SUPPLEMENTAL/BID BULLETIN NO. 1
For LBP-ICTBAC- ITB-GS-20241129-04

PROJECT: Two (2) Years Shared Cyber Defense Solution for the Government Owned and Controlled Corporation (GOCC) Cluster

DATE: 17 January 2025

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. Response to prospective bidder/s queries/clarifications per attached Annexes F-1 to F-10.

2. Section V. Special Condition of Contract (pages 32-35) Section VI. Schedule of Requirements (page 37) Section VII. Technical Specifications (pages 39-40), Checklist of the Bidding Documents (pages 62-67) and Terms of Reference (Annexes D1 – D37) have been revised. Copies of said revised portions of the Bidding Documents are herein attached.

3. The Bidder/s are reminded that the deadline of Bid Submission and Opening is on 24 January 2025 at 10:00 AM. **Late bids will not be accepted.**

4. The bidder/s is/are encouraged to use the Bid Securing Declaration as Bid Security.

5. The prospective bidders are reminded that only the current/updated Certificate of PhilGEPs Registration (Platinum Membership) shall be accepted during the opening of bids. **Expired Certificate or any of the Eligibility Documents listed in Annex "A" shall be a ground for failure of the bidder** pursuant to the provisions of the 2016 Revised Implementing Rules and Regulations (RIRR) of RA 9184.

   Valid and current Certificate of PhilGEPs Registration (Platinum Membership), in three (3) pages, including Annex "A" or the List of Class "A" Eligibility Documents **required** to be uploaded and maintained current and updated in PhilGEPs in accordance with **Section 8.5.2. of the IRR of RA 9184**.

Sections 23.1(a)(ii) and 24.1(a)(ii) of the 2016 RIRR of RA No. 9184 provides that in case the latest/updated Mayor's Permit is still not available, the prospective bidder **must submit** their **recently expired Mayor's Permit together with the official receipt <u>(OR) to the PhilGEPs</u> as proof** that the prospective bidder has **applied for renewal** within the prescribed period by the concerned local government unit for the purpose of **<u>updating the PhilGEPs Certificate of Registration</u> (Platinum Membership).** The prospective bidder should then **secure/obtain from the PhilGEPs** its **current/updated Certificate of PhilGEPs Registration (Platinum Membership) in three (3) pages, including Annex "A" or the List of Class "A" Eligibility Documents.**

SVP MARILOU L. VILLAFRANCA
Chairperson, ICT-BAC

Special Conditions of Contract

GCC Clause	
1	**Delivery and Documents –** The procurement for Two (2) Years Shared Cyber Defense Solution for the Government-Owned and Controlled Corporation (GOCC) Cluster was acquired through Competitive Bidding with Approved Purchase Order No. ________________ dated ________________, with Notice of Award and Notice to Proceed issued by the authorized signatories of the respective agencies. For purposes of the Contract, "EXW," "FOB," "FCA," "CIF," "CIP," "DDP" and other trade terms used to describe the obligations of the parties shall have the meanings assigned to them by the current edition of INCOTERMS published by the International Chamber of Commerce, Paris. The Delivery terms of this Contract shall be as follows: *For Goods supplied from abroad:* The delivery terms applicable to the Contract are DDP delivered in the address/es indicated in Section VI. Schedule of Requirements. In accordance with INCOTERMS. *For Goods supplied from within the Philippines:* The delivery terms applicable to this Contract are delivered in the address/es indicated in Section VI. Schedule of Requirements. Risk and title will pass from the Supplier to the Procuring Entity upon receipt and final acceptance of the Goods at their final destination. Delivery of the Goods shall be made by the Supplier in accordance with the terms specified in Section VI. Schedule of Requirements. For purposes of this Clause the Procuring Entity's Representative/s at the Project Site/s is/are indicated in Section VI. Schedule of Requirements. **Incidental Services –** The Supplier is required to provide all of the following services, including additional services, if any, specified in Section VI. Schedule of Requirements: a. Performance or supervision of on-site assembly and/or start-up of the supplied Goods; b. Furnishing of tools required for assembly and/or maintenance of the supplied Goods; c. Furnishing of a detailed operations and maintenance manual for each appropriate unit of the supplied Goods; d. Performance or supervision or maintenance and/or repair of the supplied Goods, for a period of time agreed by the parties, provided

that this service shall not relieve the Supplier of any warranty obligations under this Contract; and

e. Training of the Procuring Entity's personnel, at the Supplier's plant and/or on-site, in assembly, start-up, operation, maintenance, and/or repair of the supplied Goods.

The Contract price for the Goods shall include the prices charged by the Supplier for incidental services and shall not exceed the prevailing rates charged to other parties by the Supplier for similar services.

Intellectual Property Rights –

The Supplier shall indemnify the Procuring Entity against all third-party claims of infringement of patent, trademark, or industrial design rights arising from use of the Goods or any part thereof.

2.2 Pursuant to Malacañang Executive Order No. 170 (Re: Adoption of Digital Payments for Government Disbursements and Collections) issued on 12 May 2022, directing all government agencies to utilize safe and efficient digital disbursement in the payment of goods, services and other disbursements, all payments for this Contract shall be through direct credit to the supplier's deposit account with LANDBANK. Thus, the supplier shall maintain a deposit account with any LANDBANK Branch where the proceeds of its billings under this Contract shall be credited.

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

Particulars	Percentage of the Total Contract Price
1st Year:	
Upon Phase 1 implementation and acceptance: • Threat Intelligence • Incident Response	10%
Upon Phase 2 implementation and acceptance: • **Vulnerability Management and Penetration Testing**	10%
Upon Phase 3 implementation and acceptance: • **Security Monitoring Management**	10%
Upon full implementation of the Shared Cyber Defense Solution and Agency acceptance	20%

<table>
<tr><td></td><td><table><tr><td colspan="2"><b>2nd Year:</b></td></tr><tr><td>Four (4) quarterly payments at 12.5% each</td><td>50%</td></tr><tr><td><b>Total</b></td><td><b>100%</b></td></tr></table>
The following documentary requirements for payment shall be submitted:

• Sales Invoice/Billing Statement/Statement of Account on or before the 15th day after every delivery

The Supplier shall be paid within sixty (60) calendar days after submission of sales invoice or claim and complete documentary requirements.</td></tr>
<tr><td>3</td><td>Expiration of performance security should be six (6) months after the last date of delivery/end of contract and issuance of Certificate of Final Acceptance.</td></tr>
<tr><td>4</td><td>Maintain the GCC Clause.</td></tr>
<tr><td>5</td><td>Maintain the GCC Clause.</td></tr>
<tr><td>6</td><td>The Supplier has not made and will not make any offer, promise to pay or authorization of the payment of any money, gift or any other inducement to any official, political party, employee of Government or any other person, in contravention with applicable laws in connection with the execution of this Contract and performance of its obligations thereunder. Violation of this provision shall be a ground for immediate termination of this Contract.

The Supplier shall not assign this Contract or sub-contract the performance of any portion of it, without the Agency's prior written consent. Prior to the assignment or subcontracting and the approval by the Agency thereof, the Supplier must disclose to the Agency the name of its assignee/s or subcontractor/s who/which should have a written agreement/s with the Supplier indicating: (i) that the assignee/s or subcontractor/s is aware of and shall abide with all the terms and conditions of this Agreement, as may be applicable; (ii) that the term of the assignment/sub-contract shall not exceed the term of this Agreement; (iii) the detailed terms of the assignment/sub-contract.

The Supplier shall hold Agency free and harmless from any claims of third parties arising from a negligent or otherwise wrongful act, or omission by the Supplier or its employees or representatives. The Supplier shall ensure that the employees that will be deployed in the Agency's premises shall faithfully observe and comply with all of their respective rules and regulations.

Supplier shall pay taxes in full and on time.</td></tr>
</table>

	Supplier is, likewise, required to regularly present, within the duration of the Contract, a tax clearance from the Bureau of Internal Revenue (BIR) as well as a copy of its income and business tax returns duly stamped and received by the BIR and duly validated with the tax payments made thereon.

Schedule of Requirements

The delivery schedule/contract period expressed as weeks/months/years stipulates hereafter a delivery/performance period which is the period within which to deliver the goods or perform the services in the project site/s.

Description	Quantity	Delivery Period
Two (2) Years Shared Cyber Defense Solution for the Government-Owned and Controlled Corporation (GOCC) Cluster 1) Land Bank of the Philippines 2) Development Bank of the Philippines 3) Home Development Mutual Fund 4) Philippine Guarantee Corporation Phase 1: ▪ Threat Intelligence ▪ Incident Response **Phase 2:** ▪ **Vulnerability Management and Penetration Testing** **Phase 3:** ▪ **Security Monitoring and Management**	 16,000 endpoints 5,000 endpoints 10,500 endpoints 400 endpoints	Two (2) years subscription **to start upon receipt of the Notice to Proceed and acceptance of Phase 1 deliverables** The Project must be implemented by phases, as follows: Phase 1 – within five (5) calendar days Phase 2 – within ten (10) calendar days Phase 3 – within fifteen (15) calendar days The Service Provider must, therefore, provide a Project Schedule, which should present the project milestones and deliverables at each milestone. All deliverables shall become the property of the concerned Agencies.

Conforme:

____
Name of Bidder

____
Signature over Printed Name of
Authorized Representative

____
Position

Technical Specifications

<table>
<tr><th>Specifications</th><th>Statement of Compliance</th></tr>
<tr><td></td><td><b>Bidders must signify their compliance to the Technical Specifications/Terms of Reference by stating below either “Comply” or “Not Comply”</b>
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 applicable laws and issuances.</td></tr>
<tr><td>Two (2) Years Shared Cyber Defense Solution for the Government-Owned and Controlled Corporation (GOCC) Cluster
<table>
<tr><td>1. Land Bank of the Philippines</td><td>16,000 endpoints</td></tr>
<tr><td>2. Development Bank of the Philippines</td><td>5,000 endpoints</td></tr>
<tr><td>3. Home Development Mutual Fund</td><td>10,500 endpoints</td></tr>
<tr><td>4. Philippine Guarantee Corporation</td><td>400 endpoints</td></tr>
</table>
<b><u>Notes</u>:</b>
1. Technical specifications and other requirements per attached <b>revised Terms of Reference (TOR) – Annexes D-1 to D-37</b>.
2. The documentary requirements enumerated in Item C (Service Provider’s Qualification and Requirements) per <b>revised</b> Annexes D-27 to D-32 of the TOR</td><td><b>Please state here either “Comply” or “Not Comply”</b></td></tr>
</table>

shall be submitted in support of the compliance of the Bid to the technical specifications and other requirements. 3. Non-submission of the above requirements may result to post-disqualification of the bidder.	

Conforme:

____
Name of Bidder

____
Signature over Printed Name of
Authorized Representative

____
Position

Checklist of Bidding Documents for Procurement of Goods and Services

The documents for each component should be arranged as per this Checklist. Kindly provide guides or dividers with appropriate labels.

Eligibility and Technical Components (PDF File)

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

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

Legal Eligibility Documents

1. Valid PhilGEPS Registration Certificate (Platinum Membership) (all pages).

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 or Original Special Power of Attorney of all members of the joint venture giving full power and authority to its officer to sign the OSS and do acts to represent the Bidder. (sample form - Form No. 7).

3. 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).

4. Statement of the prospective bidder identifying its Single Largest Completed Contract (SLCC) similar to the contract to be bid within the relevant period as provided in the Bidding Documents. The statement shall include all information required in the sample form (Form No. 4).

Financial Eligibility Documents

5. 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.

6. 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 in lieu of its NFCC computation.

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

7. Duly signed 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.

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

9. Certification from the DTI if the Bidder claims preference as a Domestic Bidder or Domestic Entity.

- **Technical Documents**

10. Bid Security (if in the form of a Surety Bond, submit also a certification issued by the Insurance Commission).

11. ***Revised Section VI – Schedule of Requirements with signature of bidder's authorized representative.***

12. ***Revised Section VII – Technical Specifications with response on compliance and signature of bidder's authorized representative.***

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

Note: During the opening of the first bid envelope (Eligibility and Technical Component), only the above documents will be checked by the BAC if they are all present using a non-discretionary "pass/fail" criterion to determine each bidder's compliance with the documents required to be submitted for eligibility and the technical requirements.

c. **Other Documents to Support Compliance with Technical Specifications [must be submitted inside the first bid envelope (Eligibility and Technical Component)].**

14. Current Certifications from the manufacturer that Service Provider is a certified/authorized reseller of the brands being offered;

15 List of local sales and technical offices in the Philippines;

16. Valid SOC 2 Type II Attestation Report or ISO27001 Certification;

17. Valid Certificate of Registration issued by the National Privacy Commission;

18. Report on the conduct of Business Continuity Plan (BCP) testing;

19. Documentary requirements for at least two (2) local Certified Security Engineer for each proposed solution:
    a. Certificate of Employment
    b. Resume or Curriculum Vitae
    c. Certification/s of the assigned engineer/personnel

20. Documentary requirements for the dedicated 24x7x365 team within the Security Operations Center (SOC) that will be assigned to the GOCC Cluster, which shall be composed of the following:

    a. **Six (6) Tier 1 SOC Analyst:**
    - Certificate of Employment
    - Resume or Curriculum Vitae
    - At least one (1) valid Professional Certification/s from any of the following: CISA, CISM, GSEC, GMON, GCDA, GWAPT, GCIH, GCFA, GCIA, CCNA, CEH, CHFI, CNDA, CFR, CompTIA Security+CVA, OSCP, GPEN, GXPN, LPT Master, CPT, CEPT, CMWAPT, CompTIA PenTest+, CPISI, or other security-related certifications

    b. **Three (3) Tier 2 SOC Analyst:**
    - Certificate of Employment
    - Resume or Curriculum Vitae
    - At least two (2) valid Professional Certification/s from any of the following: CISA, CISM, GSEC, GMON, GCDA, GWAPT, GCIH, GCFA, GCIA, CCNA, CEH, CHFI, CNDA, CFR, CompTIA Security+CVA, OSCP, GPEN, GXPN, LPT Master, CPT, CEPT, CMWAPT, CompTIA PeTest+, CPISI, or other security-related certifications

    c. **One (1) Tier 3 SOC Analyst:**
    - Certificate of Employment
    - Resume or Curriculum Vitae

- At least two (2) valid Cybersecurity Professional Certification/s from any of the following: CISA, CISM, GSEC, GMON, GCDA, GWAPT, GCIH, GCFA, GCIA, CCNA, CEH, CHFI, CNDA, CFR, CompTIA Security+CVA, OSCP, CISSP, GPEN, GXPN, LPT Master, CPT, CEPT, CMWAPT, CompTIA PenTest+, CPISI, or other security-related certifications

d. **<u>One (1) SOC Manager:</u>**

- Certificate of Employment
- Resume or Curriculum Vitae
- At least three (3) valid Cybersecurity Professional Certification/s from any of the following: CISA, GSEC, GMON, GCDA, GWAPT, GCIH, GCFA, GCIA, CCNA, CEH, CHFI, CNDA, CFR, CVA, OSCP, CISSP, GIAC, GPEN, GXPN, LPT Master, CPT, CEPT, CMWAPT, CompTIA PenTest+, and CPISI

e. **<u>Two (2) Local Digital Forensics and Incident Response Analyst:</u>**

- Certificate of Employment
- Resume or Curriculum Vitae
- At least two (2) valid Professional Certification/s from any of the following: CISA, CISM, GSEC, GMON, GCDA, GWAPT, GCIH, EC Council Incident Handler, GCFA, GCIA, CCNA, CEH, CHFI, CNDA, CFR, CompTIA Security+CVA, OSCP, CISSP, GPEN, GXPN, LPT Master, CPT, CEPT, CMWAPT, CompTIA PenTest+, CPISI, or other security-related certifications

f. **<u>Two (2) Local Senior Threat Intelligence and Threat Hunting:</u>**

- Certificate of Employment
- Resume or Curriculum Vitae
- At least two (2) valid Cybersecurity Professional Certification/s from any of the following: CISA, CISM, GSEC, GMON, GCDA, GWAPT, GCIH, EC Council Threat Intelligence Analyst, 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

g. **<u>Two (2) Local Vulnerability Assessment and Penetration Tester:</u>**

- Certificate of Employment
- Resume or Curriculum Vitae
- At least two (2) valid Cybersecurity Professional Certification/s from any of the following: 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

h. **At least Twenty (20) Onsite Technology Support Engineers within Metro Manila:**
   - Certificate of Employment
   - Resume or Curriculum Vitae
   - At least one (1) security-related Technical Certification in the following: Networking or Network Security such as Network Devices (Network Associate and/or Professional), Firewalls, Intrusion Prevention Systems, Application Delivery Controllers Administration, Email Security, Web Security, and Server and/or Systems Administration, Directory Services

21. Documentary Requirements for One (1) **Project Manager**:
    - Certificate of Employment
    - Resume or Curriculum Vitae
    - Project Management Professional (PMP) Certification

22. Documentary Requirements for One (1) **Service Delivery and Escalation Manager**:
    - Certificate of Employment
    - Resume or Curriculum Vitae
    - IT Infrastructure Library (ITIL) Certification

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

1. 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.

2. Latest Income Tax Return filed manually or through EFPS.

3. Original copy of Bid Security (if in the form of a Surety Bond, submit also a certification issued by the Insurance Commission).

4. Original copy of duly notarized Omnibus Sworn Statement (OSS) (sample form - Form No.6).

5. Duly notarized Secretary's Certificate designating the authorized signatory in the Contract Agreement if the same is other than the bidder's authorized signatory in the bidding (sample form – Form No. 7).

Financial Component (PDF File)

- **The Financial Component shall contain 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).

***Note:** The forms attached to the Bidding Documents may be reproduced or reformatted provided the information required in the original forms and other requirements like signatures, if applicable, are complied with in the submittal.*

SHARED CYBERDEFENSE SOLUTION

Terms of Reference (GFI Cluster)

Version Number	:	1.0
Final as of	:	14 January 2025
Author	:	Land Bank of the Philippines Development Bank of the Philippines Philippine Guarantee Corporation Home Development Mutual Fund

Revised D-1

1. Name and Description of the Project

With the continued evolving nature of cybersecurity risks, the Secretary of Finance has mandated the Government Financial Institutions (GFIs) and other Agencies under the Department of Finance to establish a cost-effective defense strategy that will shield their respective IT systems from potential cybersecurity threats, along with other possible risks and data breaches in the digital landscape.

This initiative involves the two (2) segmented groups, the GFI and Insurance Clusters, under the Department of Finance (DOF).

For this Terms of Reference (TOR), it will cover the GFI Cluster composed of Land Bank of the Philippines (LBP), Development Bank of the Philippines (DBP), Home Development Mutual Fund (HDMF), and Philippine Guarantee Corporation (PhilGuarantee).

2. Project Objective and Scope

The proposed Shared Cyber Defense Solution shall require the services of a service provider for two (2) years for the conduct 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 of endpoints for each agency (i.e., LBP – 16,000, DBP – 5,000, HDMF – 10,500, and PhilGuarantee – 400) and includes project management, consulting, requirements validation, customization, training, integration, production deployment, system integration, change management and other out-of-pocket expenses (e.g., transportation allowance, per diem, etc.);

- 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)

Other Requirements

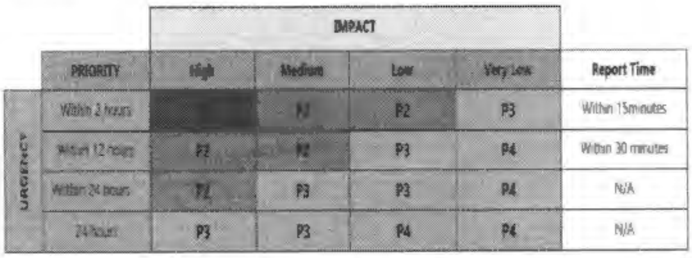
During procurement, the bidder is required to submit respective proposals for all the agencies concerned.

3. Functional and Non-Functional Requirements

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

Revised D-2

I. Functional Requirements

<table>
<tr><th>Item</th><th>Description</th><th>Complied</th><th>Remarks</th></tr>
<tr><td colspan="4"><b>A. Security Monitoring and Management</b></td></tr>
<tr><td colspan="4"><b>A.1 Security Operations Center (SOC)</b></td></tr>
<tr><td>1</td><td>The SOC 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 SOC platform provisioned for the agencies.</td><td></td><td></td></tr>
<tr><td>2</td><td>The Security Operations Center must be based in the Philippines and must not be operating in the "follow the sun" model where security analyst and support teams are distributed across multiple global locations, each covering specific time zone.</td><td></td><td></td></tr>
<tr><td>3</td><td>The service provider should have a 24 x 7 x 365 SOC with local analysts and technical support for both tools and services.</td><td></td><td></td></tr>
<tr><td>4</td><td>The service provider shall provide a 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.</td><td></td><td></td></tr>
<tr><td>5</td><td>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.</td><td></td><td></td></tr>
<tr><td>6</td><td>The solution shall have its own ticketing tool for incident ticket escalation and management</td><td></td><td></td></tr>
<tr><td>7</td><td>The SOC 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:

<table>
<tr><th></th><th></th><th colspan="4">IMPACT</th><th></th></tr>
<tr><th></th><th>PRIORITY</th><th>High</th><th>Medium</th><th>Low</th><th>Very Low</th><th>Report Time</th></tr>
<tr><td>URGENCY</td><td>Within 2 hours</td><td>[illegible]</td><td>P1</td><td>P2</td><td>P3</td><td>Within 15minutes</td></tr>
<tr><td></td><td>Within 12 hours</td><td>P2</td><td>P2</td><td>P3</td><td>P4</td><td>Within 30 minutes</td></tr>
<tr><td></td><td>Within 24 hours</td><td>P2</td><td>P3</td><td>P3</td><td>P4</td><td>N/A</td></tr>
<tr><td></td><td>24 hours</td><td>P3</td><td>P3</td><td>P4</td><td>P4</td><td>N/A</td></tr>
</table>
<ul>
<li>Impact: Severity of the security event to critical assets</li>
<li>Urgency: How soon the security incident must be addressed</li>
<li>Priority: Based on the impact and severity</li>
<li>Nature of threat</li>
<li>Potential business impact</li>
<li>Remediation recommendations</li>
</ul></td><td></td><td></td></tr>
<tr><td>8</td><td>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</td><td></td><td></td></tr>
</table>

	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 • Time to Detect • Time to Engage/Respond		
9	The service provider shall conduct SOC security briefings as part of the monthly monitoring and service management review to provide the latest local and international news and updates in cybersecurity.		
10	The service provider must be able to utilize and support the agency's existing on-premises Security Information and Event Management (SIEM) platform or migrate the logs generated by the agency over the past 12 months if the service provider proposes a new SIEM platform.		
A.2 Managed Detection and Response			
A.2.1 Deployment and Management			
11	The solution is capable to deploy endpoint technology to supported versions of Windows, Mac, and Linux assets. The solution must be able to works in a Virtual Desktop Infrastructure (VDI) environment.		
12	The solution must have defined playbooks when engaging and responding to threats		
13	The solution must have the feature to automatically redirect admin to Hybrid Analysis, VirusTotal or Google with a single click from the console, to retrieve further information on the detected file hash		
14	Solution must have Machine Learning detection and prevention capabilities for Windows, MacOS, and Linux platforms.		
15	Endpoint agent must continuously capture raw events (process, file system, registry, network activities, memory, OS events), even when not associated with alerts and detections		
16	The solution must not rely on detection or correlation rules to be written before the product can detect incidents. The solution must have advanced machine learning and behavioral analysis to detect threats, so they can identify threat even without pre-defined rules.		
17	The solution must be able to automatically decode encoded command line arguments		
18	Solution must automatically correlate and present telemetry and metadata (IOC) related to the attack in a timeline. Such as, command line arguments, file writes, DNS requests, IP connections, etc.		
19	Solution must correlate, where possible, the infection vector and threat attackers intention in relation to the attack chain by correlating to telemetry, process tree and threat intelligence.		
20	The solution shall support Endpoint Detection and Response (EDR) functionality on Windows, Linux, and Mac Operating System (OS).		
21	The solution shall not require reboot during installation, enabling, and updating of Endpoint Protection, EDR or any malware prevention modules.		
22	The solution shall utilize Central Processing Unit (CPU) (1-2%), ~100-150 MB of Random Access Memory (RAM) and fixed disk at low levels.		
23	The solution shall support IT Hygiene and must not require additional sensors to be installed or need to deploy additional agents.		
24	All modules within the solution shall not be dependent on any whitelisting, which includes Endpoint Protection, EDR and IT Hygiene.		

25	The solution must be able to identify assets, identities and configurations accurately across all systems including cloud, on-premises, and connecting them together in a graph form		
26	The solution must provide capabilities for pushing files to remote systems, executing files, running scripts, killing processes, adjusting registry keys and other tasks required during incident response		
27	EDR events should be enriched and correlated with service provider's own Threat Intelligence and not using any third-party Indicator of Compromise (IOC). Also, the solution should be one of the leaders in analyst Threat Intelligence reports.		
28	The solution shall have support for Desktop Firewall Management.		
29	The solution shall have support for Universal Serial Box (USB) device control policies.		
30	Solution must have the following Agent reports pre-configured in the console: • Agent Overview report • Agent Daily Policy report • Newly Installed Agent report • Inactive Agents report • Agent Coverage Lookup report • SHA256 Signature Support report • Agent Health report		
31	Solution must have the following Visibility reports pre-configured in the console: • Remote Access Graph report • Remote or Network Access Logon Activities report • Unique Hosts Connecting to Countries Map report		
32	Solution must have the following Audit reports pre-configured in the console: • Machine Learning Prevention Monitoring • Console UI Audit Trail • API Audit Trail • Prevention Policy Audit Trail • Prevention Policy Debug • Prevention Hashes Ignored • Agent Visibility Exclusions Audit		
33	The solution must include a dedicated Zero Trust Assessment dashboard that monitors OS settings and sensor settings of hosts within the organization. This granular assessment of eligible hosts is used to produce a score that uniquely represents the security posture of each host.		
34	The platform must include additional subscription of managed detection and response service from the proposed Endpoint Detection and Response (EDR) platform. This subscription shall augment the services provided by the service provider.		
35	The Managed Detection and Response platform must maintain and update the management platform, including enforcing best practices of prevention policies.		
A.2.2 Detection			
36	Solution must provide the following Execution details for each detection in		

	the console where applicable: • Detect Time • Hostname • Username • Severity • Objective • Tactic & Technique (MITRE ATT&CK Framework mapping) • Detection Explanation • Triggering Indicators • IOC Global & Local Prevalence • Associated File & File Path • Hash Prevention Action		
37	The solution must be able to View the following: • alerts centrally in the UI • alert's associated activity in the UI • interactive process trees for alerts detections • Process tree events coming into UI in a near real time for the detected events • System, user, and per process real-time forensics of an alert • full execution details including paths, hashes, timestamps, and command lines • disk I/O activity of processes including reads and writes • network connectivity of processes • DNS Lookups that are captured for each process and not per client		
38	The solution must be able to generate an intelligence driven detection in the UI.		
39	The solution must be able to enrich a detected event with its own threat intelligence and not any third-party Intelligence.		
40	The Threat Intelligence service as part of the MDR shall be a leading threat intelligence in any of the third-party analyst report.		
41	Should be a tested solution by MITRE against its ATT@CK Framework		
42	Should be able to associate detected events using the MITRE ATT@CK Framework Tactic & Technique		
43	Should be able to manage workflows including sorting, filtering, tracking status, assigning ownership, and creating commentary or annotations of alerts		
44	The solution must detect common credential theft techniques		
45	Should be able to detect attacks using file-less and malware-less tools such as PowerShell		
46	The solution must include a dedicated Zero Trust Assessment dashboard that monitors OS settings and sensor settings of hosts within the organization. This granular assessment of eligible hosts is used to produce a score that uniquely represents the security posture of each host.		
47	For non-supported systems, other means of monitoring must be performed, such as network detection and response (NDR or similar) tool shall be provided. On-prem appliance must have the following capabilities: • Must utilize cloud-scale machine learning and AI to detect advanced threats • Must provide detection for at least 126 MITRE ATT&CK Techniques • Must decode over 80 network protocols to generate metrics and metadata for threat detection • Must have 1 dedicated network capture port, and 1 network management port • Must have 88GB of capacity for datastore		

	• Must be capable of 1 Gbps continuous traffic analysis and includes capabilities for L2-L7 analysis. Has onboard packet capture storage SSD. Includes 20GB of daily record ingest		
A.2.3 Prevention			
48	The solution must be a Next-Generation Endpoint Protection Platform that uses Machine Learning for pre-execution prevention for both known and unknown malware. The solution must not rely on signatures or hash-lookups for malware prevention		
49	The solution must be able to perform preventative controls while both online and offline.		
50	The solution must not require daily updates or DAT files to keep protection at its highest level.		
51	The solution must be able to submit quarantine files to sandbox for automatic analysis using both advanced static and dynamic analysis.		
52	Solution must be able to detect or prevent Volume Shadow Copy activities. Provide evidence of setting from the endpoint policy.		
53	Solution must provide post-execution behavior based detection and prevention based on Indicator of Attack (IOA) mapped against the MITRE ATT&CK framework		
54	Solution must provide the ability to create custom Indicator of Attack (IOA) profiles based on behavior-based threats.		
55	The solution must provide the ability to convert detections to a prevention, including behavior based detections		
56	Solution must provide post-execution behavioural analysis to protect against common ransomware activities (encrypting files, deleting shadow files, etc)		
57	The endpoint security solution should support Firmware Analysis to detect BIOS level attacks.		
58	The Solution must be able to prevent malicious usage of PowerShell and scripted attacks		
A.2.4 Threat Hunting			
59	Must have a 24X7 Managed Threat Hunting Service		
60	Solution must continuously monitor endpoint activities and captures events and forensic details of interest in near real time		
61	Solution must provide predefined queries for all user and endpoint related activities		
62	Must be able to pivot to Events from results retrieved from the pre-built hunting application for additional raw data		
63	Must be able to search for a MD5 or SHA256 file hash to show historical data about its execution		
64	The solution must include fully customizable real-time and historical search capabilities (e.g. data stacking) with no impact on the endpoints while searching		
65	The solution must provide report to demonstrate full timeline of events occurring on a host		
66	Solution must provide predefined queries for forensic artefacts (e.g. hash, domain, raw events, registry keys)		
67	The solution must have the following Hunting reports pre-configured in the console: • Command Line and ASEP Activity from Network-capable Processes report • Executables Running from Recycle Bin report • Executables Running from Temporary Directories report • Files Written to Removable Media report		

	• Firewall Set Rules report • Powershell Hunt report • Scheduled Tasks Registered report		
68	Must be able to hunt events for an offline machine in near real time before it went offline		
69	Solution must be able to have retrospective search capabilities.		
70	Solution must be able to show lateral movement incident data in the console in the form of an interactive graphical format.		
71	Solution must provide report to demonstrate full timeline of events for a process and on a host in the form of an interactive detection tree.		
72	The solution should include Managed Threat Hunting Service which shall be provided by the proposed EDR solution/ vendor itself and not from any 3rd Party Services		
73	The MDR solution must have been in the industry for at least 5 years		
74	The MDR Service of the proposed solution should have experience with their own MDR offering for more than five (5) years		
75	The solution should be supported and augmented by experienced and certified Incident Responders from the service provider to perform 24X7 remote response for Endpoint Incidents/Events		
76	The solution must be supported and augmented by the service provider's local Threat Intelligence Team		
A.2.5 Response			
77	Solution must provide capabilities for pushing files to remote systems, executing files, running scripts, killing processes, adjusting registry keys and other tasks required during incident response		
78	Connection to remote host should be supported for Windows, Mac, and Linux		
79	Must be able to network contain a host (Windows, Mac and Linux) directly from a detection window		
80	Must be able to show all endpoints that are currently in a network contained state		
81	Must be able to remotely contain an endpoint using mechanisms not related to the operating system firewall. Containment must persist after a reboot.		
82	Must be able to view the amount of time required to network contain and lift containment		
83	Must be able to manage whitelisted IP addresses for network containment		
84	Solution must provide for custom file hash whitelisting and blacklisting		
85	Must be able to view and preserve containment and blacklists across reboots		
86	Must be able to view containment action audit logs		
87	Should support execution of custom Powershell Scripts as a part of remote response action		
A.2.6 API and Platform Integration			
88	The solution must support API-to-API capabilities to enhance both the platform and partner applications, security solutions/tools, including Cloud, CI/CD, and DevSecOps Software Development Toolkits (SDKs).		
A.2.7 Compromise Assessment			
89	The solution provider must perform an annual compromise assessment to assess the agency's assets, including third party applications (if applicable) to determine whether a compromise has occurred, measure the extent of breaches, and review existing security controls and vulnerabilities.		
90	The solution provider must provide the following reports such as but not limited to: • A thorough report detailing the results of the assessment • Recommendations for remediations and improvement • Agency-specific executive summary		

A.2. 8 Third Party Validation			
91	The solution should be leader in the latest Gartner's Magic Quadrant for Endpoint Protection Platform		
92	The solution must be positioned as a MDR Leader in the industry analyst reports and must be positioned as a Leader in the latest Forrester Wave for the following categories: • Endpoint Security Software as a Service • Endpoint Detection and Response • Managed Detect & Response		
93	The Solution must regularly participate in independent AV tests to prove effectiveness and efficiency, such as AV-Comparatives, SE Labs, etc.		
94	The solution must have received an "AAA" score from SE Labs for the Breach Response Test - Detection Mode and Breach Response Test - Protection Mode.		
95	The solution must be a registered member of Anti-Malware Testing Standards Organization (AMTSO)		
96	The solution must have participated in non-sponsored public testing, such as MITRE ATTACK.		
A.3 Security Information and Event Management (SIEM)			
97	The solution shall be designed and set-up through a secured connection, a log collection platform or similar to enable transfer of monitored logs to the service provider		
98	The service provider 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.		
99	The service provider shall ensure the availability of searchable raw logs, including agency's logs for the previous twelve (12) months with comprehensive search functionality. The logs shall be retained for the contract period, after which they will be archived and provided to the agencies in an agreed format. The logs, including evidence of security incidents, should be tamper-proof and made available for legal and regulatory purposes as required. All logs must be stored in a purpose-built secured log management system of the proposed solution.		
100	The service provider's SIEM shall provide for flexibility and scalability for the agencies' current and future needs		
101	The SIEM solution must be able to store events and flows, keeping all information available for immediate ad hoc queries, while retaining data long term for forensics, rules validation, and compliance.		
102	The SIEM solution must be able to retain logs in their original format for as long as it needs to support the specific compliance needs of the agencies.		
103	The SIEM solution must be able to provide context about each and every log, making every parsed log record more valuable. Information included shall be: • The source or destination IP address • Identity context • The hostname or service being used • Network topological information • Policy and privacy information		
104	The SIEM solution must be able to monitor and analyze data from a broad heterogeneous security infrastructure and offers two-way integration via		

	open interfaces.		
105	The SIEM solution must be able to collect security event and network flow data from hundreds of third-party sources such as but not limited to: • firewalls • VPN • switches • routers • authentication systems • servers		
106	The SIEM solution must have a global threat intelligence subscription service to quickly identify attack paths and past interactions with known bad actors and increase threat detection accuracy while reducing response time.		
107	The SIEM solution must be able to ingest threat information reported via Structured Threat Information eXpression (STIX)/Trusted Automated eXchange of Indicator Information (TAXII) and/or third-party web URLs and take action based on analysis.		
108	The SIEM solution must allow administrator to check new attacks and vulnerabilities against history to detect past events		
109	The SIEM Manager must provide its own native database for both real time and historical data, thus eliminating any third-party dependencies and time-consuming DB administration		
110	The SIEM Manager must support adaptive baselining of incident patterns that constitute normal behavior and must highlight and alert where incidents exceed these observed base- lines for any given time window. This includes attacker, target, ports, protocols and session data and others		
111	The SIEM solution must support the Unified Compliance Framework (UCF), which associates over 240 regulations to a common set of control with no additional cost		
112	The SIEM solution must be able to do Risk-base and Rule-base correlation		
113	The SIEM solution must have an advanced correlation engine solution that can be deployed in either real time or historical modes.		
114	The SIEM solution must have predefined set of correlation rules - out-of-the-box set of correlation rules to detect "classical" attacks (scans, worm crawling, brute force attacks, DDoS, trojans, port abuse etc..)		
115	The SIEM solution must have content packs that are prebuilt configurations for common security use cases that provide sets of rules, alarms, views, reports, variables, and watchlists.		
116	The SIEM solution must have both customizable and prebuilt dashboards, comprehensive audit trails, and reports for more than 240 global regulations and control frameworks, including PCI-DSS, HIPAA, NERC-CIP, FISMA, GLBA, GPG13, JSOX, and SOX.		
117	The SIEM Manager must provide an intuitive and easy to learn graphical interface for building of custom correlation rules		
118	The SIEM solution must provide means to create reports based on collected and correlated data.		
119	The SIEM solution must provide an intuitive reporting interface that can leverage existing reports or the creation of new reports that does not require complex SQL queries		
120	The SIEM reports must be exported to PDF, MS Excel/CSV file and HTML		
121	The SIEM solution must have prebuilt report templates, such as but not limited to: • PCI DSS • ISO 27002		

	• FISMA • HIPAA • SOX • GLBA • BASEL II • EU 8th • GIODO • NERC • KPI • SLA • Vulnerability		
122	The SIEM solution must have executive report templates - existing templates for executive- level reports (Incident per severity, top threats, compliance levels, trends, major issues etc.)		
123	The service provider shall ensure the availability of searchable the ingested raw logs for at least twelve (12) months with comprehensive searchability.		
124	The solution shall be able to identify, interpret, and parse customized or proprietary logs of the agencies without additional cost.		
125	The solution must be capable to automatically generate predefined or customized reports, and send them to an email address.		
A.4 Security Orchestration, Automation and Response (SOAR)			
126	The SOAR solution must be a stand-alone platform that can be integrated with the SIEM and fully orchestrate security operations and provide security teams with case management, automation, and investigation within a single pane of glass		
127	The SOAR solution must have visibility into the security operation provided via dashboards, KPIs and customizable reporting		
128	The SOAR solution must provide a graph representation, based on a unique cyber ontology, to bring a full set of threat management capabilities that utilize true real-time alerts		
129	The SOAR solution must render alerts, cases, query reports, and events into clustered and contextualized threat storylines with a high degree of visualization		
130	The SOAR 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.		
131	The SOAR solution must be able to provide plugins for non-technology partners		
132	The SOAR solution must be able to identify significant cases, clustering them with related threat indicators to prioritize a threat.		
133	The SOAR solution must have access right mechanisms		
134	The SOAR solution must be able to support enterprise case management capabilities including SLA, case permissions, user roles, auditing, comments, logging, artifact upload, filtering, escalation, shift change, one-click reporting and more		
135	The SOAR solution must have collaboration functionalities in the platform		
136	The SOAR solution must have some Machine learning recommendation capabilities		
137	The SOAR solution must be able to integrate with other security tools for faster root cause analysis, rapidly pivoting from threat detection to response and mitigation		
138	The SOAR solution must be able to query objects in real-time, drill-down for additional detail, and perform mitigation and remediation actions in a click of a button		

139	The SOAR solution must be able to accelerate all processes by automating or semi automating workflows		
140	The SOAR solution must be able to build custom playbook by intuitively dragging and dropping actions, triggers and logical operators.		
141	The SOAR solution must be able to develop playbooks of best practices to scale operations, drive consistency in response and meet compliance requirements. • Brute force attempt • DNS Reconnaissance • DOS/DDOS: DoS/DDoS attacks 10,000 in 15 minutes • Anti-virus failed to clean or quarantine • Email with Malicious attachment • Database connections: unsuccessful connection attempts. • Device out of compliance (antivirus, patching, etc.). • Excessive SMTP traffic outbound • Excessive traffic inbound (streaming, web, etc.). • Excessive port blocking attempts from anti-virus or other monitoring systems • Excessive scan timeouts from anti-virus • Known Exploit Payload detected • Malicious Website • Logs deleted from source • Suspicious traffic to known vulnerable host • Unauthorized subnet access to confidential data • Port Scan IPS from External to Internal • Ransomware Infection • Sinkhole Attack • System Compromise: CnC communication • System Compromise: Suspicious Behavior • Waterhole attack • IRC Connections proceeded by Server Initiated Connection to Dynamic Hosts • Login to sleeping account: Login attempt to account that was unused for last xx days • Admin Login Fail: Admin 3 Failed logins to any system within 24 hours • Freq. Account Locked: Frequent account locked 3 in 7 days [3/7d] • Login 1 to many: Login attempt from 1 station to more than 2 accounts • Login at off hours Night: Admin login in non-working hours (customizable) • Login more than 2 to 1: Login attempt from 3 stations to 1 account • Login Root: Login Directly to Root and not via "SU" • Malware Infections • Multiple Account Locking: Multiple locked accounts from same source IP • Multiple changes from administrative accounts • Same account different countries within 5 days (user traveled abroad) • SMTP traffic from an unauthorized host. • Privilege Elevation: Permissions were changes from user to Admin • Threat Intel Feed: IOCs detection		

	• Trojan Infection • Virus Found • Vulnerable Software Version Detected		
142	The SOAR solution must be able to provide the needed business intelligence capabilities to present current workload, capacity, and effectiveness of security operations.		
143	The SOAR solution must be highly flexible, providing customizable dashboards that highlight most relevant insights for on-going improvement.		
144	The SOAR solution should provide pre-set (and customizable) KPI metrics to monitor threat response efficacy and team performance.		
145	The SOAR solution should provide integrated BI platform to help create advanced dashboards and reports based on KPI's to be tracked		
146	The SOAR solution must have presentable dashboards with customization, reporting, scheduling and report distribution capabilities.		
147	The SOAR solution must provide built-in reports provide executive level and detailed technical reporting out of the box		
148	The SOAR solution must be able to provide customizable reports at the click of a button for any event or case.		
149	The SOAR solution must be able to automate the reporting process to routinely deliver standard and customized reports		
150	The SOAR solution must be able to cater to the demands of different audiences within the organization with powerful templating engine.		
B. Vulnerability Management and Penetration Testing			
B.1 Vulnerability Management			
151	The solution must be a cloud-based offering but supports on-premise scanners		
152	The solution must fully integrate vulnerability assessment (scanning) and security configuration assessment to include combined licensing and consolidation of data, analysis, and querying		
153	The solution must include an integrated active/passive scanning capability for full visibility of assets, vulnerabilities, and configurations.		
154	The solution must offer predictive prioritization of remediation based on business risk.		
155	The solution must enable organizations to effectively measure their Cyber Exposure and benchmark their performance internally against different groups as well as externally against industry peers.		
156	The solution's offering must include 24/7/365 global technical support.		
157	The solution must receive new vulnerability detections/checks and does not rely on 3rd party data set		
158	The solution must not rely on IP Addresses as the only means to track an asset.		
159	The solution must be able to resolve multiple IPs to a single asset, for assets that have multiple IPs at one time or over time.		
160	The solution must provide an elastic licensing model to ensure the product continues to function without interruption when the license limit is temporarily exceeded.		
161	The solution must provide an integrated storage model that does not rely on a third-party database product.		
162	The solution must provide comprehensive public cloud security which includes continuous visibility and assessment and benchmarking in Amazon Web Services, Microsoft Azure, Google and other cloud platforms.		
163	The solution must be able to monitor network traffic continuously to detect and assess short-lived systems and hard-to-scan devices, such as sensitive OT and IoT systems.		

164	The solution must provide a comprehensive and fully-documented API for automation of processes and integration with 3rd party applications.		
165	The solution must scale to millions of assets.		
166	The solution must include the option for agents that provide vulnerability assessment and security configuration assessment.		
167	The solution must be able to use groups of scanners in a single job.		
168	The solution must be able to scan assets on customers' internal networks as well as assets which are external facing / publicly accessible.		
169	Scanners must be managed by the platform, e.g. updates to vulnerability detections, code and other updates.		
170	The solution must provide role-based access control (RBAC) to control user access to specific data sets and functionality.		
171	The solution must have the ability to ensure that certain IPs or ports can be blocked from scanning.		
172	The solution must provide the ability to accept or modify risk for vulnerabilities, with such functionality restricted by user role and any vulnerability risk acceptance documented.		
173	The solution must be able to define and manage user groups, including limiting scan functions and report access.		
174	The solution must support a variety of scan engine platforms to include Windows, Linux, macOS, as well as virtual-based appliances.		
175	The solution must support multiple geographically distributed scanning engines managed by a central console.		
176	The solution must include the ability to schedule scan blackout windows to prevent scanning during prohibited hours.		
177	The solution must provide the ability to configure ports, protocols, and services for connections to scanners deployed throughout the network.		
178	The solution must be configurable to allow for scan throttling to prevent generation of traffic that could disrupt normal network infrastructure.		
179	The solution must allow for entry and secure storage of user credentials, including Windows local and domain accounts.		
180	The solution must provide the ability to escalate privileges on target systems from normal user access to root/administrative access.		
181	The solution must support customized scan scheduling, including the ability to have scans run at designated times, with predetermined frequency.		
182	The solution must be able to perform sensitive data searches to discover sensitive data at rest on *applicable and currently used operating system versions* of Windows, and Linux systems.		
183	The solution must be able to offer centralized scan and scan policy management.		
184	The solution must provide for an "auto-aging" license model to ensure stale or retired assets no longer count against the license.		
185	The solution must support an asset discovery capability that does not count against licensing. The solution must provide a passive network monitoring capability for asset discovery.		
186	The solution must support the ability to gain near real-time visibility and inventory of public cloud assets as cloud instances are turned on or decommissioned.		
187	The solution must be able to discover mobile devices and integrate with several different Mobile Device Management Systems (MDMs).		
188	The solution must provide integrated web and database service discovery.		
189	The solution must be capable of detecting services that are running on non-standard ports.		

190	The solution must be capable of detecting services configured not to display connection banners.		
191	The solution must be capable of testing multiple instances of the same service running on different ports.		
192	The solution must be capable of scanning dead hosts (devices which do not respond to ping).		
193	The solution must support the optional use of netstat for rapid and accurate enumeration of open ports on a system when credentials are supplied.		
194	The solution must support the use of SMB and WMI for scanning Windows systems.		
195	The solution must be capable of automatically starting remote registry services on Windows systems when performing a credentialed scan, then automatically stopping the service again once the scan is complete.		
196	The solution must provide the ability to tune scan policies for minimal impact on networks and targets.		
197	The solution must provide active and passive discovery of wireless access points (WAPs).		
198	The solution must provide both authenticated and non-authenticated network-based scanning of target systems.		
199	The solution must not rely on any third-party scanners for vulnerability scanning, compliance auditing / security configuration assessment.		
200	The solution must be capable of agentless testing for both local (authenticated) and remote (non-authenticated) vulnerability detection without the need for a client-side agent installed on the target device.		
201	The solution must be capable of agent testing for local vulnerability detection at no additional charge.		
202	The solution must provide an externally-hosted scanning service for scanning perimeter networks.		
203	The solution must be capable of tracking DHCP changes by associating scan results of a given system with something other than the IP address.		
204	The solution must detect and rank issues, risks, and vulnerabilities. It must also provide detailed information regarding the nature of the risk and recommendations to mitigate it.		
205	The solution must be CVE compatible and provide at least 10 years of CVE coverage.		
206	The solution must provide coverage for third-party applications such as Java and Adobe.		
207	The solution must provide integration with patch management systems for patch auditing and delta reporting against scan findings such as Microsoft WSUS/SCCM, Red Hat Satellite, IBM Tivoli Endpoint Manager (formerly BigFix), Symantec Altiris, an Ques/Dell KACE.		
208	The solution must provide integration with Mobile Device Management (MDM) products, such as VMware AirWatch, Apple Profile Manager, BlackBerry UEM, Good MDM, Microsoft Intune, IBM MaaS360 and MobileIron, among others, for mobile device discovery and auditing.		
209	The solution must provide predictive vulnerability prioritization that uses real-time threat intelligence and machine learning algorithms to score vulnerabilities and predict which ones are most likely to be exploited in the near future.		
210	The solution must provide vulnerability prioritization context that helps users understand the key factors influencing each vulnerability score (e.g., threat recency, exploit code maturity, intel source categories).		

211	The solution must also include vulnerability scoring according to the Common Vulnerability Scoring System Version 3 (CVSS v3).		
212	The solution must provide information about existence of exploit kits for a given vulnerability, including a summary of vulnerabilities that are exploitable by malware and affected assets.		
213	The solution must intelligently select vulnerability and configuration tests for a given asset based on information gained from initial scans of that asset.		
214	The solution must track dates for vulnerability discovery and observation that can be used in filtering and reporting in time-based filters.		
215	The solution must not be dependent on operating system ability to schedule tasks.		
216	The solution must support IPv6 scanning, with passive discovery of IPv6 targets		
217	The solution must assess public cloud assets for misconfigurations and vulnerabilities via active scanning and agents.		
218	The solution must accurately track assets and their vulnerabilities, including highly dynamic IT assets like mobile devices, virtual machines, and cloud instances		
219	The solution must provide an optional externally-hosted scanning service that is PCI ASV certified for satisfying PCI DSS section 6.6 and 11.2.2 requirements for quarterly external vulnerability scans.		
220	The solution must support PCI Compliance vulnerability scanning. The solution must include pre-defined PCI scan profiles that meet current PCI DSS criteria for network scanning. Functionality must exist to filter all other non-PCI relevant vulnerabilities.		
221	The solution must optionally have the ability to support an unlimited number of quarterly PCI attestations.		
222	The solution must be able to support multiple PCI assets.		
223	The solution must have the ability to periodically change the designated PCI assets.		
224	The solution must be capable of agentless compliance auditing without the need for a client- side agent installed on the target device		
225	The solution must provide security and configuration auditing benchmarks for regulatory compliance standards and other industry and service provider best practice standards.		
226	The solution must provide patch auditing for common Microsoft operating systems and applications to include Windows XP, Windows 7, Windows 8 / 8.1, Windows 10, Windows Server 2008 / 2008 R2, Windows Server 2012 / 2012 R2, Windows Server 2016, Windows Server 2019, Internet Explorer, Microsoft Edge, Microsoft Office, IIS, Exchange.		
227	The solution must provide patch auditing for other major operating systems to include macOS, Linux (multiple distributions), Solaris, IBM AIX, HP-UX, and more.		
228	The solution must provide security and configuration auditing benchmarks for service provider best practices such as Microsoft, Linux, routers and switches, firewalls, etc.		
229	The solution must provide auditing of the following for security and configuration settings of applicable and currently used operating system versions.: • Microsoft operating systems • Linux operating systems • Major versions and types of databases		

	• Agency applications • Network infrastructure • Mobile device management • Public cloud (e.g., AWS, Microsoft Azure, Salesforce) and cloud-native infrastructure (e.g., Docker, Kubernetes) • Specific endpoint security products for installation and boot status. • Personally identifiable information (PII) and other sensitive content.		
230	The solution must allow audit policies to be customizable for organizational specific needs.		
231	The solution must provide CIS Certified Benchmarks.		
232	The solution must offer SCAP support.		
233	The solution must aggregate the results of individual scans into cumulative vulnerability views with filtering and analysis to allow drilldown and pivot capabilities.		
234	The solution must have the ability to flag a vulnerability as having been previously resolved.		
235	The solution must provide comprehensive filtering of aggregate vulnerability results with drilldown capabilities.		
236	The solution must provide the ability to automate reporting by being able to schedule reports.		
237	The solution must provide the ability to produce ad hoc reports while viewing results in the console.		
238	The service provider shall be capable to generate multi-format reports, including exporting of report data in PDF, Microsoft Excel, XML, CSV, and HTML.		
239	The reports must have the ability to include hostnames (NetBIOS, DNS) along with IP addresses.		
240	The solution must include customizable graphical and list-based dashboard elements for displaying vulnerabilities and status of the assessed environment.		
241	The solution must encrypt data at rest using at least one level of AES-256 encryption.		
242	The solution must encrypt data in transit using TLS v1.2 with a 4096-bit key.		
243	The solution must support Single sign-on (SSO) authentication methods.		
244	The solution product must be able to partition/segregate data for one customer from data for other customers.		
245	The solution must be able to scan both internal and external web applications and API endpoints		
246	The solution must be able to define parts of critical web applications that are safe to scan, and define other parts that should never be scanned, in order to prevent performance latency and disruptions.		
247	The solution must be able to scan HTML5 and AJAX web applications, API Endpoints along with traditional HTML apps.		
248	The solution must be able to report on all web application vulnerabilities - internally and externally facing - in one unified view.		
249	The solution must assess web applications for generic OWASP Top 10 vulnerabilities and specific application component vulnerabilities.		
250	The solution must add new vulnerability detections (plugins) on a consistent basis. Describe the frequency of updates		
251	The solution must support rollover scans for scans that did not previously finish due to timing out.		
252	The solution must be easy to use and scalable to include all of the agency's		

	web applications.		
253	The solution must be able to conduct rapid security assessments		
254	The solution must be able to detect improperly issued or soon-to-expire SSL/TLS certificates		
255	The solution must be able to track the status of agencies vulnerabilities		
256	The solution must provide for an "auto-aging" license model to ensure stale or retired assets no longer count against the license.		
257	The solution must be easy to use and scalable to include all of the agency's web applications.		
B.2 Vulnerability Assessment and Penetration Testing (VAPT)			
258	The engagement shall include Quarterly Vulnerability Assessments and Penetration Testing (VAPT) on a minimum of 15 externally accessible websites, external IP addresses, and minimum of 15 internal applications.		
259	The engagement shall include VAPT for a minimum of 10 mobile applications (regardless of mobile OS), and all subsequent upgrades or revisions shall be scanned and tested prior to their official release.		
260	The engagement shall ensure coverage of various attack surfaces by employing a diverse set of testing methodologies, including but not limited to, manual penetration testing, automated scans, and social engineering campaigns, to simulate real-world attack scenarios.		
261	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) • Point Of Sale (POS) Applications • 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 **Each VAPT run shall include:** • Presentation of identified vulnerabilities and recommended remediation • Formal report for the conducted VAPT activity • Validation run to verify implemented remediation of identified vulnerabilities		
262	The engagement shall include the following activities: a. Planning of activities and timelines to be agreed with agencies b. Vulnerability assessment of the identified websites c. Penetration testing of the identified websites d. Automated and manual testing of discovered vulnerabilities which includes the following:		

	• SQL Injection • SQL injection (Boolean) • SQL Injection (Blind) • Cross-site Scripting • Command Injection • Command Injection (Blind) • Local File Inclusion • Remote File Inclusion • Code Evaluation • HTTP Header Injection • Open Redirection • Expression Language Injection • Web App Fingerprint • RoR Code Execution • WebDAV • Reflected File Download • Insecure Reflected Content • XML External Entity • File Upload • Windows Short Filename • Server-Side Request Forgery (Patter Based) • Server-Side Request Forgery (DNS) • SQL Injection (Out of Band) • XML External Entity (Out of Band) • Cross-site Scripting (Blind) • Remote File Inclusion (Out of Band) • Code Evaluation (Out of Band) e. False Positive Validation f. Proof-of-concept of discovered exploits g. Recommend remediation of identified vulnerabilities h. Post remediation validation of identified vulnerabilities. This would also include handholding with the agencies concerned to properly remediate/mitigate vulnerabilities, findings, and observations. The remediation of identified vulnerabilities shall be done by agencies.		
263	At the end of each VAPT, the following deliverables will be due: a. Completion of VAPT activities b. Detailed report on conducted VAPT. c. Recommended remediation of identified vulnerabilities d. Executive summary of the project e. Presentation of project results f. Technical Report		
B.3. Attack Surface Management			
264	The solution should have the capability to access every internet-accessible asset of the agency, from web servers and name servers to IoT devices and network printers.		
265	The solution must enable the discovery and analysis of an unlimited number of domain names, empowering the agencies to mitigate cyber risk and uncover potential threats.		
266	The solution must provide continuous data refreshes, updating terabytes of data to ensure the agencies have the most up-to-date view of their attack surface.		
267	The solution must facilitate the analysis of changes in the attack surface through subscriptions, providing automatic alerts for new and significant alterations.		
268	The solution must be enriched with internet-accessible assets with over 200		

	fields of metadata, including CMS type, TLS certificate expiration date, geo-IP location, and cloud or CDN provider.		
269	The solution must have the capability to automatically discover domain names related to assets and suggest them with detailed ownership verification, aiding organizations in identifying owned domains.		
270	The solution must support easy sorting and management of assets based on filters, tags, and other criteria, streamlining asset management processes.		
271	The solution must provide automated risk prioritization, allowing the agencies to quickly identify and address critical threats to their external attack surface.		
272	The solution must have real-time threat alerts for unauthorized changes or suspicious activities detected on the external attack surface, ensuring prompt responses to potential risks.		
273	The solution must support compliance with industry standards and regulations related to the external attack surface, establishing a robust foundation for regulatory adherence.		
274	The solution must provide a well-documented restful API, allowing organizations to create customized integrations that support their security systems and workflows.		
275	The solution must provide the ability to automate reporting by being able to schedule reports.		
276	The solution must provide the ability to produce ad hoc reports while viewing results in the console.		
277	The solution must support the ability to produce reports in the following but not limited to the following report formats: PDF, CSV, HTML,		
278	The solution must include customizable graphical and list-based dashboard elements for displaying vulnerabilities and status of the assessed environment.		
279	The solution must have the ability to create remediation goals and track whether the remediation projects are aptly tracking and closing critical findings within a specific period.		
280	The solution must aggregate the results of individual scans into cumulative vulnerability views with filtering and analysis to allow drilldown and pivot capabilities.		
281	The solution must have the ability to flag a vulnerability as having been previously resolved.		
282	The solution must be a proven solution with advanced features and capabilities for continuous discovery, analysis, prioritization, remediation and monitoring of the cybersecurity vulnerabilities and potential attack vectors. Its effectiveness should be validated through third-party evaluations by industry-recognized research and advisory firms like Gartner and/or IDC, and/or Forrester. The solution must have been identified as a leader in the latest release of the Risk based Vulnerability Management and Vulnerability Risk Management.		
C. Threat Intelligence and Brand Monitoring			
283	The solutions shall deliver threat intelligence and brand monitoring for the following: • Brand protection - company names/domain • Social media pages • External Internet Protocol (IP) addresses • Website and mobile banking monitoring • VIP e-mails • Sector monitoring Financial, Government • Society for Worldwide Interbank Financial Telecommunication (SWIFT) codes • Credit cards		

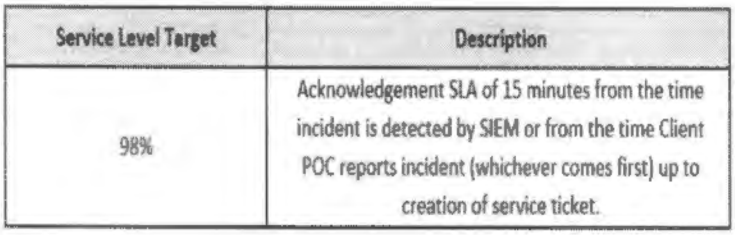
	• GitHub • Custom queries • Unlimited Site take downs (i.e., phishing, social media sites, and others) • Scarping databases that contain large amounts of data found in the deep and dark web • Third party queries • Investigation • Threat library		
284	Must provide Unlimited take downs of the following but not limited to: • Phishing Websites • Type-squatted domains involved in sending phishing emails • Fake or counterfeit content • Website fraudulently claiming affiliation of your brand • Domain abuse involving copyright/trademark infringement • Type squatting websites hosting malicious/copyrighted/trademark content • Fake accounts on social media or professional network platforms impersonating the banks and its employees. • Unauthorized or sensitive content on GitHub, Bitbucket and other code repositories and file sharing sites. • Breach Data Hosted on public cloud storage • Fake and/or suspicious mobile applications posing as a legitimate application. • Google search results such as ads and sponsored pages leading to phishing websites and fraudulent activities. • Personal information of the bank executives.		
285	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, service provider 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		
286	The threat intelligence solution must be able to: • Detect and take down servers launching phishing attacks • Identify fraudulent social media accounts that are impersonating the Government Agencies and its executives • Take down of fake applications that impersonate legitimate ones from app stores. • Take immediate action on the Government Agencies' behalf and provide all the context to execute rapid take-down of malicious servers, websites or social media accounts.		
287	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.		
288	The solution shall report information on the intention to target agencies or other government industries, major activist campaigns, and indications of		

	activism against the agencies, banking sector, and the government.		
289	The solution shall monitor the domains and IP addresses that have bad reputation.		
290	The collection of intelligence from the various sources must be automated, using technologies such as machine learning, temporal analysis and Natural Language Processing, which allows mass collection and processing of intelligence with low false positives, in near real-time.		
291	The threat intelligence solution must use machine learning and natural language processing to parse text from millions of unstructured documents across different languages and classify them using language-independent ontologies and events, enabling analysts to perform powerful and intuitive searches that go beyond bare keywords and simple correlation rules		
292	The threat intelligence solution must have at least 5 years of historical data and should be included in real time query results in its portal with event details.		
293	The threat intelligence solution must be capable of deduplicating multiple references or mentions of the same threat indicators, links or social media accounts.		
294	The threat intelligence solution must be able to collect data across all countries and industries.		
295	The threat intelligence solution must provide and display information in near real-time as new information or context is gathered from various sources.		
296	The threat intelligence solution must provide IOC with dynamic risk score. Scores must be justified with rational behind the given scores and provide sources of reference in which score is derived from (e.g., if score arises from data found in pastebin, reference and hyperlink to pastebin must be made available).		
297	The solution must also provide risk evidence into why these risk scores are given and through the solution, see the references that alluded to the risk score		
298	The threat intelligence solution must provide research into indicators (including IP Addresses, File Hashes, CVEs, Threat Actors, Malware, Domains) and to be delivered and visualized with context and associations of related entities, these related entities should include at minimal: hashes, IPs, CVEs and Threat Actors, Threat Vectors, Targets, Malware, Product impacted etc that are found associated with the indicator of interest.		
299	The contextualized threat information should be delivered in a simple and easy to digest format over a single page view to display all information regarding the indicator.		
300	The threat intelligence solution must have references to the source of information presented, either through a direct link to the source or a cached copy.		
301	The threat intelligence solution must be able to support analysis with: • Real-time trends and developments • Historical view of related events • Reported roles involved in the events (attackers/threat actors, targets/organizations) • Reported TTPs (attack vectors, malware, exploits) • Reported indicators (IP addresses, domains, hashes, URLs etc.) • Related operations • Access to the original references with cached content for the volatile ones		

	• Other contextual details about the events		
302	The threat intelligence solution must allow for categorization of the historical data of the threat actor, threat activity, threat objects (historical data of the IPs, URLs, etc. used by the malicious entity).		
303	The threat intelligence solution must provide nontechnical data/information/intelligence related to threat actor, attack campaign, analysis report, tactics, techniques and protocols (TTPs)		
304	The threat intelligence solution must allow end user expert analysts within the organization to collaborate by adding notes or cross referencing indicators.		
305	The threat intelligence solution must include provisioning of IR hunting tools, such as YARA rules, SNORT rules or MITRE ATT&CK Identifiers to assist in hunting for adversaries, malware, or traffic of interest.		
306	The threat intelligence solution must provide Risk Score for Vulnerability which are Pre-NVD (No CVSS score upon release)		
307	The threat intelligence solution must provide the capability for Analysts to upload artefacts for sandbox analysis. Sandbox must not disseminate the uploaded artefact file to the wider world on VirusTotal or similar websites.		
308	The threat intelligence solution must allow users to provide instant feedback via the user interface to request for data review or validation.		
309	The threat intelligence solution must enable end users to set up notifications to inform different recipients of different types of intelligence or an increase in the prevalence of references.		
310	The threat intelligence solution must include exportable/integrated data via the following formats: • Machine readable feeds, available as CSV or STIX files, and containing high-risk indicators with supporting evidence that are accessible by end-users, • Human readable finished intelligence reports written on-demand or on a regular basis; reports are "live" and have references to the latest intelligence.		
311	The threat intelligence solution must provide the latest cybersecurity news and/or advisories, including local threats and incidents across various industries, with a focus on but not limited to the financial sector and government. Advisories should be delivered daily via email.		
312	The threat intelligence solution must include validated research documents from in-house Threat Researchers. When searching for an indicator (e.g., Malware or Threat Actor), the result should contact all the research documents related to the indicator		
313	The threat intelligence solution must provide web browser extension to deliver dynamic risk scores based on real-time intelligence for a quick triage of information on any web page. All indicators on the page are automatically identified and displayed in order from highest to lowest risk, allowing Analysts to confidently prioritize where to focus.		
314	The threat intelligence solution must be able to minimally provide brand protection capabilities such as typo squats attempts, track DNS changes, detect logo abuse, impersonation attempts and fake applications detection		
315	The threat intelligence solution must be able to minimally provide data leakage detection capabilities such as account sale, CC sales credentials leak in open/dark web, domain leakage on code repositories and leakage on ransomware extortion sites		
316	The threat intelligence solution must be able to perform industry peer comparison and ability to trend attack methods (e.g., track new phishing malware)		

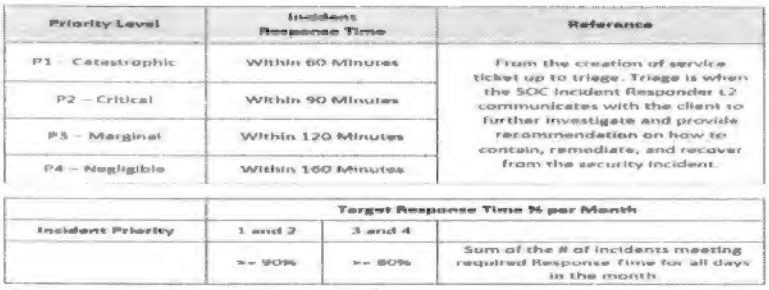
Incident Response			
317	The service provider shall review the agencies' Incident Response Plan (IRP), which would guide the agencies on the creation, enhancement, and documentation of incident response playbooks, policies, and guidelines, such as, but not limited to: • Escalation process • Incident containment process • Incident eradication process ▪ Incident recovery process • Incident identification process • Process flow		
318	The service provider for each agency shall cover an unlimited number of IRs where the service provider shall act as the Incident Response (IR) Manager for the agency, facilitating the six phases of IR. The provider's Incident Response Team must be on-call 24/7 and capable of providing IR activities onsite within twelve (12) hours of a reported and confirmed cybersecurity incident (i.e., in the event of a successful breach)		
319	The service provider shall conduct an annual, or as needed, incident readiness training including response drill or simulation exercises with the agencies' Computer Security Incident Response Team (CSIRT) to enhance detection and internal readiness for cybersecurity incidents. The training must be designed to cover best practices for isolation, containment, and remediation of security incidents, as well as internal and external incident communications, minimizing the impact on operational continuity, reporting to regulators (e.g., NPC, BSP), CSIRT readiness, blue team capabilities, tabletop exercises, and other relevant areas		
320	The service provider shall likewise provide IT security awareness trainings to both technical and non-technical audience of the agencies.		
321	The service provider shall map security playbook and runbooks for applicable security use cases to guide client on their incident response.		
322	The service provider shall deliver ON-SITE technical assistance to the agencies' CSIRTs during emergency breach responses within 12 hours. All incident response team members of the service provider must be present on-site when deemed necessary by the agency.		
323	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.		
324	The service provider shall deliver network/firewall/web applications breach response.		
325	The service provider shall identify, cleanse or contain malicious code, malware, spyware, and system-file hacks		
326	The service provider shall deliver root cause analysis to identify the intrusion vector and provide mitigating procedures to address network and system vulnerabilities.		
327	The service provider shall identify indicators of attackers and scan the network to search for other related infected systems.		
328	The service provider shall deliver insider threat investigation, as needed.		
329	The service provider shall deliver employee misconduct investigations, as needed.		
330	The service provider shall deliver incident and investigation reports.		

331	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.		
332	The service provider shall assist in the following: • Incident handling preparation and execution • Crisis management • Breach communication • Forensic analysis • Remediation		
333	The service provider shall rate the prioritization and severity of security incidents and create a service ticket as per agreed Service Level Agreement (SLA).		
334	The service provider must have crisis/emergency management capabilities/expertise.		
E. Service Level Agreement			
335	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 Client POC reports incident (whichever comes first) up to creation of service ticket.

336			



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 Incident Responder L2 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 # of incidents meeting required Response Time for all days in the month

Time to respond or provide request from when incident or request is reported based on severity level.

Non-Functional Requirements			
A. Access Management			
337	The service provider's solutions shall provide access platform to each agency and shall accessed through a centralized portal, which enforces session timeouts, mandates the use of multi-factor authentication (MFA), and can monitor user behavior.		
338	All credentials with the service provider shall be stored in a monitored central management system.		
339	The service provider shall maintain logical access controls including the access of each agencies which are role-based and segregation of duties.		
340	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.		
341	All access on the service provider's managed endpoints to sensitive resources shall be conducted through secured means, such as Virtual Desktop Infrastructure, ensuring secure access and control management.		
342	The service provider shall provide physical and environmental controls at the security operations center		
B. Training and Other Requirements			
343	The service provider shall conduct technology updates or workshops at least twice a year for the agencies. These updates or workshops must be aligned with the solutions and services provided by the service.		
344	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.		
345	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.		
346	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.		
347	The service provider must notify the agency's designated IT security personnel, who will be the point of contact for the service provider, of any related cyber security supply chain incidents such as, but not limited to compromise/breaches involving the vendor/supplier/client data, the product hardware or software, etc. It must be reported within a risk-informed time frame of at-least 24 hours upon learning of the incident. Must provide documentation on incident response handling procedure.		
348	The service provider must notify the agency's designated IT security personnel, who will be the point of contact for the service provider, of any critical security vulnerabilities, firmware upgrades, and performance patches or fixes that need to be applied. Additionally, they must provide a detailed support plan and procedure.		
349	The monthly service performance report should contain the following: • 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		
350	The service provider must provide an annual executive report that provides trend analysis reports based but on the following but not limited to: • Monitoring Summary - current view of overall environment health and potential threats. • Incident Summary -provide a detailed account of security incidents, their handling, and outcomes of the agency. • Threat Summary - high-level overview of the current threat landscape facing the agency • Actionable Alerts - contextual information such as historical trends, threat intelligence insights, or relevant industry benchmarks to help executives better understand the significance of the alert and its implications for the organization.		
351	The winning bidder must comply with requirements related to third-party/vendor assessments conducted by the agency's internal audit, as well as with external audits required by regulatory agencies such as the Bangko Sentral ng Pilipinas.		

352	The winning bidder will be subject to regular performance assessments. The results of these assessments will be considered when renewing the contract. Additionally, the performance of the winning bidder will be taken into account for any future contracts with the agency.		
C. Service Provider's Qualification and Requirements **Note: Submission of required documents shall be during the submission of bids.**			
353	The service provider must be a certified/authorized reseller of the brand / solutions being offered. The service provider must submit current certifications from the manufacturer.		
354	The service provider must have local sales and technical offices in the Philippines. The service provider must submit the list of local sales and technical offices in the Philippines. This is subject for actual site visit to the facility.		
355	The service provider must demonstrate its commitment to and compliance with the minimum standards of Service Organization Control 2 (SOC 2). The provider must present at least one (1) attestation from a globally recognized auditing firm or its member, verifying that it has met its service commitments and system requirements based on the applicable trust criteria. The SOC 2 Type II assessment must have been conducted within the five (5) years preceding the bid submission date.		
356	The service provider must have undergone ISO 27001 certification within the last three (3) years to ensure that controls, processes, and procedures that the service provider has put in place to ensure the confidentiality, integrity, and availability of the data in its possession. The service provider must submit its valid ISO 27001 certification as proof of compliance.		
357	The service provider must demonstrate the adherence to the Data Privacy Act of 2012 and must submit a copy of valid Certificate of Registration issued by the National Privacy Commission		
358	The service provider must submit proof that they have a Business Continuity Plan (BCP) and has been tested for disaster scenarios to ensure service continuity during disruptions. The service provider must submit a report on the conduct of BCP testing, which should include a summary of the activities performed, defined targets, actual results, and details on Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).		
359	The service provider must have at least **Two (2) local Certified Security Engineer for each proposed solution** to support the re-configuration, maintenance and 24x7 uptime services within the maintenance period. • Managed Detection and Response • Security Information and Event Management • Security Orchestration, Automation and Response • Network Detection and Response • Vulnerability Management • Must be employed with the bidder for at least one (1) year before the bid opening • At least one (1) year experience in administration of the solution Must submit the following: • Certificate of Employment for the assigned personnel indicating the date of hire • Resume or Curriculum Vitae indicating that the personnel assigned have performed or are currently performing at least three (3) engagements with the bidder comparable to the proposed engagement. • Certification of the assigned engineer/personnel		

360	The service provider must have at least 24x7x365 team within the Security Operations Center assigned for the agencies: **Six (6) -Tier 1 Security Operation Center (SOC) Analyst** responsible for the following tasks: a) Monitoring via existing SIEM/Analytics Platform b) Funneling of alerts (noise elimination) c) Incident Validation d) Case Management e) Threat Containment (Using Existing EDR or agreed process) – with guidance from L2 and up f) General Communication g) Weekly Summary Reports • Must be employed with the bidder for at least one (1) year before the bid opening • At least one (1) year experience in security monitoring (SIEM and/or SOAR) or system and network administration experience **Must submit the following:** • Certificate of Employment for the assigned personnel indicating the date of hire • Resume or Curriculum Vitae indicating that the personnel assigned have performed or are currently performing at least three (3) engagements with the bidder comparable to the proposed engagement. • At least one (1) of any of the following unexpired professional certifications: CISA, CISM, GSEC, GMON, GCDA, GWAPT, GCIH, GCFA, GCIA, CCNA, CEH, CHFI, CNDA, CFR, CompTIA Security+ CVA, OSCP, CISSP, GPEN, GXPN, LPT Master, CPT, CEPT, CMWAPT, CompTIA PenTest+, CPISI, or other security-related certifications.		
361	**Three (3) Tier 2 Security Operation Center (SOC) Analyst** who will be responsible to conduct further analysis and decides on a strategy for containment such as: a) Proactive Searches/ Threat Hunting b) Qualification of Incident Priority/Severity c) Investigation via SIEM/Analytics Platform and other accessible sources d) Rule Tuning e) Ad hoc Vulnerability Advisory & Research f) Threat Containment (Using Existing EDR or agreed process) g) Incident Response/Recommendations • Must be employed with the bidder for at least three (3) years before the bid opening • At least three (3) years experience in security monitoring or system and network administration experience **Must submit the following:** • Certificate of Employment for the assigned personnel indicating the date of hire		

	• Resume or Curriculum Vitae indicating that the personnel assigned have performed or are currently performing at least three (3) engagements with the bidder comparable to the proposed engagement. • At least two (2) of any of the following unexpired professional certifications: CISA, CISM, GSEC, GMON, GCDA, GWAPT, GCIH, GCFA, GCIA, CCNA, CEH, CHFI, CNDA,CFR, CompTIA Security+ CVA, OSCP, CISSP, GPEN, GXPN, LPT Master, CPT, CEPT, CMWAPT, CompTIA PenTest+, CPISI, or other security-related certifications.		
362	**One (1) Tier 3 Security Operation Center (SOC) 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 such as: a) Manage High Severity Triage b) Incident Response and Forensics Capabilities c) Threat Containment (Using Existing EDR or agreed process) d) Reporting and Post Incident Review e) Use Case Development f) Threat Searches g) New Correlation Rules • Must be employed with the bidder for at least five (5) years before the bid opening • At least three (3) years experience in security operations center monitoring and management **Must submit the following:** • Certificate of Employment for the assigned personnel indicating the date of hire • Resume or Curriculum Vitae indicating that the personnel assigned have performed or are currently performing at least three (3) engagements with the bidder comparable to the proposed engagement. • At least two (2) of the following unexpired cybersecurity professional certifications: CISA, CISM, GSEC, GMON, GCDA, GWAPT, GCIH, GCFA, GCIA, CCNA, CEH, CHFI, CNDA, CFR, CompTIA Security+ CVA, OSCP, CISSP, GPEN, GXPN, LPT Master, CPT, CEPT, CMWAPT, CompTIA PenTest+, CPISI, or other security-related certifications.	?	
363	**One (1) Local Security Operation Center (SOC) Manager** responsible in overseeing the day-to-day operations and strategic direction of a Security Operations Center. SOC manager also responsible in ensuring effective incident management Reporting of current threat environment, incidents and projected threats to its clients. • Must be employed with the bidder for at least five (5) years before the bid opening • At least three (3) years experience in security operations center monitoring and management. **Must submit the following:** • Certificate of Employment for the assigned personnel indicating the date of hire		

	• Resume or Curriculum Vitae indicating that the personnel assigned have performed or are currently performing at least three (3) engagements with the bidder comparable to the proposed engagement. • At least three (3) of the following unexpired cybersecurity professional certifications: Certified Information Systems Auditor (CISA), 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), Computer Hacking Forensic Investigator (CHFI), Certified Network Defense Architect (CNDA), CyberSec First Responder (CFR), 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+, CompTIA Security Analytics Professional, Certified Payment Card Industry Security Implementer (CPISI)		
364	**At least two (2) Local Digital Forensics and Incident Response Analysts** • Must be employed with the bidder for at least two (2) years before the bid opening • At least two (2) years experience in security operations center monitoring and management **Must submit the following:** • Certificate of Employment for the assigned personnel indicating the date of hire • Resume or Curriculum Vitae indicating that the personnel assigned have performed or are currently performing at least three (3) engagements with the bidder comparable to the proposed engagement. • Has at least two (2) of the following unexpired professional certifications: CISA, CISM, GSEC, GMON, GCDA, GWAPT, GCIH, EC Council Incident Handler, 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.		
365	**At least two (2) Local Senior Threat Intelligence and Threat Hunting Analysts** responsible in collecting, processing, organizing and interpreting of data into actionable information that relates to capabilities, opportunities, actions and intent adversaries in the cyber domain. • Must be employed with the bidder for at least two (2) years before the bid opening • At least two (2) years experience in security operations center **Must submit the following:** • Certificate of Employment for the assigned personnel indicating the date of hire		

	• Resume or Curriculum Vitae indicating that the personnel assigned have performed or are currently performing at least three (3) engagements with the bidder comparable to the proposed engagement. • At least-two (2) of the following unexpired cybersecurity professional certifications: CISA, CISM, GSEC, GMON, GCDA, GWAPT, GCIH, EC Council Threat Intelligence Analyst, 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		
366	**At least two (2) Local Vulnerability Assessment and Penetration Tester** responsible in conducting regular vulnerability assessment across systems, networks and applications to identify security weaknesses, misconfigurations, and potential vulnerabilities. • Must be employed with the bidder for at least one (1) year before the bid opening • At least one (1) year experience in providing VA/PT or similar services **Must submit the following:** • Certificate of Employment for the assigned personnel indicating the date of hire • Resume or Curriculum Vitae indicating that the personnel assigned have performed or are currently performing at least three (3) engagements with the bidder comparable to the proposed engagement. •At least two (2) of the following unexpired cybersecurity 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, Certified Red Team Professional or other security-related certifications		
367	**At least Twenty (20) Onsite Technology Support Engineers within Metro Manila that** *can provide auxiliary support services for the tools and platforms used by the agencies and offer technical assistance, specifically in recommending additional security controls for existing platforms beyond the proposed solutions, to enhance the mitigation of cybersecurity incidents and exposure to attacks.* • Must be employed with the bidder for at least one (1) year before the bid opening • At least one (1) year experience in implementation, configuration and support services of networking and/or network security and/or systems administration, directory Services Must submit the following: • Certificate of Employment for the assigned personnel indicating the date of hire • Resume or Curriculum Vitae indicating that the personnel assigned have performed or are currently performing at least three (3) engagements with the bidder comparable to the proposed engagement. • Has at least (1) of the following security-related technical certification in the following: networking or network security such as Network Devices (Network Associate and/or Professional), Firewalls, Intrusion Prevention Systems, Application Delivery Controllers Administration, Email Security,		

	Web Security, and Server and/or Systems Administration, Directory Services		
368	**One (1) Project Manager who** shall oversee the implementation of platforms, ensuring they are properly implemented and fine-tuned. • Must be employed with the bidder for at least five (5) years before the bid opening • At least three (5) years experience in project management **Must submit the following:** • Certificate of Employment for the assigned personnel indicating the date of hire • Resume or Curriculum Vitae indicating that the personnel assigned have handled Information Technology Security solutions or managed security services projects, for at least three (3) Philippine banks and one (1) non-bank client. Must include the End-User/Client company name, Project Name and Project Duration (start date and end date). • Project Management Professional (PMP) Certification of the assigned personnel		
369	**One (1) Service Delivery and Escalation Manager** shall oversee the service quality, ensuring that issues are resolved efficiently The role of the Service Delivery shall also include overseeing the implementation, operation, and improvement of service delivery, ensuring that the service provider meets the agreed-upon SLAs and expectations of the agency. The manager will manage and resolve service-related issues and incidents, identify areas for service improvement, and implement necessary changes. • Must be employed with the bidder for at least five (5) years before the bid opening • At least three (5) years experience in service delivery management Must submit the following: • Certificate of Employment for the assigned personnel indicating the date of hire • Resume or curriculum vitae indicating that the personnel assigned to the Service Delivery Management role assigned to at least three (3) Philippine banks and one (1) non-bank client. The resume must include the end-user/client company name, project name, and project duration (start and end dates) • IT Infrastructure Library (ITIL) Certification of the assigned personnel		
370	The winning bidder shall be required to demonstrate the salient features of the proposed Shared Cyber Defense Solution at the Project Site or via online.		
371	In cases where there are limiting conditions or measures to demonstrate the functional specifications, the winning bidder shall provide documentation to attest its compliance with the specifications; and		
372	The winning bidder shall likewise be required to submit a Certification from the manufacturer stating therein that the proposed solutions to be finally delivered per SCC Clause No. 4 of the issued Bidding Documents are fully		

<table>
<tr><td></td><td>compliant with the technical specifications stipulated under Section VII. Technical Specifications.

The Certification issued by the Manufacturer and the Demo Units must be submitted and delivered within seven (7) calendar days from receipt of the notice of Lowest Calculated Bid (LCB) or Single Calculated Bid (SCB). The demo units must likewise be set-up within the same period, except when the unit/s requires elaborate testing or equipment is sourced from abroad and other similar or analogous cases where extension may be granted. Failure to submit all deliverables on or before the deadline shall result in the disqualification of the winning bidder.</td><td></td><td></td></tr>
<tr><td colspan="4"><b>Delivery Time/Completion Schedule</b></td></tr>
<tr><td>373</td><td>Two (2) years subscription to <b>start upon receipt of Notice to Proceed and acceptance of Phase 1 deliverables.</b></td><td></td><td></td></tr>
<tr><td>374</td><td>The Project must be implemented by phases: Phase 1 - Threat Intelligence and Incident Response within five (5) calendar days, Phase 2 – <b>Vulnerability Management and Penetration</b> Testing with ten (10) calendar days, Phase 3 - <b>Security Monitoring and Management</b> within fifteen (15) calendar days. The service provider must therefore provide a project schedule which should present the project milestones and deliverables at each milestone.

All deliverables shall become the property of the concerned agencies.</td><td></td><td></td></tr>
<tr><td colspan="4"><b>Payment and Delivery Terms and Condition</b></td></tr>
<tr><td>375</td><td>The service provider shall be paid upon receipt of its deliverables, based on the submitted Project Schedule and issuance of the Certificate of Acceptance. The Service Provider shall be paid based on the following milestones:
<table>
<tr><th>First (1st) Year:</th><th>% of Contract Price</th></tr>
<tr><td>Upon Phase 1 implementation and acceptance:
• Threat Intelligence
• Incident Response</td><td>10%</td></tr>
<tr><td><b>Upon Phase 2 implementation and acceptance:</b>
• <b>Vulnerability Management and Penetration Testing</b></td><td>10%</td></tr>
<tr><td><b>Upon Phase 3 implementation and acceptance:</b>
• <b>Security Monitoring and Management</b></td><td>10%</td></tr>
<tr><td>Upon full implementation of the Shared Cyber Defense solution and Agency acceptance</td><td>20%</td></tr>
<tr><td><b>Second (2nd) Year:</b></td><td></td></tr>
<tr><td>Four (4) quarterly payments at 12.5% each</td><td>50%</td></tr>
<tr><td><b>Total</b></td><td><b>100%</b></td></tr>
</table></td><td></td><td></td></tr>
</table>

Land Bank of the Philippines:

NAME	SIGNATURE
Edward A. Juan TWG Head, Information Technology Officer	

Development Bank of the Philippines:

NAME	SIGNATURE
Leandro D. Cabanilla Assistant Manager	

Philippine Guarantee Corporation:

NAME	SIGNATURE
Lloyd A. Sioson Vice President	

Annex D-36

Home Development Mutual Fund:

NAME	SIGNATURE
Teresa M. Manabat Vice President	Tmanabat

Annex D-37

CLASS D

Project Identification No	**LBP-ICTBAC-ITB-GS-20241129-04**
Project Name	**Two (2) Years Shared Cyber Defense Solution for the Government-Owned and Controlled Corporation (GOCC) Cluster**
Subject	**Responses to Bidder's Queries**

Item No.	Portion of Bidding Documents	Queries And/Or Suggestions	TWG Responses
	Page 64 Point 20, SOC Team	Can you please confirm if GOCC is looking for dedicated 39 resources given in RFP under page no 64 or service provider can leverage shared team from our delivery center to deliver 24x7 shared security monitoring?	The 39 resources should be dedicated for the cluster.
A. Security Monitoring and Management			
8	A.1 Security Operations Center (SOC), pages 80-81, Annex D-3-4 Monthly monitoring service management: The service provider shall conduct regular meetings ...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 **• Time to Detect** **• Time to Engage/Respond**	May we confirm that the "mean time to detect" refers to the time from the alert detection to the creation of ticket while the "mean time to engage/ respond" refers to the time from initial detection until the provision of analysis and recommendation?	Yes, for both.
10	A.1 Security Operations Center (SOC) page 80, Annex D-3 Item #10 - The service provider must be able to utilize and support the agency's existing on-premises Security Information and Event Management (SIEM)	May we confirm that the proposed SIEM, VM Scanner and NDR are the required on-premise tools, and the rest of the solution can be proposed/offered as cloud based solutions?	Yes

Annex F-1

	platform or migrate the logs generated by the agency over the past 12 months if the service provider proposes a new SIEM platform.		
	A.2.1 Deployment and Management page 83, Annex Item #47 For non-supported systems, other means of monitoring must be performed, such as network detection and response (NDR or similar) tool shall be provided. On-prem appliance must have the following capabilities:...		
	D-6 B.1 Vulnerability Management page 90, Annex D-13 Item#152: The solution must be a cloud-based offering but supports on- premise scanners		
	A.1 Security Operations Center (SOC)	Could you please elaborate how currently SOC services being delivered to all the 4 entities? Is current service provider providing 24x7 services using single SIEM and SOAR platform or you have separate license for all the 4 entities?	There is no specific requirement on the SIEM and SOAR licensing, as long as the data segregation requirement is met. (*Kindly refer to item 244 under SOAR*) If under SOAR, reference should be from items 126 to 151
		Please confirm the SIEM and SOAR tool currently being used to deliver 24x7 security monitoring. Also confirm if we can leverage existing investments to deliver 24x7 security monitoring?	This information shall only be provided to the winning bidder. The SIEM and SOAR is part of the deliverables to be provided by the winning bidder.

		What are the HA/DR requirements for the respective environment (if any and if OnPrem)	There is no specific requirement on the HA/DR as long as the 24/7 uptime services are met. *(Kindly refer to item 3 under Security Monitoring and Management and 359 under Service Provider Qualifications and Requirements)*
		Please confirm the SIEM and SOAR solutions are deployed on prem or SaaS?	SIEM on prem; SOAR either on prem or on cloud Refer to Items 97 to 125 for the SIEM and 126 to 151 for the SOAR.
		Please share the log sources details (Agency Wise) which we need to be onboarded into SIEM .	This information shall only be provided to the winning bidder.
		Pls share current EPS, log ingestion (GB/Day) and No of alerts/month (Qualified Alerts) per agency if you have separate SIEM and SOAR for every agency	This information shall only be provided to the winning bidder.
		Which ticketing tool is currently getting leveraged? Is the auto ticketing of alerts are in place?	The solution shall have its own ticketing tool. Refer to item 6 of Security Monitoring and Management.
		What is the ratio of False positives and True Positives alerts?	This information shall only be provided to the winning bidder.
		How many correlations rules (Use Cases) are defined and is currently active?	This information shall only be provided to the winning bidder.
		Are the correlation rules are mapped with MITRE attack tactics and techniques?	This information shall only be provided to the winning bidder.
		What is the log retention period defined for Online and offline logs?	Kindly refer to item 99 under SIEM.
		Is the existing SIEM solution is monitoring both events and flows or events only?	Kindly refer to item 98 under SIEM.
		What are the challenges in existing SIEM solution?	This information shall only be provided to the winning bidder.
	A.2 Managed Detection and Response	How currently the Machine Learning based detection and prevention are happening?	This information shall only be provided to the winning bidder.
		Which EDR solution is in place in all the 4 agencies ? Also confirm if endpoint agents deployed on all the endpoints .	This information shall only be provided to the winning bidder.

		Please confirm if EDR is currently integrated with SIEM or not?	Yes, EDR is integrated with SIEM.
		Please confirm if you are looking for a MDR service directly from the product vendor or can the service provider provide similar service? A.2.1.34	The additional MDR should directly come from the product vendor/manufacturer.
		Is there are Playbooks defined for taking automated actions on Endpoints using EDR?	Yes
Security Orchestration, Automation, and Response (SOAR)			
	A.4 Security Orchestration, Automation and Response (SOAR)	Is there any existing SOAR platform getting leveraged?	No, the SOAR is part of the deliverables to be provided by the winning bidder.
		Are the SOAR platform is integrated with the available set of security solutions for each entities?	No
		Are the SOAR playbooks are defined for both Intrusive and Non-Intrusive actions?	Yes
		How many playbooks are currently configured?	This information shall only be provided to the winning bidder.
		Is there is any Case management functionality available in existing SOAR solution.	Yes
		Is the existing SOAR solution is capable of grouping multiple alerts to a single case?	Yes
		What are the current challenges in the existing SOAR solutions?	This information shall only be provided to the winning bidder.
137	A.4 Security Orchestration, Automation and Response (SOAR), page 88, Annex D-11 The SOAR solution must have crisis/emergency management capabilities	May we request that it be revised to include crisis/emergency management capabilities within the Incident Response (service) section, as this pertains to the service deliverables and capabilities of the provider, rather than the tool itself?	**For issuance of Bid Bulletin:** **Requirement to be transferred FROM Security Orchestration, Automation and Response (SOAR) TO Incident Response (IR).**
B. Vulnerability Management and Penetration Testing			
	B.1 Vulnerability Management	Which Vulnerability Assessment solutions is in place currently.?	This information shall only be provided to the winning bidder.
		What is the frequency of VA scanning?	Regular and as needed, Refer to items 152 to 257
		What is the frequency of Ad hoc scanning request?	As needed
		Does the number of endpoints corresponds directly to Number of IP/assets to be scanned?	No. This information shall only be provided to the winning bidder.

		Is patch management also under scope?	No, kindly refer to item 207 under Vulnerability Management
		Is there any existing ITSM solution in place? If not what is preferred ITSM solution? Does client want to integrate ITSM solution with VM solution?	Yes. -- It depends on the ITSM solution in place by the respective agencies.
		Is 31900 endpoints count inclusive of all optional scope services (External scan/ web app scan/ Policy compliance/PCI DSS) if no, what is the count of endpoints in optional scope?	No. This information shall only be provided to the winning bidder.
		What is the preferred benchmark (NSIT or CIS)? Also, is there any compliance or regulations that scanning needs to adhere to base on the geographic distribution of assets?	There is no preferred benchmark as long as it is compliant with relevant industry benchmarks. None
		Does the client have any prioritization and risk rating calculation already existing in the system?	Yes, however should be part of the deliverables to be provided
		How does the client expect to be notified/reported about the found vulnerabilities?(Excel reports, power point presentations or through virtual dashboards)	Kindly refer to item 238 under Vulnerablity Management
		Is the current VA solution is capable of doing asset management?	Yes
		Is the VA solution is integrated with SIEM for correlating the vulnerable assets.	Yes, kindly refer to item 4 under Security Monitoring and Management
		Is the VA solution is integrated with SOAR platform for initiating automated scans?	No
	B.1 Vulnerability Management, page 90, Annex D-13 The solution must be able to monitor network traffic continuously to detect and assess short-lived systems and hard-to-scan devices, such as sensitive OT and IoT systems.	May we confirm if the agencies already have existing OT/IoT systems in place? Additionally, can we confirm that the requirement is for the solution's capability to support the detection of OT and IoT systems?	Yes, for both.

Vulnerability Assessment and Penetration Testing (VAPT)			
	B.2 Vulnerability Assessment and Penetration Testing (VAPT)	Which tool is used to performing Pen testing activities?	This information shall only be provided to the winning bidder.
		What is the frequency of Pen-testing ?	Regular and as required. Refer to items 258 to 263
		Are the applications developed in-house, purchased, or had the development outsourced?	This information shall only be provided to the winning bidder.
		Are there any special testing restrictions required (i.e. only off-hour testing)?	Yes
		How many API endpoints will be in-scope for the assessment?	This information shall only be provided to the winning bidder.
		Are there any language requirements other than English?	None
		Is remediation validation testing required as part of this engagement?	Yes
		Are these IPs are on-prem or cloud service IPs?	This information shall only be provided to the winning bidder.
		Are there security controls that would detect or prevent testing e.g. IPS or WAFs? If yes can whitelisting be performed to prevent interference.	Yes, for both.
		What are the type of API technology (e.g. REST, SOAP) being used by the in-scope endpoints?	This information shall only be provided to the winning bidder.
		For mobile applications penetration testing share the OS expected (Android/iOS)?	All applicable OS
		Will testers be provided with test data (Postman collection, SoapUI project, Swagger JSON, API documentation)?	This information shall only be provided to the winning bidder.
258	The engagement shall include Quarterly Vulnerability Assessments and Penetration Testing (VAPT) on a minimum of 15 externally accessible websites, external IP addresses, and minimum of 15 internal applications.	May we get the actual number of external and internal websites (per agency)?	This information shall only be provided to the winning bidder.
Attack Surface Management			
	B.3. Attack Surface Management	Is there an existing solution that the agency use for ASM?	None
265	B.3. Attack Surface Management, p. 96, Annex D-19	May we confirm what is the total number of internet-accessible assets (domain names, subdomains, or IP addresses) that each agency has?	This information shall only be provided to the winning bidder

	The solution must enable the discovery and analysis of an **unlimited number of domain names**, empowering the agencies to mitigate cyber risk and uncover potential threats.		
C. Threat Intelligence and Brand Monitoring			
	Threat Intelligence	What is the existing Tech Stack for Threat Intelligence Platform and Threat Intelligence Monitoring?	This information shall only be provided to the winning bidder.
		How frequent the feeds are updated in the existing TI solution?	Real-time
		Do we need to create a separate environment for each entity for Threat Intelligence?	Yes
		What is the employee count for each individual entity?	This information shall only be provided to the winning bidder.
		As a part of threat intelligence, is the executive level monitoring is expected for impersonation, darkweb etc?	Yes
		Are there any specific reporting needs from Threat Intelligence Platform?	Yes
		Is the existing TI solution is integrated with SIEM or SOAR solution for correlations and automations?	Yes
	Delivery Time/Completion Schedule	Should the implementation be completed end-to-end for each phase on the specified calendar days?	Yes
		Delivery Time/Completion Schedule Security Monitoring and Management with ten (10) calendar days, Is the agency open to use a different solution? The estimated number of days which is 10 days will only cover taking over of an existing solution. In case of a new solution, is the agency open to taking over of management and monitoring of existing solution and be able to deploy the new solution within 90 days?	For issuance of Bid Bulletin Yes, as long as it is compliant with the requirements stated in the TOR. We retain the timeline durations stated in our TOR. However, to give ample time with the deployment, we will interchange Phase 2 & 3.

ANNEX F - 7

Incident Response			
319	D. Incident Response, page 101, Annex D-24 The local Service Provider for each agency shall cover an unlimited number of IRs where the service provider shall act as the Incident Response (IR) Manager for the agency, facilitating the six phases of IR. The provider's Incident Response Team must be on-call 24/7 and capable of providing IR activities onsite within twelve (12) hours of a reported and confirmed cybersecurity incident (i.e., in the event of a successful breach)	May we confirm that the unlimited number of IRs covers P1 security events only, as shown in Section A.1. Item no. 7? P1 security events refers to high severity/ impact of the security event to critical assets (e.g., active directory and business email compromise), and other events that will be agreed upon during the agency onboarding.	No
Non-Functional Requirements			
347	Non-Functional Requirements, B. Training and Other Requirements, page 103, Annex D-26 The local Service Provider must notify the agency's designated IT security personnel, who will be the point of contact for the service provider, of any related cyber security supply chain incidents such as, but not limited to compromise/breaches involving the vendor/supplier/client data, the product hardware or software, etc. It must be reported within a risk-informed time frame of at-least 24 hours upon learning of the incident. Must provide documentation on incident response handling procedure.	May we confirm that the notification for any related cyber security supply chain incidents will be limited to the data sources ingested in the SIEM? As for the "documentation on incident response handling procedure," may we confirm that this refers to the recommendation of the local Service provider on how the agencies can safeguard themselves from the specific cyber security supply chain incident?	No Yes

348	Non-Functional Requirements, B. Training and Other Requirements, page 103, Annex D-26 The local Service Provider must notify the agency's designated IT security personnel, who will be the point of contact for the service provider, of any critical security vulnerabilities, firmware upgrades, and performance patches or fixes that need to be applied. Additionally, they must provide a detailed support plan and procedure.	May we confirm that the performance assessments will be conducted on an annual basis? Furthermore, may we request for the metrics of the performance assessments?	Yes This information shall only be provided to the winning bidder.
Delivery Time/Completion			
373	Delivery Time/Completion Schedule page 110, Annex D-33 Two (2) years subscription to start upon receipt of Notice to Proceed.	This shared cybersecurity bidding comprise of 4 x agencies. As per bid documents, this will be treated as 1 x Bid for the 4 x agencies and 1 winning bidder will be declared. however. Aside from the award from the procuring entity, each agency will issue its Notice of Award, Notice to Proceed, Purchase Order and Sales Contract. Will each of the agency issue these award with the same date/timeframe? It may be of the same date and in the event that same dates are not possible, at least within the same week for all agencies? In the event that an agency (or agencies) issuance of NOA, NTP, PO, Contract is later than the other agencies, the winning bidder will consider the date when all of the agencies have issued the NOA, NTP, PO and Contract in order to facilitate the needed for the bid. Example: Agency 1 issuance of NOA, NTP, PO and contact: 03Mar25 Agency 2 issuance of NOA, NTP, PO and contact: 05Mar25	**For issuance of Bid Bulletin:** **Requirement to be changed FROM:** **Two (2) years subscription to start upon receipt of Notice to Proceed.** **TO:** **Two (2) years subscription to start upon receipt of the Notice to Proceed and acceptance of Phase 1 deliverables**

		Agency 3 issuance of NOA, NTP, PO and contact: 07Mar25 Agency 4 issuance of NOA, NTP, PO and Contract: 28Mar25 The winning bidder will commence on 28Mar25 for all of the agencies as this is the final award and all 4 x agencies will have the same start and end date	
374	Delivery Time/Completion Schedule page 110, Annex D-33 The Project must be implemented by phases: Phase 1 - Threat Intelligence and Incident Response within five (5) calendar days, Phase 2 – Security Monitoring and Management with ten (10) calendar days, Phase 3 - Vulnerability Management and Penetration Testing within fifteen (15) calendar days. Commencement date will be from the receipt of Notice to Proceed (NTP) by the winning bidder. The service provider must therefore provide a project schedule which should present the project milestones and deliverables at each milestone. All deliverables shall become the property of the concerned agencies.	During the pre-bid, it was confirmed if this is for hardware only to which the TWG responded Yes. In the statement, "All deliverables shall become the property of the concerned agencies," may we reconfirm in writing that this provision specifically applies only to the hardware? The solution includes both hardware and software/cloud subscriptions, and we would like to clarify that only the hardware will become the property or ownership of the agency.	Except for subscriptions, anything that contain the agencies' data, including hardware will become the property of the agency.