

---

# **SHARED CYBERDEFENSE SOLUTION**

## **Terms of Reference (GFI Cluster)**

**Version Number** : 2.0

**Final as of** : 19 January 2022

**Author** : Land Bank of the Philippines  
Development Bank of the Philippines  
United Coconut Planters Bank  
Philippine Guarantee Corporation  
Home Development Mutual Fund

---

## 1. Name and Description of the Project

With the continued evolving nature of cybersecurity risks, the Secretary of Finance has mandated the Government-Owned and Controlled Corporations (GOCCs) / 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 GOCC and Insurance Clusters, under the Department of Finance (DOF).

For this Terms of Reference (TOR), it will cover the GOCC Cluster composed of Land Bank of the Philippines (LBP), Development Bank of the Philippines (DBP), United Coconut Planters Bank (UCPB), Home Development 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 – 7,600, DBP – 5,000, UCPB – 6,000, HDMF – 10,000, 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)

The GFI cluster shall be procured in one lot which shall consist of sublots per agency. Likewise, this shall be the basis for awarding per agency.

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

### Other Requirements

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

### 3. Functional and Non-Functional Requirements

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

#### I. Functional Requirements

A. Security Monitoring and Management	COMPLIED	REMARKS																																							
<b>A.1 Security Operations Center (SOC)</b>	<b>Y/N</b>																																								
1. The SOC shall detect and monitor threats, correlate with threat intelligence sources, generate alerts, conduct investigation, and escalate tickets to the agencies on a 24x7x365 basis, using the SOC platform provisioned for the agencies.																																									
2. The service provider should have a 24 x 7 x 365 SOC with L1, L2 and L3 support.																																									
3. 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.																																									
4. There must be a proper onboarding and integration period between the service provider and the agencies prior to full SOC operation to ensure completeness of SOC visibility and familiarization with the agencies' processes and network behavior.																																									
5. The solution shall have its own ticketing tool for incident ticket escalation and management																																									
6. 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 border="1" data-bbox="164 1230 1042 1411"> <thead> <tr> <th colspan="2"></th> <th colspan="4">Impact</th> <th></th> </tr> <tr> <th colspan="2">Response Time</th> <th>High</th> <th>Medium</th> <th>Low</th> <th>Very Low</th> <th>Report Time</th> </tr> </thead> <tbody> <tr> <th rowspan="4">Priority</th> <td>Within 2 hours</td> <td>P1</td> <td>P2</td> <td>P2</td> <td>P3</td> <td>within 15 minutes</td> </tr> <tr> <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>Within 24 hours</td> <td>P2</td> <td>P3</td> <td>P3</td> <td>P4</td> <td>N/A</td> </tr> <tr> <td>24 hours</td> <td>P3</td> <td>P3</td> <td>P4</td> <td>P4</td> <td>N/A</td> </tr> </tbody> </table> <ul style="list-style-type: none"> <li>▪ Impact: Severity of the security event to critical assets</li> <li>▪ Priority: Based on the impact and probability (Annex A)</li> <li>▪ Nature of threat</li> <li>▪ Potential business impact</li> <li>▪ Remediation recommendations</li> </ul> <p><i>Response Time: How soon the security incident must be acknowledged</i></p> <p><i>Report Time: How soon a reference number/ problem ticket must be created by the service provider and received by the agency. The Report Time is included in the Response Time.</i></p>			Impact					Response Time		High	Medium	Low	Very Low	Report Time	Priority	Within 2 hours	P1	P2	P2	P3	within 15 minutes	Within 12 hours	P2	P2	P3	P4	within 30 minutes	Within 24 hours	P2	P3	P3	P4	N/A	24 hours	P3	P3	P4	P4	N/A		
		Impact																																							
Response Time		High	Medium	Low	Very Low	Report Time																																			
Priority	Within 2 hours	P1	P2	P2	P3	within 15 minutes																																			
	Within 12 hours	P2	P2	P3	P4	within 30 minutes																																			
	Within 24 hours	P2	P3	P3	P4	N/A																																			
	24 hours	P3	P3	P4	P4	N/A																																			
7. Monthly monitoring service management:																																									

<p>The service provider shall conduct regular meetings with the agencies' IT stakeholders to review SOC performance and discuss the overall IT security posture of the agencies, including fine-tuning of configurations and provision of best practices advice, to aid in continuous improvement. Regular written reports must also be available to track the status of cases and the assistance needed. Monthly reports shall contain, but not limited to:</p> <ul style="list-style-type: none"> <li>• SLA Performance</li> <li>• Correlated Events Overview</li> <li>• Correlated Events Graph Distribution Overtime</li> <li>• Correlated Events and Rules Triggered Summary</li> <li>• Summary of Incident Ticket per Use Cases Incident Management</li> </ul>		
<p>8. The service provider shall facilitate SOC security briefing at least once a month for the agencies to present the latest local and international news and updates in Cyber security.</p>		
<p><b>A.2 Managed Detection and Response</b></p>	<p>COMPLIED</p>	<p>REMARKS</p>
<p><b>A.2.1 Deployment and Management</b></p>	<p>Y/N</p>	
<p>1. The solution is capable to deploy endpoint technology to workstations and servers, including all versions of Windows, Mac, Unix and Linux assets.</p>		
<p>2. The solution works in a Virtual Desktop Infrastructure (VDI) environment.</p>		
<p>3. The solution shall support Endpoint Detection and Response (EDR) functionality on Windows, Linux, Unix, and Mac Operating System (OS).</p>		
<p>4. The solution shall detect and prevent attacks within the OS instances / workloads in public clouds such as Amazon Web Services (AWS), Azure, and Google.</p>		
<p>5. The solution shall not require reboot during installation, enabling, and updating of Endpoint Protection, EDR or any malware prevention modules.</p>		
<p>6. The solution shall utilize Central Processing Unit (CPU) (1-2%), Random Access Memory (RAM) and fixed disk at low levels.</p>		
<p>7. The solution shall have an endpoint technology console protected by two-factor authentication (2FA).</p>		
<p>8. The solution shall support IT Hygiene and Vulnerability Management without need to deploy additional agents.</p>		
<p>9. All modules within the solution shall not be dependent on any whitelisting, which includes Endpoint Protection, EDR and IT Hygiene.</p>		
<p>10. Endpoint Protection, machine learning, behavior analytics and EDR including the remote response should be part of a one single agent and should not require multiple agent deployment. In the system process tree, the modules should not show multiple process entries.</p>		
<p>11. The solution shall provide all the functionalities including Prevention, Detection and Remote Response Remediation using the same agent and same management console.</p>		

12. The solution should support EDR for Mobile supporting Android and IOS from the same platform and without installing any additional management infrastructure		
13. 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.		
14. The solution shall have support for Desktop Firewall Management.		
15. The solution shall have support for Universal Serial Bus (USB) device control policies.		
16. The solution must be able to conduct a continuous compromise assessment, which shall include at the minimum: <ul style="list-style-type: none"> <li>▪ Identification of the specific vulnerabilities and/or compromised assets</li> <li>▪ Evaluation of scanned assets and identification of possible vulnerability linkages through a detailed analysis of the results</li> <li>▪ Update of Indicators of Compromise (IOC) and watchlist repository, whenever applicable</li> </ul>		

<b>A.2.2 Prevention</b>	COMPLIED Y/N	REMARKS
1. Endpoint Security should not require any signatures to protect known and unknown attacks. It should be 100% based on Machine Learning and Behavior Patterns. Endpoint security should be owned by the service provider and not by a third party.		
2. Machine Learning and Behavior IOA patterns should have support for Windows, Mac, Unix, and Linux and other non-supported or legacy endpoints.		
3. The solution must be able to block the following:		
• exploitation behavior using IOAs and no signatures.		
• ransomware behavior using Behavior IOA patterns and no signatures.		
• file-less malware using Behavior IOA patterns.		
• malware-free tradecraft using Behavior IOA patterns.		
4. Endpoint Security should show the number of other Anti-Virus/Endpoint Security detecting the same file on the same detection window.		
5. Endpoint Security should support Firmware Analysis to detect BIOS level attacks.		
<b>A.2.3 Detection</b>	COMPLIED Y/N	REMARKS
1. The solution must be able to View the following:		
• alerts centrally in the UI		
• alerts associated activity in the UI		
• interactive process trees for alerts detections		

<ul style="list-style-type: none"> <li>Process tree events coming into UI in a near real time for the detected events</li> </ul>		
<ul style="list-style-type: none"> <li>System, user, and per process real-time forensics of an alert</li> </ul>		
<ul style="list-style-type: none"> <li>full execution details including paths, hashes, timestamps, and command lines</li> </ul>		
<ul style="list-style-type: none"> <li>disk I/O activity of processes including reads and writes</li> </ul>		
<ul style="list-style-type: none"> <li>network connectivity of processes</li> </ul>		
<ul style="list-style-type: none"> <li>DNS Lookups that are captured for each process and not per client</li> </ul>		
2. The solution must be able to generate an intelligence driven detection in the UI.		
3. The solution must be able to enrich a detected event with its own threat intelligence and not any third-party Intelligence.		
4. The Threat Intelligence service as part of the MDR shall be a leading threat intelligence in any of the third-party analyst report.		
5. Should be a tested solution by MITRE against its ATT@CK Framework		
6. Should be able to associate detected events using the MITRE ATT@CK Framework Tactic & Technique		
7. Should be able to manage workflows including sorting, filtering, tracking status, assigning ownership, and creating commentary or annotations of alerts		
8. Should be able to detect advanced tradecraft and activity across the kill-chain including Exploitation, Execution, Privilege Escalation, Social Engineering, Credential Theft, Persistence, Exfiltration, Actions on Objectives, among others		
9. Should be able to detect attacks using file-less and malware-less tools such as PowerShell		
10. Should provide out-of-the-box Zero Trust Assessment dashboard showcasing the OS and Endpoint protection configuration		
<b>A.2.4 Threat Hunting</b>	<b>COMPLIED Y/N</b>	<b>REMARKS</b>
1. Must have a 24X7x365 Managed Threat Hunting Service		
2. Must have pre-built hunting applications and pre-made queries		
3. Must be able to pivot to Events directly from an alert for additional raw data		
4. Must be able to pivot to Events from results retrieved from the pre-built hunting application for additional raw data		
5. Must be able to search for a MD5 or SHA256 file hash to show historical data about its execution		
6. Must be able to search for a host name to show activity collected about that host historically (Including RAW Data)		

7. Must be able to search for a username to show activity by that user historically (Including RAW Data)		
8. Must be able to search for a domain to show historical data about its use		
9. Must be able to search for events associated with unique visibility including account creation, login activity, local firewall modification, service modification, sources of remote operations (including scheduled task creations, registry changes, WMIC execution, among others)		
10. Must be able to hunt events for an offline machine in near real time before it went offline		
11. Must be able to run a simple search for any string such as, but not limited to, domain.com, 192.x.x.x, powershell.exe, among others (including RAW Data Search)		
12. Must be able to run custom queries as needed for validation		
13. Must be able to pivot from one event to additional related events		
14. Must be able to pivot from an event to find its parent, child, and sibling processes (ancestry)		
15. Must be able to pivot from a single event to an interactive process tree		
16. Must be able to search on all this data within the retention period regardless if PC is online/offline		
17. Must be able to export any results for further analysis		
18. Managed Threat Hunting Service should be from EDR service provider itself and not from any 3rd Party Services		
19. The MDR solution must have been in the industry for at least 5 years		
20. Service Provider should have experience with their own MDR offering for more than five (5) years		
21. The solution should be supported by experienced and certified Incident Responders to perform 24X7x365 remote response for Endpoint Incidents/Events		
22. The solution must be supported by the service provider's own Threat Intelligence Team		
<b>A.2.5 Response</b>	<b>COMPLIED Y/N</b>	<b>REMARKS</b>
1. Remote Response by administrators such as containment, deleting files, killing process among others should not require any additional agent and should be performed using the same EDR <sup>1</sup> agent		
2. Connection to remote host should be supported for Windows, Mac, Unix and Linux		
3. Must be able to network contain a host (Windows, Mac and Linux, Unix) directly from a detection window		

<sup>1</sup> Service provider shall use the existing subscription of agencies that have the exact same EDR solution already in place

4. Must be able to show all endpoints that are currently in a network contained state		
5. Must be able to view the amount of time required to network contain and lift containment		
6. Must be able to manage whitelisted IP addresses for network containment		
7. Must be able to blacklist file hashes through the UI		
8. Must be able to view and preserve containment and blacklists across reboots		
9. Must be able to view containment action audit logs		
10. Should support execution of custom Powershell Scripts as a part of remote response action		
<b>A.2.6 API and Platform Integration</b>	COMPLIED Y/N	REMARKS
1. Must be able to setup real-time streaming of alerts via API and/or SIEM integration		
2. Must be able to search for IOCs via API		
3. Must be able to navigate process trees via API		
4. Must be able to query device status via API including OS, version, first seen, last seen		
5. Must be able to ingest external IOCs via API		
6. Must be able to export all raw sensor data		
7. Must be able to share the RAW endpoint events to each agency's data lake		
<b>A.2.7 Third Party Validation</b>	COMPLIED Y/N	REMARKS
1. The solution should be leader in both Endpoint Point Protection and EDR as per latest Forrester Report		
2. The solution should be leader in the latest Gartner's Magic Quadrant for EPP		
<b>A.3 Security Information and Event Management (SIEM)</b>	COMPLIED Y/N	REMARKS
1. 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.		
2. 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.		
3. The service provider shall ensure availability of searchable raw logs for at least twelve (12) months with comprehensive searchability. The retention of the logs shall be within the duration of the contract, after which, the logs will be archived and given to the agencies in an agreed format. The logs, including evidences of security incidents, should be tamper proof and made available for legal and regulatory purposes, as required.		



4. The service provider's SIEM shall provide for flexibility and scalability for the agencies' current and future needs.		
5. 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.		
6. 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.		
7. 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: <ul style="list-style-type: none"> <li>- The source or destination IP address</li> <li>- Identity context</li> <li>- The hostname or service being used</li> <li>- Network topological information</li> <li>- Policy and privacy information</li> </ul>		
8. 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.		
9. 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: <ul style="list-style-type: none"> <li>- firewalls</li> <li>- VPN</li> <li>- switches</li> <li>- routers</li> <li>- authentication systems</li> <li>- servers</li> </ul>		
10. 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.		
11. 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.		
12. The SIEM solution must allow administrator to check new attacks and vulnerabilities against history to detect past events		
13. 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		
14. 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		
15. 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		

16. The SIEM solution must be able to do Risk-base and Rule-base correlation		
17. The SIEM solution must have an advanced correlation engine solution that can be deployed in either real time or historical modes.		
18. 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..)		
19. 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.		
20. 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.		
21. The SIEM Manager must provide an intuitive and easy to learn graphical interface for building of custom correlation rules		
22. The SIEM solution must provide means to create reports based on collected and correlated data.		
23. 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		
24. The SIEM reports must be exported to PDF, MS Excel/CSV file and HTML		
25. The SIEM reports must be automatically generated based on defined criteria and sent to email address		
26. 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		
27. 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.)		
<b>A.4 Security Orchestration, Automation and Response (SOAR)</b>	COMPLIED Y/N	REMARKS

1. The SOAR solution must be able to fully orchestrate security operations and provide security teams with case management, automation, and investigation within a single pane of glass		
2. The SOAR solution must have visibility into the security operation provided via dashboards, KPIs and customizable reporting		
3. The SOAR solution must be able to support machine driven and analyst led response to remediate threats in a consistent and auditable manner		
4. 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		
5. The SOAR solution must render alerts, cases, query reports, and events into clustered and contextualized threat storylines with a high degree of visualization		
6. 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.		
7. The SOAR solution must be able to provide plugins for non technology partners		
8. The SOAR solution must be able to identify significant cases, clustering them with related threat indicators to prioritize a threat.		
9. The SOAR solution must have access right mechanisms		
10. 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		
11. The SOAR solution must have collaboration functionalities in the platform.		
12. The SOAR solution must have some Machine learning recommendation capabilities		
13. The SOAR solution must have crisis/emergency management capabilities		
14. 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		
15. 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		
16. The SOAR solution must be able to accelerate all processes by automating or semi automating workflows		
17. The SOAR solution must be able to build custom playbook by intuitively dragging and dropping actions, triggers and logical operators.		
18. The SOAR solution must be able to develop playbooks of best practices to scale operations, drive consistency in response and meet compliance requirements.		
19. The SOAR solution must provide extensive library of pre-defined playbooks to various types of threat:		

• 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]		

<ul style="list-style-type: none"> <li>• Login 1 to many: Login attempt from 1 station to more than 2 accounts</li> </ul>		
<ul style="list-style-type: none"> <li>• Login at off hours Night: Admin login in non-working hours (customizable)</li> </ul>		
<ul style="list-style-type: none"> <li>• Login more than 2 to 1: Login attempt from 3 stations to 1 account</li> </ul>		
<ul style="list-style-type: none"> <li>• Login Root: Login Directly to Root and not via "SU"</li> </ul>		
<ul style="list-style-type: none"> <li>• Malware Infections</li> </ul>		
<ul style="list-style-type: none"> <li>• Multiple Account Locking: Multiple locked accounts from same source IP</li> </ul>		
<ul style="list-style-type: none"> <li>• Multiple changes from administrative accounts</li> </ul>		
<ul style="list-style-type: none"> <li>• Same account different countries within 5 days (user traveled abroad)</li> </ul>		
<ul style="list-style-type: none"> <li>• SMTP traffic from an unauthorized host.</li> </ul>		
<ul style="list-style-type: none"> <li>• Privilege Elevation: Permissions were changes from user to Admin</li> </ul>		
<ul style="list-style-type: none"> <li>• Threat Intel Feed: IOCs detection</li> </ul>		
<ul style="list-style-type: none"> <li>• Trojan Infection</li> </ul>		
<ul style="list-style-type: none"> <li>• Virus Found</li> </ul>		
<ul style="list-style-type: none"> <li>• Vulnerable Software Version Detected</li> </ul>		
20. The SOAR solution must be able to provide the needed business intelligence capabilities to present current workload, capacity, and effectiveness of security operations.		
21. The SOAR solution must be highly flexible, providing customizable dashboards that highlight most relevant insights for on-going improvement.		
22. The SOAR solution should provide pre-set (and customizable) KPI metrics to monitor threat response efficacy and team performance.		
23. The SOAR solution should provide integrated BI platform to help create advanced dashboards and reports based on KPI's to be tracked		
24. The SOAR solution must have presentable dashboards with customization, reporting, scheduling and report distribution capabilities.		
25. The SOAR solution must provide built-in reports provide executive level and detailed technical reporting out of the box		
26. The SOAR solution must be able to provide customizable reports at the click of a button for		

any event or case.		
27. The SOAR solution must be able to automate the reporting process to routinely deliver standard and customized reports		
28. The SOAR solution must be able to cater to the demands of different audiences within the organization with powerful templating engine.		

<b>B. Vulnerability Management and Penetration Testing</b>		
<b>B.1 Vulnerability Management</b>	COMPLIED Y/N	REMARKS
1. The solution must be a cloud-based offering but supports on-premise scanners		
2. The solution must fully integrate vulnerability assessment (scanning) and security configuration assessment to include combined licensing and consolidation of data, analysis, and querying.		
3. The solution must include an integrated active/passive scanning capability for full visibility of assets, vulnerabilities, and configurations.		
4. The solution must offer predictive prioritization of remediation based on business risk.		
5. 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.		
6. The solution's offering must include 24/7/365 global technical support.		
7. The solution must receive new vulnerability detections/checks and does not rely on 3rd party data set		
8. The solution must not rely on IP Addresses as the only means to track an asset.		
9. 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.		
10. The solution must provide an elastic licensing model to ensure the product continues to function without interruption when the license limit is temporarily exceeded.		
11. The solution must provide an integrated storage model that does not rely on a third-party database product.		
12. 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.		
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.		
14. The solution must provide a comprehensive and fully documented API for automation of processes and integration with 3rd party applications.		
15. The solution must scale to millions of assets.		

16. The solution must include the option for agents that provide vulnerability assessment and security configuration assessment.		
17. The solution must be able to use groups of scanners in a single job.		
18. The solution must be able to scan assets on customers' internal networks as well as assets which are external facing / publicly accessible.		
19. Scanners must be managed by the platform, e.g., updates to vulnerability detections, code, and other updates.		
20. The solution must integrate with AWS SSM to derive vulnerabilities without trigger any scan from scanner or agent		
21. The solution must provide role-based access control (RBAC) to control user access to specific data sets and functionality.		
22. 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.		
23. The solution must be able to define and manage user groups, including limiting scan functions and report access.		
24. The solution must have the ability to ensure that certain IPs or ports can be blocked from scanning.		
25. The solution must support a variety of scan engine platforms to include Windows, Linux, macOS, as well as virtual-based appliances.		
26. The solution must support multiple geographically distributed scanning engines managed by a central console.		
27. The solution must include the ability to schedule scan blackout windows to prevent scanning during prohibited hours.		
28. The solution must provide the ability to configure ports, protocols, and services for connections to scanners deployed throughout the network.		
29. The solution must be configurable to allow for scan throttling to prevent generation of traffic that could disrupt normal network infrastructure.		
30. The solution must allow for entry and secure storage of user credentials, including Windows local and domain accounts, and Unix su and sudo over SSH.		
31. The solution must provide the ability to escalate privileges on target systems from normal user access to root/administrative access.		
32. The solution must support customized scan scheduling, including the ability to have scans run at designated times, with predetermined frequency.		
33. The solution must be able to perform sensitive data searches to discover sensitive data at rest on all versions of Windows, Unix and Linux systems.		
34. The solution must be able to offer centralized scan and scan policy management.		

35. The solution must provide for an “auto-aging” license model to ensure stale or retired assets no longer count against the license.		
36. The solution must support an asset discovery capability that does not count against licensing.		
37. The solution must provide a passive network monitoring capability for asset discovery.		
38. 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.		
39. The solution must be able to discover mobile devices and integrate with several different Mobile Device Management Systems (MDMs).		
40. The solution must provide integrated web and database service discovery.		
41. The solution must be capable of detecting services that are running on non-standard ports.		
42. The solution must be capable of detecting services configured not to display connection banners.		
43. The solution must be capable of testing multiple instances of the same service running on different ports.		
44. The solution must be capable of scanning dead hosts (devices which do not respond to ping).		
45. The solution must support the optional use of netstat for rapid and accurate enumeration of open ports on a system when credentials are supplied.		
46. The solution must support the use of SMB and WMI for scanning Windows systems.		
47. 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.		
48. The solution must support secure shell (SSH) with the ability to escalate privileges for vulnerability scans and configuration audits on Unix systems.		
49. The solution must provide the ability to tune scan policies for minimal impact on networks and targets.		
50. The solution must provide active and passive discovery of wireless access points (WAPs).		
51. The solution must provide both authenticated and non-authenticated network-based scanning of target systems.		
52. The solution must not rely on any third-party scanners for vulnerability scanning, compliance auditing / security configuration assessment.		
53. 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.		
54. The solution must be capable of agent testing for local vulnerability detection at no		



additional charge.		
55. The solution must provide an externally hosted scanning service for scanning perimeter networks.		
56. The solution must be capable of tracking DHCP changes by associating scan results of a given system with something other than the IP address.		
57. 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.		
58. The solution must be CVE compatible and provide at least 10 years of CVE coverage.		
59. The solution must provide patch auditing for 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, and more.		
60. The solution must provide patch auditing for all Unix operating systems to include macOS, Linux (multiple distributions), Solaris, IBM AIX, HP-UX, and more.		
61. The solution must provide coverage for third-party applications such as Java and Adobe.		
62. 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.		
63. 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.		
64. 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.		
65. 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).		
66. The solution must also include vulnerability scoring according to the Common Vulnerability Scoring System Version 3 (CVSS v3).		
67. The solution must provide vulnerability exploitability information from 3rd party sources such as Core Impact, Metasploit, and Canvas.		
68. 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.		
69. The solution must intelligently select vulnerability and configuration tests for a given asset based on information gained from initial scans of that asset.		
70. The solution must track dates for vulnerability discovery and observation that can be used in		

filtering and reporting in time-based filters.		
71. The solution must not be dependent on operating system ability to schedule tasks.		
72. The solution must support IPv6 scanning, with passive discovery of IPv6 targets.		
73. The solution must assess public cloud assets for misconfigurations and vulnerabilities via active scanning and agents.		
74. The solution must accurately track assets and their vulnerabilities, including highly dynamic IT assets like mobile devices, virtual machines, and cloud instances.		
75. 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.		
76. 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.		
77. The solution must optionally have the ability to support an unlimited number of quarterly PCI attestations.		
78. The solution must be able to support multiple PCI assets.		
79. The solution must have the ability to periodically change the designated PCI assets.		
80. The solution must be capable of agentless compliance auditing without the need for a client-side agent installed on the target device.		
81. The solution must provide security and configuration auditing benchmarks for regulatory compliance standards and other industry and service provider best practice standards.		
82. The solution must provide security and configuration auditing benchmarks for service provider best practices such as Microsoft, Linux, MDM solutions such as VMware AirWatch, routers and switches, firewalls, etc.		
83. The solution must provide auditing of the following for security and configuration settings:		
<ul style="list-style-type: none"> <li>• All Microsoft operating systems</li> </ul>		
<ul style="list-style-type: none"> <li>• All Linux/Unix operating systems</li> </ul>		
<ul style="list-style-type: none"> <li>• All types and versions of databases</li> </ul>		
<ul style="list-style-type: none"> <li>• Agency applications</li> </ul>		
<ul style="list-style-type: none"> <li>• Network infrastructure</li> </ul>		
<ul style="list-style-type: none"> <li>• Mobile device management</li> </ul>		
<ul style="list-style-type: none"> <li>• Public cloud (e.g., AWS, Microsoft Azure, Salesforce) and cloud-native infrastructure (e.g., Docker, Kubernetes)</li> </ul>		
<ul style="list-style-type: none"> <li>• Specific endpoint security products for installation and boot status.</li> </ul>		

<ul style="list-style-type: none"> <li>Personally identifiable information (PII) and other sensitive content.</li> </ul>		
84. The solution must allow audit policies to be customizable for organizational specific needs.		
85. The solution must provide CIS Certified Benchmarks.		
86. The solution must offer SCAP support.		
87. The solution must aggregate the results of individual scans into cumulative vulnerability views with filtering and analysis to allow drilldown and pivot capabilities.		
88. The solution must have the ability to flag a vulnerability as having been previously resolved.		
89. The solution must provide comprehensive filtering of aggregate vulnerability results with drilldown capabilities.		
90. The solution must provide the ability to automate reporting by being able to schedule reports.		
91. The solution must provide the ability to produce ad hoc reports while viewing results in the console.		
92. The service provider shall be capable to generate multi-format reports, including exporting of report data in PDF, Microsoft Excel, XML, CSV, and HTML.		
93. The reports must have the ability to include hostnames (NetBIOS, DNS) along with IP addresses.		
94. The solution must include customizable graphical and list-based dashboard elements for displaying vulnerabilities and status of the assessed environment.		
95. The solution must encrypt data at rest using at least one level of AES-256 encryption.		
96. The solution must encrypt data in transit using TLS v1.2 with a 4096-bit key.		
97. The solution must support Single sign-on (SSO) authentication methods.		
98. The solution product must be able to partition/segregate data for one customer from data for other customers.		
<b>B.2 Vulnerability Assessment and Penetration Testing (VAPT)</b>	<b>COMPLIED Y/N</b>	<b>REMARKS</b>
1. The engagement shall cover quarterly vulnerability assessment and penetration testing for a minimum of fifteen (15) websites identified by each agency		
2. The service provider shall perform common service discovery and fingerprinting functionalities for the following, whether on-premise or cloud-based:		
<ul style="list-style-type: none"> <li>Application servers</li> </ul>		
<ul style="list-style-type: none"> <li>Authentication servers</li> </ul>		
<ul style="list-style-type: none"> <li>Backdoors and remote access services</li> </ul>		
<ul style="list-style-type: none"> <li>Backup applications/tools</li> </ul>		

<ul style="list-style-type: none"> <li>• Database servers</li> </ul>		
<ul style="list-style-type: none"> <li>• Active Directory, Lightweight Directory Access Protocol (LDAP)</li> </ul>		
<ul style="list-style-type: none"> <li>• Domain Name Systems (DNS)</li> </ul>		
<ul style="list-style-type: none"> <li>• Mail servers and Simple Mail Transfer Protocols (SMTP)</li> </ul>		
<ul style="list-style-type: none"> <li>• Network File Systems (NFS), Network Basic Input/Output System (NetBIOS) and Common Internet File Systems (CIFS)</li> </ul>		
<ul style="list-style-type: none"> <li>• Network Time Protocols (NTP)</li> </ul>		
<ul style="list-style-type: none"> <li>• Point Of Sale (POS) Applications</li> </ul>		
<ul style="list-style-type: none"> <li>• Remote Procedure Calls</li> </ul>		
<ul style="list-style-type: none"> <li>• Routing protocols</li> </ul>		
<ul style="list-style-type: none"> <li>• Simple Network Monitoring Protocol (SNMP)</li> </ul>		
<ul style="list-style-type: none"> <li>• Telecommunications Network (TelNet), Trivial File Transfer Protocol (TFTP), Secure Shell (SSH)</li> </ul>		
<ul style="list-style-type: none"> <li>• Virtual Private Network (VPN)</li> </ul>		
<ul style="list-style-type: none"> <li>• Web and mobile applications</li> </ul>		
<ul style="list-style-type: none"> <li>• Web servers</li> </ul>		
<p>3. Each VAPT run shall include:</p> <ul style="list-style-type: none"> <li>• Presentation of identified vulnerabilities and recommended remediation</li> </ul>		
<ul style="list-style-type: none"> <li>• Formal report for the conducted VAPT activity</li> </ul>		
<ul style="list-style-type: none"> <li>• Validation run to verify implemented remediation of identified vulnerabilities</li> </ul>		
<p>4. The engagement shall include the following activities:</p>		
<p>a. Planning of activities and timelines to be agreed with agencies</p>		
<p>b. Vulnerability assessment of the identified websites</p>		
<p>c. Penetration testing of the identified websites</p>		
<p>d. Automated and manual testing of discovered vulnerabilities which includes the following:</p>		
<ul style="list-style-type: none"> <li>▪ SQL Injection</li> </ul>		
<ul style="list-style-type: none"> <li>▪ SQL injection (Boolean)</li> </ul>		
<ul style="list-style-type: none"> <li>▪ SQL Injection (Blind)</li> </ul>		
<ul style="list-style-type: none"> <li>▪ Cross-site Scripting</li> </ul>		
<ul style="list-style-type: none"> <li>▪ Command Injection</li> </ul>		

▪ 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.		
5. 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>C. Threat Intelligence</b>	<b>COMPLIED</b>	<b>REMARKS</b>
1. The solutions shall deliver threat intelligence such as but not limited to 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		
2. The threat intelligence solution must, at minimally, harvest data from the following open, technical and closed source 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)		

<ul style="list-style-type: none"> <li>• Dark Web (including multiple tiers of underground communities and marketplaces)</li> </ul>		
<ul style="list-style-type: none"> <li>• Original research from in-house human intelligence analysts</li> </ul>		
3. The threat intelligence solution must be able to:		
<ul style="list-style-type: none"> <li>• Detect and take down servers launching phishing attacks</li> </ul>		
<ul style="list-style-type: none"> <li>• Identify fraudulent social media accounts that are impersonating the Government Agencies and its executives</li> </ul>		
<ul style="list-style-type: none"> <li>• Take down of fake applications that impersonate legitimate ones from app stores.</li> </ul>		
<ul style="list-style-type: none"> <li>• 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.</li> </ul>		
4. The solution shall be capable to detect leaked Personally Identifiable Information (PIIs) and the agencies' information from the deep and dark web, social media, and other forms of instant messaging platforms and provide recommended action plan.		
5. The 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.		
6. The solution shall monitor the domains and IP addresses that have bad reputation.		
7. 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.		
8. 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		
9. The threat intelligence solution must have at least 10 years of historical data and should be included in real time query results in its portal with event details.		
10. The threat intelligence solution must be capable of deduplicating multiple references or mentions of the same threat indicators, links or social media accounts.		
11. The threat intelligence solution must be able to collect data across all countries and industries.		
12. The threat intelligence solution must provide and display information in near real-time as new information or context is gathered from various sources.		
13. The threat intelligence solution must provide IOC with dynamic risk score.		
<ul style="list-style-type: none"> <li>• 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).</li> </ul>		

<ul style="list-style-type: none"> <li>• Scores must be dynamic to represent the real-time risk of the said IOC, aging of score that commensurate with current risk posture of IOC must be provided.</li> </ul>		
<ul style="list-style-type: none"> <li>• 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</li> </ul>		
14. 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.		
15. 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.		
16. 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.		
17. The threat intelligence solution must be able to support analysis with:		
<ul style="list-style-type: none"> <li>• Real-time trends and developments</li> </ul>		
<ul style="list-style-type: none"> <li>• Historical view of related events</li> </ul>		
<ul style="list-style-type: none"> <li>• Reported roles involved in the events (attackers/threat actors, targets/organizations)</li> </ul>		
<ul style="list-style-type: none"> <li>• Reported TTPs (attack vectors, malware, exploits)</li> </ul>		
<ul style="list-style-type: none"> <li>• Reported indicators (IP addresses, domains, hashes, URLs etc.)</li> </ul>		
<ul style="list-style-type: none"> <li>• Related operations</li> </ul>		
<ul style="list-style-type: none"> <li>• Access to the original references with cached content for the volatile ones</li> </ul>		
<ul style="list-style-type: none"> <li>• Other contextual details about the events</li> </ul>		
18. 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).		
19. The threat intelligence solution must provide nontechnical data/information/intelligence related to threat actor, attack campaign, analysis report, tactics, techniques, and protocols (TTPs)		
20. The threat intelligence solution must allow end user expert analysts within the organization to collaborate by adding notes or cross-referencing indicators.		
21. 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.		
22. The threat intelligence solution must provide Risk Score for Vulnerability which are Pre-NVD (No CVSS score upon release)		
23. 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.		



24. The threat intelligence solution must allow users to provide instant feedback via the user interface to request for data review or validation.		
25. 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.		
26. The threat intelligence solution must include exportable/integrated data via the following formats:		
<ul style="list-style-type: none"> <li>Machine readable feeds, available as CSV or STIX files, and containing high-risk indicators with supporting evidence that are accessible by end-users,</li> </ul>		
<ul style="list-style-type: none"> <li>Human readable finished intelligence reports written on-demand or on a regular basis; reports are "live" and have references to the latest intelligence.</li> </ul>		
27. The threat intelligence solution must provide both Portal (web browser) and Mobile App access.		
28. The threat intelligence solution must be able to provide alerts to respective authorities via portal, email, feeds & mobile app.		
29. The threat intelligence solution must provide the cyber security news on a daily basis and its analyzed point of view. This must be delivered via email daily		
30. The threat intelligence solution must also be able to offer takedown services from the portal as required by each agency. The solution should support takedown for Websites, Domains, Fake Ads, Social Media impersonating accounts, Fake Apps on App Store etc.		
31. 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		
32. 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.		
33. 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		
34. 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		
35. The threat intelligence solution must be able to perform industry peer comparison and ability to trend attack methods (e.g., track new phishing malware)		

<b>D. Incident Response</b>	<b>COMPLIED Y/N</b>	<b>REMARKS</b>
1. The service provider shall review the agencies' Incident Response Plan (IRP), which would guide the agencies on the creation, enhancement, and documentation of		

<p>incident response playbooks, policies, and guidelines, such as, but not limited to:</p> <ul style="list-style-type: none"> <li>• Escalation process</li> <li>• Incident containment process</li> <li>• Incident eradication process</li> <li>• Incident recovery process</li> <li>• Incident identification process</li> <li>• Process flow</li> </ul>		
<p>2. The service provider shall act as the Incident Response (IR) Manager and facilitate the six (6) phases of IR. The service provider must be on-call and will conduct the IR activities onsite, as necessary (i.e., in cases of breach). The IRs per agency shall cover 200 accumulated hours per year. Beyond the required 200 hours, the Government Agencies shall shoulder the cost. In case the 200 hours allotted for IR is not fully or not consumed, it can be converted to other services, such as training among others, that the provider can render for information security.</p>		
<p>3. The service provider shall conduct an annual, or as needed, IR readiness training to the agencies' Computer Security Incident Response Teams (CSIRT), including IT security awareness trainings to both technical and non-technical audiences of the agencies. The readiness training shall include best practices recommendation in isolation, containment, and remediation activities of the security incident.</p>		
<p>4. The service provider shall conduct an annual, or as needed, incident response drill or simulation exercises with the agencies-CSIRTs to improve detection and internal readiness for cyber security incidents. This will include internal and external incident communications, reduced impact on operation continuity, reporting to regulators (e.g., NPC, BSP), CSIRT readiness, blue team capability, tabletop exercises, among others.</p>		
<p>5. The Service Provider shall map security playbook and runbooks for applicable security use cases to guide client on their incident response.</p>		
<p>6. The service provider shall deliver technical assistance to the agencies-CSIRTs during emergency (successful) breach response.</p>		
<p>7. The Service Provider shall have a facility to receive client's reported incident (via authorized point of contact from client) for incidents not captured on the monitoring tool.</p>		
<p>8. The service provider shall deliver network/firewall/web applications breach response.</p>		
<p>9. The service provider shall identify, cleanse or contain malicious code, malware, spyware, and system-file hacks.</p>		
<p>10. The service provider shall deliver root cause analysis to identify the intrusion vector and provide mitigating procedures to address network and system vulnerabilities.</p>		
<p>11. The service provider shall identify indicators of compromise and scan the network to search for other related infected systems.</p>		
<p>12. The service provider shall deliver insider threat investigation, as needed.</p>		
<p>13. The service provider shall deliver employee misconduct investigations, as needed.</p>		
<p>14. The service provider shall deliver incident and investigation reports.</p>		

15. The service provider shall have a certified and recently trained (at least in the past 12 months) in-house cyber security forensics specialist, to support advanced investigation.		
16. The service provider shall assist in the following: <ul style="list-style-type: none"> <li>• Incident handling preparation and execution</li> <li>• Crisis management</li> <li>• Breach communication</li> <li>• Forensic analysis</li> <li>• Remediation</li> </ul>		
17. The Service Provider shall rate the prioritization and severity of security incidents and create a service ticket as per agreed Service Level Agreement (SLA).		

Service Level Agreement (SLA)																												
1. Acknowledgement SLA - The Acknowledgement SLA Percentage shall be computed per month base on the total number of missed hours exceeding the Acknowledgement SLA guarantee of fifteen (15) minutes per incident																												
<table border="1"> <thead> <tr> <th>Service Level Target</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>98%</td> <td>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.</td> </tr> </tbody> </table>			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.																						
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.																											
2. Incident Response SLA - Time to respond or provide request from when incident or request is reported based on severity level.																												
<table border="1"> <thead> <tr> <th>Priority Level</th> <th>Incident Response Time</th> <th>Reference</th> </tr> </thead> <tbody> <tr> <td>P1 – Catastrophic</td> <td>Within 60 Minutes</td> <td rowspan="4">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.</td> </tr> <tr> <td>P2 – Critical</td> <td>Within 90 Minutes</td> </tr> <tr> <td>P3 – Marginal</td> <td>Within 120 Minutes</td> </tr> <tr> <td>P4 – Negligible</td> <td>Within 160 Minutes</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th colspan="4">Target Response Time % per Month</th> </tr> <tr> <th>Incident Priority</th> <th>1 and 2</th> <th>3 and 4</th> <th></th> </tr> </thead> <tbody> <tr> <td></td> <td>&gt;= 90%</td> <td>&gt;= 80%</td> <td>Sum of the # of incidents meeting required Response Time for all days in the month</td> </tr> </tbody> </table>			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		
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																									

## II. Non-functional Requirements

A. Access Management	COMPLIED Y/N	REMARKS
1. All credentials with the service provider shall be stored in a monitored central management system. These are leased to the agencies once strong authentication has been implemented and for the specific task for which it was authorized.		
2. The service provider's solution shall be accessed through a centralized portal, which		

enforces session timeouts, mandates the use of multi-factor authentication (MFA), and provides anomaly detection for monitoring user behavior.		
3. The service provider shall maintain logical access controls which are role-based, including principles of least privilege and segregation of duties.		
4. All passwords must have a minimum of twenty (20) characters. Passwords must be changed every ninety (90) days and cannot be the same as the prior three (3) passwords. The service provider's system must mask passwords when entered and store password files separately from the application system data. Only encrypted hashes of passwords may be stored and transmitted.		
5. All access from the service provider's manage endpoints to sensitive resources shall be done via VPN configured with MFA. Opportunistic Transport Layer Security (TLS) is configured by default for e-mail. Remote hardware is managed by comprehensive enterprise management software that allows for maintenance and access control management.		
6. The service provider shall provide physical and environmental controls at the primary and secondary sites for this project.		
7. The agencies' data shall be logically separated by using unique tagging to ensure segregation of data from the other agencies. The agencies should retain as the legal owner of the data processed and managed by the service provider.		

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

<b>C. Service Provider's Qualification and Requirements</b> <i>Note: Submission of required documents shall be during the submission of bids.</i>	COMPLIED Y/N	REMARKS
1. The service provider must be a certified/authorized reseller of the brand being offered. The service provider must submit current certifications from the manufacturer.		
2. The service provider must have 24 x 7 x 365 local technology operation center (SOC/NOC facilities/infrastructure and service) and support with at least 20 certified onsite support engineers within Metro Manila.		
3. 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.		
4. The service provider's SOC must be housed in a data center with TIA-942 Rated 3 Facility Certification.		
5. The service provider's SOC Analysts must have at least one or more of the following certifications: Certified Ethical Hacker (CEH), CyberSec First Responder, Security, Information Technology Infrastructure Library (ITIL), or any relevant product certification to the SIEM platform that Service Provider offer.		
6. The service provider must be at least 10 years in Security and ICT Industry and must have more than three (3) years of experience in providing SOC services. SOC must also be certified to ISO 27001:2013 Information Security Management System (ISMS).		
7. To ensure that the service provider has background skills and experienced on the security Tools of the client, the Service Provider must have at least Two (2) local Certified Network and Security Engineer on each the following security tools below: <ul style="list-style-type: none"> <li>• SOAR</li> <li>• SIEM</li> <li>• Vulnerability Management</li> <li>• Threat Intel</li> </ul>		
8. The service provider must assign a dedicated local Project Manager (PM) that oversees the project and conducts regular monthly service performance review and reporting to client's management. The service provider must submit the following and failure to submit the lists is subject for disqualification. <ul style="list-style-type: none"> <li>• Resume/CV of the PM</li> <li>• Company ID</li> <li>• Certificate of employment</li> <li>• List of projects handled by the PM for at least two (2) banks and One (1) non-bank client/s</li> <li>• End-User /Client company name of the projects handled by the PM</li> <li>• Project Name and Project Duration (Start date and end-date).</li> </ul>		
9. The monthly service performance report of the PM should contain the following:		

<ul style="list-style-type: none"> <li>• SLA Performance</li> </ul>		
<ul style="list-style-type: none"> <li>• Correlated Events Overview</li> </ul>		
<ul style="list-style-type: none"> <li>• Correlated Events Graph Distribution Overtime</li> </ul>		
<ul style="list-style-type: none"> <li>• Correlated Events and Rules Triggered Summary</li> </ul>		
<ul style="list-style-type: none"> <li>• Summary of Incident Ticket per Use Cases Incident Management</li> </ul>		
<b>Personnel Qualifications/Requirements</b>	<b>COMPLIED Y/N</b>	<b>REMARKS</b>
<p>✓ One (1) Project Manager:</p> <ul style="list-style-type: none"> <li>▪ Must be with the service provider's organization one (1) year before the bid opening</li> <li>▪ Has performed and managed three (3) engagements within the last five (5) years comparable to the proposed engagement</li> <li>▪ At least five (5) years active IT security experience</li> <li>▪ At least three (3) years SIEM or system and network administration experience.</li> <li>▪ Has any two (2) of the following unexpired professional certifications: Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), GIAC Security Essentials (GSEC), GIAC Continuous Monitoring (GMON), GIAC Certified Detection Analyst (GCDA), GIAC Web Application Penetration Tester (GWAPT), GIAC Incident Handler (GCIH), GIAC Certified Forensic Analyst (GCFA), GIAC Certified Intrusion Analyst (GCIA), Cisco Certified Network Associate (CCNA), Information Technology Infrastructure Library (ITIL), Certified Ethical Hacker (CEH), Computer Hacking Forensic Investigator (CHFI), Certified Network Defense Architect (CNDA), CyberSec First Responder (CFR), CompTIA Security+, Certified Vulnerability Assessor (CVA), Offensive Security Certified Professional (OSCP), Certified Information System Security Professional (CISSP), Global Information Assurance Certification (GIAC) Penetration Tester (GPEN), GIAC Exploit Researcher &amp; Advanced Penetration Tester (GXPN), EC-Council Licensed Penetration Tester (LPT) Master, Certified Penetration Tester (CPT), Certified Expert Penetration Tester (CEPT), Certified Mobile and Web Application Penetration Tester (CMWAPT), CompTIA PenTest+, Certified Payment Card Industry Security Implementer (CPI SI), or other security-related certifications.</li> </ul>		
<p>✓ One (1) Team Lead:</p> <ul style="list-style-type: none"> <li>▪ Must be with the service provider's organization one (1) year before the bid opening</li> <li>▪ Has functioned as lead in the performance of three (3) engagements within the last five (5) years comparable to the proposed engagement</li> <li>▪ At least five (5) years active IT security experience</li> <li>▪ At least three (3) years SIEM or system and network administration experience</li> <li>▪ Has any two (2) of the following unexpired professional certifications: CISA, CISM, GSEC, GMON, GCDA, GWAPT, GCIH, GCFA, GCIA, CCNA, ITIL, CEH, CHFI, CNDA, CFR, CompTIA Security+ CVA, OSCP, CISSP, GPEN, GXPN, LPT Master, CPT, CEPT, CMWAPT, CompTIA PenTest+, CPI SI, or other security-related certifications.</li> </ul>		

<p>✓ At least One (1) Team Member:</p> <ul style="list-style-type: none"> <li>▪ Must be with the service provider’s organization one (1) year before the bid opening</li> <li>▪ Has performed three (3) engagements within the last five (5) years comparable to the proposed engagement</li> <li>▪ At least three (3) years active IT security experience</li> <li>▪ At least three (3) years SIEM or system and network administration experience</li> <li>▪ Has any one (1) of the following unexpired professional certifications: CISA, CISM, GSEC, GMON, GCDA, GWAPT, GCIH, GCFA, GCIA, CCNA, ITIL, CEH, CHFI, CNDA, CFR, CompTIA Security+ CVA, OSCP, CISSP, GPEN, GXPEN, LPT Master, CPT, CEPT, CMWAPT, CompTIA PenTest+, CPISI, or other security-related certifications.</li> </ul>		
<p>10. 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.</p>		
<p>11. 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</p>		
<p>12. 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 compliant with the technical specifications stipulated under Section VII. Technical Specifications.</p> <p>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.</p>		

**4. Delivery Time/Completion Schedule**

The Project must be implemented by phases: Phase 1 - Threat Intelligence and Incident Response 15 working days after from the issuance of Notice to Proceed, Phase 2 – Security Monitoring and Management 45 working days from the issuance of Notice to Proceed, Phase 3 - Vulnerability Management and Penetration Testing 65 working days from the issuance of Notice to Proceed. 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.



## 5. Payment Milestone

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

First (1 <sup>st</sup> ) Year:	% of Contract Price
Upon Phase 1 implementation and acceptance: <ul style="list-style-type: none"> <li>• Threat Intelligence</li> <li>• Incident Response</li> </ul>	10%
Upon Phase 2 implementation and acceptance: <ul style="list-style-type: none"> <li>• Security Monitoring and Management</li> </ul>	10%
Upon Phase 3 implementation and acceptance: <ul style="list-style-type: none"> <li>• Vulnerability Management and Penetration Testing</li> </ul>	10%
Upon full implementation and Agency Acceptance. This includes stabilization period plus training and knowledge transfer of the Shared Cyber Defense solution.	20%
<b>Second (2<sup>nd</sup>) Year:</b>	
Four (4) quarterly payments at 12.5% each	50%
<b>Total</b>	<b>100%</b>

---

**SHARED CYBER DEFENSE SOLUTION PROJECT**


Land Bank of the Philippines:

NAME	SIGNATURE
<b>Alan V. Bornas</b> Executive Vice President	
<b>Alden F. Abitona</b> Chief Information Officer	

---

**SHARED CYBER DEFENSE SOLUTION PROJECT**

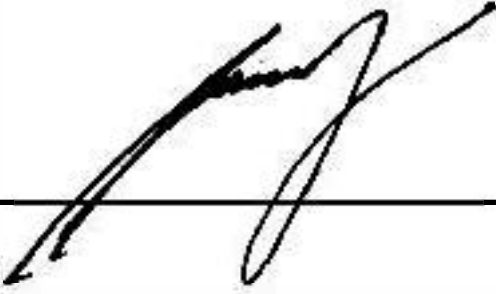
Development Bank of the Philippines:

NAME	SIGNATURE
Emmanuel Z. Muñiz III Chief Information Officer	

---

**SHARED CYBER DEFENSE SOLUTION PROJECT**


**United Coconut Planters Bank:**

NAME	SIGNATURE
Randall Rogelio A. Evangelista Chief Information Officer	

---

**SHARED CYBER DEFENSE SOLUTION PROJECT**

**Philippine Guarantee Corporation:**

NAME	SIGNATURE
Lloyd A. Sioson Vice President - IT Department	 

Priority Level	Description
P1	Catastrophic
P2	Critical
P3	Marginal
P4	Negligible

PROBABILITY	IMPACT			
	High	Medium	Low	Very Low
High	P1	P2	P2	P3
Medium	P2	P2	P3	P4
Low	P2	P3	P3	P4
Very Low	P3	P3	P4	P4