winning bidder. The vendor must therefore provide a project schedule which should present the project milestones and deliverables at each milestone. License subscriptions will start upon contract implementation.

All deliverables shall become the property of the concerned agencies**.**

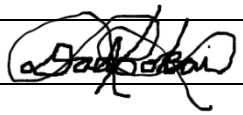
5. Payment Milestone

The Service provider shall be paid upon receipt of its deliverables, based on the submitted Project Schedule and issuance of the Certificate of Acceptance from the Insurance Cluster. The Service Provider shall be paid based on the following milestones:

Milestone	Percentage of the Total Contract Price
Year 1:	
Upon implementation of Threat Intelligence, Security Monitoring & Management, and Incident Response for the Insurance Cluster (Phase 1)	15%
After Phase 1 and upon implementation of Vulnerability Management for the Insurance Cluster (Phase 2)	15%
After Phase 2 and upon full implementation of the Shared Defense Solution and Insurance Cluster issuance of Certificate of Completion and Acceptance of the License subscription covering the first 12 months (1st Year)	20%
Year 2:	
Two (2) semi-annual payments at 25% each	50%
TOTAL	100%

SHARED CYBER DEFENSE SOLUTION Project

Bureau of the Treasury:

NAME	SIGNATURE
Mr. David Andrei P. de Mesa	

Government Service Insurance System:

NAME	SIGNATURE
Mr. Jonathan Pineda	

Social Security System:

NAME	SIGNATURE
Ms. Jocelyn Dela Peña	

Philippine Deposit Insurance Corporation:

NAME	SIGNATURE
Ms. Maria Belinda San Jose	Digitally signed by San Jose Maria Belinda Cusi Date: 2023.08.03 12:11:45 +08'00'