| Sl. No | RFQ Page no | RFQ Clause no | Existing clause Details | Clarification Sought | IFTAS Response |
|---|---|---|---|---|---|
| 1 | 26 | Annexure-V: Technical Specifications of Vulnerability Management | The proposed solution shall be able to automatically pause scheduled scans if unable to complete within the predefined durations | The proposed solution shall be able to manually pause scheduled scans if unable to complete within the predefined durations | RFQ clause remains unchanged. Scan should automatically timeout after predefined time. |
| 2 | 26 | Annexure-V: Technical Specifications of Vulnerability Management | The proposed solution must be able to perform discovery, vulnerability scanning, web scanning, and compliance assessment in a single scan. | Does Web Scanning indidcates here Web Application Scanning? Kindly clarify | Web scanning amended to web application scanning |
| 3 | 26 | Annexure-V: Technical Specifications of Vulnerability Management | The proposed solution must be able to perform TCP scanning in full connection scan and stealth scan, including but not limited to SYN, SYN+FIN, SYN+RST, SYN+ECE. | Please clarify what you mean by SYN+FIN etc. | Sometimes a firewall administrator or device manufacturer will attempt to block incoming connections with a rule such as “drop any incoming packets with only the SYN flag set”. They limit it to only the SYN flag because they don't want to block the SYN/ACK packets which are returned as the second step of an outgoing connection. So SYN+FIN/RST/ECE must be supported |

| | | | | | |
|---|---|---|---|---|---|
| 4 | 26 | Annexure-V: Technical Specifications of Vulnerability Management | The proposed solution must label unsafe checks and allow users to disable these on a per-scan basis. The proposed solution must include scan templates designed to limit the impact on target assets. | Kindly explain and elaborate on the use case | Provide the use case for unsafe checks and disable portals automatically while doing the scan and share available scan templates |
| 5 | 26 | Annexure-V: Technical Specifications of Vulnerability Management | The proposed solution vendor must maintain a fixed coverage updates to all deployed consoles. Describe release cycles for newly developed coverage, including attached service-level agreements. | Please explain the use case and clarify, what native exploit information indicates too | Addons /upgradation /latest scans/attacks etc. as per industry standards |
| 6 | 26 | Annexure-V: Technical Specifications of Vulnerability Management | The proposed solution must be able to provide information on how to develop exploit(s) to demonstrate and validate the vulnerability found. | The solution will provide the detailed CVE and CVSS id and how the attacker will exploit the system. Please clarify what does this mean by develop exploit | Proposed solution should provide information to create exploits. |
| 7 | 26 | Annexure-V: Technical Specifications of Vulnerability Management | The proposed solution must correlate vulnerabilities across multiple tiers of the IT stack. | This can be achieved through SIEM integration with VM solution | Bidders can provide additional information with respect to their solution including SIEM integration. |
| 8 | 26 | Annexure-V: Technical Specifications of Vulnerability Management | The proposed solution must be able to export scan data in format including but not limited to ARF, CSV, CyberScope XML, Simple, XML 1.0 and 2.0, SCAP XML, SQL Query Export and XCCDF. | The proposed solution must be able to export scan data in format including but not limited to CSV, XML, HTML and PDF. | Clause Stands modified to --<br>The proposed solution must be able to export scan data in format including but not limited to CSV, XML, HTML and PDF. |

| | | | | | |
|---|---|---|---|---|---|
| 9 | 26 | Annexure-V: Technical Specifications of Vulnerability Management | The proposed solution must provide remediation reports including engineer level instructions and cross linking to external databases for patches, downloads and references. | Reports can be provided on the basis of the vulnerabilities patched. Please clarify what you mean by engineering level instruction and cross link to databases for patches | To assist in technical teams for patching |
| 10 | 26 | Annexure-V: Technical Specifications of Vulnerability Management | The proposed solution must support identification and management of vulnerability exceptions. Exceptions should support an approval workflow. | The solution provides exceptions, but workflow is internal and depends on organisations to accept the vulnerability as a risk or no risk. Kindly remove the "approval workflow" clause and amend accordingly | Proposed solution should be compatible for those recommendations |
| 11 | 26 | Annexure-V: Technical Specifications of Vulnerability Management | The proposed solution must be able to automatically exclude vulnerabilities that cannot be exploited by integration with penetration testing platform. | Please provides more details on the same | Requirement stands removed |
| 12 | 26 | Annexure-V: Technical Specifications of Vulnerability Management | The proposed solution must be able to integrate with tools that provide KPIs and guidance to improved defenses on your endpoints. | Please provides more details on the same | Should support integration with other security tools like SIEM, PIM etc., |
| 13 | 9 | 6.6 Project Timeline | Delivery and Implementation of the license to be completed within 6 - 7 days from the date of Purchase Order. | Delivery and Implementation of the license to be completed within 8 weeks from the date of Purchase Order. | RFQ clause remains unchanged |

| | | | | | |
|---|---|---|---|---|---|
| 14 | 11 | 7.2 Technical Evaluation Matrix | Implementation Experience | As per Eligibility criteria "The bidder should be currently in the service of providing Vulnerability management/Managed services in Security solutions"<br>Please clarify bidder can provide two implementation of Vulnerability management/Managed services in Security solutions | Implementation experience required in VM solution deployment and daily operations |
| 15 | 8 | 6.2 (B) | The Bidder further represents and warrants that all licenses delivered /rendered under and in accordance with this Contract shall have no defect, arising from design or from any act, error/defect or omission of the Bidder | Bidder submits that the licenses will be provided with standard warranties with respect to the same and that the warranty shall not cover claims resulting from:<br>1. improper use, site preparation, or site or environmental conditions or other non-compliance with applicable supporting material;<br>2. Modifications or improper system maintenance or calibration not performed by bidder or authorized by bidder;<br>3. failure or functional limitations of any non-bidder software or product impacting systems receiving bidder support or service<br>4. malware (e.g. virus, worm, etc.) not introduced by bidder; or | RFQ clause remains unchanged |

| | | | | | |
|---|---|---|---|---|---|
| | | | | 5. abuse, negligence, accident, fire or water damage, electrical disturbances, transportation by Customer, or other causes beyond bidder's control. | |
| 16 | 12 | 8.1 (Other Payment Conditions) | b. Payment will be released within 45 days of receipt of correct invoices along with necessary documents / certificates duly signed by authorized IFTAS official. | Bidder requests that all payments be made within 30 days from the date of the invoice and that the Customer provide a list of the documents to be submitted by bidder along with the invoices. | RFQ clause remains unchanged |
| 17 | 12 | 8.1 (Other Payment Conditions) | d. Price shall remain fixed during the contract period. There shall be no increase in price for any reason whatsoever and therefore no request for any escalation of the cost / price shall be entertained. | Bidder submits that in the event of any increase in the price due to reasons not attributable to the bidder, the parties will mutually agree on the increased pricing. | RFQ clause remains unchanged |
| 18 | 13 | 9 | Service Level Standards/ Requirements/ Agreement | Bidder submits that all penalties be capped cumulatively at 10% of the annual charges payable by customer. | RFQ clause remains unchanged |
| 19 | 14 | 11 | Performance Bank Guarantee | Bidder submits that the PBG will be issued within 30 days from the date of execution of the governing contract between the parties. Further, inability of the parties to execute the governing contract as per mutual agreement shall not be considered a violation under this clause. | RFQ clause remains unchanged |

| | | | | | |
|---|---|---|---|---|---|
| 20 | 14 | 12 | Terminantion of Purchase Order/Contract | Bidder submits that the customer provide a notice period of at least 30 days prior to termination. Further, in the event of termination, customer shall pay all amounts due and payable for the services rendered till the effective date of termination along with such other amounts as may be agreed between the parties.<br>Furthermore, bidder requests deletion of the risk purchase clause. | RFQ clause remains unchanged |
| 21 | 17 | 18 | The bidder shall, at its own cost and expenses, defend and indemnify IFTAS against all third-party claims including those of the infringement of Intellectual Property Rights, including patent, trademark, copyright, trade secret or industrial design rights, arising from use of the products or any part thereof in India. | Bidder submits that the bidder shall defend and settle and/or pay damages awarded by the court the customer against any third party claims arising from the following: a. Claims for loss or damage to third party tangible property; b. claim by any person in respect of bodily injury or death; c. claims by any third party in respect of any IP infringement; brought against or recovered from customer by reasons of any act or omission of the bidder, its agents or employees in the performance of the contractual obligation. | RFQ clause remains unchanged |

| | | | | | |
|---|---|---|---|---|---|
| 22 | 22 | Annexure III | Conformation to Terms and Conditions | Bidder requests to relax this term to enable the Bidder to propose/suggest alternate terms on the material terms and conditions of the RFP.<br>Also, the Bidder submits that the contract will be signed based on mutually agreed terms between the parties. | RFQ clause remains unchanged |
| 23 | NEW | NEW | NEW | We request inclusion of material terms and conditions in the governing contract, including but not limited to the following:1. Limitation of Liability: To the extent allowed under Indian laws, the Aggregate Liability of either party under the contract, torts or any other legal theory for all claims, loss, damages, breach, etc shall in no event exceed the annual purchase order value/annual value under this contract.  Both parties agree that neither party shall be liable for any indirect, remote, consequential loss or damages including but not limited to loss of profit, loss of anticipated earning, loss of data, revenues, goodwill, or business value whether or not that party was aware or should have been aware of the possibility of such costs, expenses or damages.2. Intellectual | As per RFQ terms and conditions |

| | | | | | |
|---|---|---|---|---|---|
| | | | | Property Rights: No transfer of ownership of any intellectual property will occur under the Agreement. Customer grants bidder a non-exclusive, worldwide, royalty-free right and license to any intellectual property that is necessary for bidder and its designees to perform the ordered services.3. Any other material terms and conditions as may be mutually agreed between the parties. | |
| 24 | 12 | 8.1 | Delivery, Implementation, Training and Support<br>a. 100 % of the implementation cost will be paid on completion of installation and acceptance sign-off from IFTAS.<br>b. Subscription cost will be paid annually in arrears and for the first year on completion of installation and acceptance sign-off from IFTAS. | no specofoc time can be defined while scanning, pausing a scan is a manual task. Request you kindly change the clause accordingly | RFQ clause remains unchanged |
| 25 | NEW | NEW | | Any changes in Statutory tax at the time of invoicing to be at actuals | As per RFQ terms and conditions |

| | | | | | |
|---|---|---|---|---|---|
| 26 | 10 | 7.4 | The bidder should be currently in the service of providing Vulnerability management/Managed services in Security solutions including at least two Government/public/BFSI in India | Due to Covid-19 situation, many customers will be unable to give "client certificate". Request if PO / Work Order would be fine to be considered | Project completion or UAT signoff letter from client would be considered if client certificate is not available. |
| 27 | 26 | Annexure V point 2, page 26 | The proposed solution must be offered as either Software Product or Software as a Service | Kindly mention the license of the software should be either perpetual or subscription based | Subscription Based |
| 28 | 26 | Annexure V point 5, page 26 | The proposed solution's hardware appliance or any equivalent technology (if proposed) must run off 64-bit OS architecture and must be able to utilize resources going beyond 4GB RAM. | Kindly elaborate and explain on "able to utiliize resource beyond 4GB RAM" | VM software should be able to utilize RAM resources efficiently. Should work on 64 bit OS version. |
| 29 | 27 | Annexure V point 13, page 27 | The proposed solution must include web-based management user interface over encrypted traffic. It must not be accessed in clear text. | Kindly elaborate and explain | Logging into VM solution (web interface) should be over https not on http |
| 30 | 27 | Annexure V point 14, page 27 | The proposed solution must support command line console within web GUI. | Why a specific requirment to have the CLI within the GUI. Please explain | For passing basic troubleshooting commands like ping, trace route etc., using CLI |
| 31 | 28 | Annexure V point 27, page 28 | The proposed solution shall be able to automatically pause scheduled scans if unable to complete within the predefined durations | No specofoc time can be defined while scanning, pausing a scan is a manual task. Request you kindly change the clause accordingly | RFQ clause remains unchanged |

| | | | | | |
|---|---|---|---|---|---|
| 32 | 30 | Annexure V point 46, page 30 | The proposed solution must label unsafe checks and allow users to disable these on a per-scan basis. The proposed solution must include scan templates designed to limit the impact on target assets. | Kindly explain and elabirate on the use case | Provide the user case for unsafe checks and disable portals automatically while doing the scan and share available scan templates |
| 33 | 30 | Annexure V point 51, page 30 | The proposed solution must be able performs local checks with credentials. Describe the ability of your product to manage credentials for hosts in a large enterprise. | Any credentail scanning can be automated and be integrated with the PIM/PAM soultion IFFTAS is using. Please mention the PIM/PAM solution and include in the clause | PIM solution details shall be shared with successful bidder. |
| 34 | 30 | Annexure V point 58, page 30 | The proposed solution vendor must maintain a fixed coverage updates to all deployed consoles. Describe release cycles for newly developed coverage, including attached service-level agreements. | Fixed Coverage update please explain and clarify | Should support timely updates to all deployed devices in VM solution |
| 35 | 32 | Annexure V point 67, page 32 | The proposed solution must be able to integrate native exploit information from well-known sources. | Please explain the use case and calrify, what native exploit information indicates too | It should have connectors to integrate with already known exploit modules in market. To create an efficient and easy PT testing scope |
| 36 | 32 | Annexure V point 83, page 32 | The proposed solution must provide a policy editor for custom configuration policy scans. | Are you referring of customizing policies within GUI when you indicate it as policy editor? Kindly clarify | Proposed solution should support customized policies. |

| | | | | | |
|---|---|---|---|---|---|
| 37 | 33 | Annexure V point 86, page 33 | The proposed solution must have the ability to prioritize solutions for failures to show quickest path to remediation. | Failures indicate to high rated vulnerabilities and its path to remediation? Please explain and ckarify | Solution should prioritize the remediation of vulnerabilities based on severity |
| 38 | 36 | Annexure V point 126, page 36 | The proposed solution's remediation reports must provide step-by- step guide for administrators to fix the vulnerabilities found. Steps shall be well organized with correct orders without duplicates. Steps shall also include estimated down time as a reference for the administrators. | Any VM solution provides the link for remediation, i.e. from where the solution can be found and patched. The link it doscovers agaisnt a vulnerability is on the basis of the what the vendor has posted on its website. It is not the VM solution who can provide the downtime and step by step guide. Request you kindly modify the clause and amend accordingly | Should support remediation process and tool should give top remediation plans to minimize the risk impact at large |
| 39 | 36 | Annexure V point 128, page 36 | The proposed solution must be able to create reports that aggregate common remediation steps across patches and other remediation steps, such as configuration changes. | Please explain the use case and clarify the clause | Should support remediation process and tool should give top remediation plans to minimize the risk impact at large |
| 40 | 37 | Annexure V point 130, page 37 | The proposed solution must support other technology alliance partners to which it can leverage on discovered vulnerability findings to extend the value within the organization. List and describe the solution's relationships with security technology partners. | Please provide the list of vendors to which IFFTAS is lookiing for integration | Will be shared with successful bidder |

| | | | | | |
|---|---|---|---|---|---|
| 41 | 37 | Annexure V point 131, page 37 | The proposed solution must have integration with existing PIM solution at IFTAS. Details will be provided to the successful bidder. | Please provide the details of the PIM/PAM solution | Will be shared with successful bidder |
| 42 | 37 | Annexure V point 132, page 37 | The proposed solution must support integration with virtual environments. | Please give details of virtual environments | Vmware, KVM, Hyper-v |
| 43 | 37 | Annexure V point 132, page 37 | The proposed solution must support integration with network topology and risk analysis products. | Please provides more details on the same | Should support integration with existing monitoring and security tools |
| 44 | 37 | Annexure V point 136, page 37 | The proposed solution must support integration with IDS/IPS products. | Please provide details of IPS/IDS products | Will be shared with successful bidder. Top players in industry are in use |
| 45 | 37 | Annexure V point 137, page 37 | The proposed solution must support integration with IT GRC products. | Please provides more details on the same | Will be shared with successful bidder. Top players in industry are in use |
| 46 | 37 | Annexure V point 138, page 37 | The proposed solution must support integration with any NGSOC Solutions | Please provides more details on the same | Will be shared with successful bidder. Top players in industry are in use |
| 47 | 37 | Annexure V point 139, page 37 | The proposed solution must support integration with external penetration testing platforms to perform and automatic vulnerabilities exploitation without running any manual imports to confirm that vulnerabilities can be exploited. | Please provides more details on the same | The details provided are self-explanatory; however bidders can provide additional information with respect to their solution. |

| | | | | | |
|---|---|---|---|---|---|
| 48 | 37 | Annexure V point 140, page 37 | The proposed solution must be able to automatically exclude vulnerabilities that cannot be exploited by integration with penetration testing platform. | Please provides more details on the same | The details provided are self-explanatory; however bidders can provide additional information with respect to their solution. |
| 49 | 37 | Annexure V point 141, page 37 | The proposed solution must be able to integrate with tools that provide KPIs and guidance to improved defenses on your endpoints. | Please provides more details on the same | The details provided are self-explanatory; however bidders can provide additional information with respect to their solution. |
| 50 | 9 | Point 6.6, page 9 | Delivery and Implementation of the license to be completed within 6 - 7 days from the date of Purchase Order. | Delivery and Implementation of the license to be completed within 15 days from the date of Purchase Order. | RFQ clause remains unchanged |
| 51 | 8 | Point 6.1 N, Page 8 | Vulnerability Management console should run in active & passive mode in DC and DR. | Can be achieved through 3rd party failover | Bidder can propose appropriate solution to achieve the same. |
| 52 | 33 | Annexure 5 Point 80, Page 33 | The proposed solution must support SCAP compliance policy checks and customized SCAP policy uploads. | Pleae share an Total number and Detailed Type of OS for customization | Should not be restricted to OS level demarcation. |

| | | | | | |
|---|---|---|---|---|---|
| 53 | 6 | Section 6, Page 6 | B. Vulnerability Assessment and Penetration Testing should cover the intranet and internet application and its components including web server, app server, DB Server, Thick client, Thin clients, Mobile applications, Networking systems, Security devices, load balancers etc. , websites maintained at IFTAS's premises in Mumbai and Hyderabad. C. Vulnerability assessment must be carried out for all the applications/critical devices of the IFTAS on quarterly basis and required 1024 IP/asset's license for Vulnerability. D. The Bidder shall conduct scheduled penetration testing (i.e. quarterly once) for identified devices / networks to identify security issues/vulnerabilities that could be exploited by remote attackers. The penetration testing exercise must give IFTAS an holistic view of overall infrastructure security of the asset as seen from the Internet/outside organization. | Can VA and PT activities be conducted remotely? | VA should be on-premise and no data shall be shared outside organization. PT can be remotely performed with mutually agreed NDA |

| | | | | | |
|---|---|---|---|---|---|
| 54 | 40 | Annexure V Penetration Testing Requirements 16-20, Page 40 | Social Engineering Campaign | Is social engineering activity to be conducted as part of this RFP? | Bidders to consider the social engineering activity. |
| 55 | 39 | Annexure V Penetration Testing Requirements, Page 39 | Solution must be able to integrate with VA SCANNING TOOLS to discover host's OS, running services and vulnerabilities via existing scan results or new scans. | We use multiple tools for Penetration Testing, hence integration may not be possible. Please confirm. | VA solution should support integration with major PT tools which assists in faster PT testing as per VA report on a particular asset. |
| 56 | | 4 | The proposed solution must offer both the console and scanner engines available as a hardware appliance. | Will the hardware be provided by IFTAS, kindly clarify | Proposed solution to be deployed in IFTAS's own private cloud infrastructure. |
| 57 | Web Scanning | 88 - 95 | Clarification on Points 88 - 95 | Our solution provides Web Application Scanning (WAS) as a separate module and is a cloud offering. Please let us know your acceptance on the same. If else, we suggest you separate this from the current RFP. It would not be fair to evaluate the requirement based on one OEM's perspective. | RFQ clause remains unchanged |
| 58 | | | Performance Bank Guarantee may be discharged by IFTAS upon being satisfied that there has been due performance of the obligations of the bidder under the contract.<br>Performance Bank Guarantee shall be | Pricing is invited for 5 years but payment will be released every year.So bank guarantee will be 10 percent of one year cost right?<br>This performance bank guarantee will be | RFQ clause remains unchanged |

| | | | | | |
|---|---|---|---|---|---|
| | | | valid for contracted period | refunded by what time.Is there a timeline to it. | |
| 59 | | | The bidder should be currently in the service of providing Vulnerability management/Managed services in Security solutions including at least two Government/public/BFSI in India Proof of Client Certificate is to be Submitted. | We are providing security services to organizations like CCIL,Kribhco.Can we participate in the RFP.What is the format of Proof of Client Certificate | Any reference letter mentioning the similar services offered by vendor from client would suffice |
| 60 | | | The Bidder should have a minimum annual turnover of at least Rs. 1 Crores in each of the last three financial years. The Bidder should have made positive net worth in each of the last three financial years | 2020 - 1 cr statement is yet to be made<br>2019 - 75 L<br>2018 - 47 L<br>Can we still bid for this RFP | RFQ clause remains unchanged |
| 61 | | 7. Eligibility Criteria / 10 | Bidder must have registration under companies Act, 1956, also registered with the Goods & Service Tax authorities, and must have completed 3 years of existence as on Bid calling date. | Requet to consider resgration as Propriority Firm / Registered under MSME | RFQ clause remains unchanged |
| 62 | | 7. Eligibility Criteria / 10 | The Bidder should have a minimum annual turnover of at least Rs. 1 Crores in each of the last three financial years. The Bidder should have made positive net worth in each of the last three financial years. | Request to consider the turn over as an Average 1 Cr for last 3 years | RFQ clause remains unchanged |

| | | | | | |
|---|---|---|---|---|---|
| 63 | | 7. Eligibility Criteria / 10 | The bidder may be either an OEM or highest-level Authorized Partner of the OEM (Original Equipment Manufacturer) whose product they are proposing. In case the OEM does not deal directly, an OEM may bid through their Authorized Service Partners or System Integrator | Request to consider as Authorized Partner in lieu of Highest Level Partner | RFQ clause remains unchanged |
| 64 | | 7. Eligibility Criteria / 10 | The Vulnerability Management application of the proposed solution must be in the Leaders Quadrant of Gartner's Magic Quadrant 2019 or latest or any other such equivalent. | Clarification required If Forester Wave Report is considered | Other equal and recognized independent agency can be considered. |
| 65 | | | | Request for extension for Bid submission Date | Refer Amendment 1 for revised schedule |