Pre-Bid Replies - REQUEST FOR PROPOSAL (RFP) FOR CYBER INSURANCE POLICY OF NATIONAL BANK FOR AGRICULTURE AND RURAL DEVELOPMENT (NABARD) FOR 2022-		
S N	**Query**	**Response**
1.	Claims/instances/circumstances for past 5 years	None since starting of insurance (2 year)
2.	Business Continuity plan	Available with insurance broker
3.	Operational recovery procedure: description of the existing back-up procedures and capabilities?	Real time replication for enterprise applications and two backup copies including tapes.
4.	Information Security Incident Response Policy	Cyber Crisis Management Policy is in place
5.	IT Security policy, BCP plan, CISO presentation	IS and BCP Policy are available with insurance broker
6.	Filled questionnaire	Available with insurance broker
7.	Filled Ransomware and 12 c form details	Available with insurance broker
8.	Proposal form	Available with insurance broker
9.	Are employees allowed to use personal devices for official usage?	Yes, only for internet facing applications
10.	Is webmail accessible outside the corporate network? If yes, How is access to emails protected?	Yes, we are using Microsoft 365 with Advanced Threat Protection, DMARC, DKIM, SPF.
11.	Are any servers / desktops accessible via remote connectivity i.e remote desktop, team viewer, etc.?	Only through VPN from whitelisted systems

Pre-Bid Replies - REQUEST FOR PROPOSAL (RFP) FOR CYBER INSURANCE POLICY OF NATIONAL BANK FOR AGRICULTURE AND RURAL DEVELOPMENT (NABARD) FOR 2022-		
S N	**Query**	**Response**
12.	If yes. How is access to those servers protected?	Disabled plug and play devices, no copy paste from local system is allowed, no internet on servers
13.	Is there a BCP plan in place?	Yes
14.	Has this been tested for a scenario where all employees must work either from home or alternate locations?	Yes
15.	Do you have log monitoring	Yes, SIEM
16.	Do they store PII/PCI/ PHI Data if yes	No
17.	What type of data do they store ?	NA
18.	List of all external IPs along with URL details.	Enclosed, URL shall be provided to successful bidder
19.	Queries regarding Log4j vulnerabilities:	Given below:
20.	i. What have you done to identify assets that use Log4j in your environment, especially internet-facing ones?	SOC team created plan and shared with all the teams, identified vulnerable machines, guided teams with respect to advisory related to log4j, searched in directory for log4j files and folder, AV tools were used to scan devices for vulnerability.
21.		If any threat detected, SOC team prepared and released advisories with respect to attacks, SOC team constantly followed up with the concern stakeholders for closure. It is also monitored as a part of regular VAPT
22.		SOC team enabled rapid 7 tenable. Team manually logged in to servers and search for specific files, removed or upgraded files/folder(wherever required)
23.	ii.What affected systems have you patched so far, and when did you patch them?	All systems running Log4j services were patched in Dec 2021
24.	iii. How are you handling the potential compromise of those systems?	No compromise as on date. Regular Backup and Proactive Monitoring to handle this situation is in place.

Pre-Bid Replies - REQUEST FOR PROPOSAL (RFP) FOR CYBER INSURANCE POLICY OF NATIONAL BANK FOR AGRICULTURE AND RURAL DEVELOPMENT (NABARD) FOR 2022-		
S N	**Query**	**Response**
25.	Iv. What steps have you taken to block Log4 Shell attacks, and what extra monitoring, if any, are you doing?	SOC team had deployed use cases, issued advisories, raised or reported alerts, enabled monitoring, blocked IOCs , IOCs added to thread feed. Proactively blocked all malicious IPs on firewalls.
26.		Updated required definition/signature on antivirus.
27.	Changes in the policy proposed compared to the expiring terms	None
28.	Claims experience for the last 5 years.	Please refer to point no 1
29.	Policy wordings to be used	Available with insurance broker
30.	Proposal Form	Available with insurance broker
31.	Information Security policy	Available with insurance broker
32.	Business Continuity Plan	Available with insurance broker
33.	Business Continuity Management Policy	Available with insurance broker
34.	Disaster Recovery Plan	Available with insurance broker
35.	Latest Available IT audit report	Will be shared with successful bidder
36.	Which organization software can be accessed outside the corporate network?	HRMS, Corporate Intranet, Data Collector, Enterprise Content Management, CLMAS etc.

Pre-Bid Replies - REQUEST FOR PROPOSAL (RFP) FOR CYBER INSURANCE POLICY OF NATIONAL BANK FOR AGRICULTURE AND RURAL DEVELOPMENT (NABARD) FOR 2022-		
S N	**Query**	**Response**
37.	What checks and security measures are taken to secure these software outside the corporate network	WAF implemented for internet facing portals
38.	Fully filled Cyber proposal form	Available with insurance broker
39.	Risk Engineer engagement form	Not required
40.	Ransomware questionnaire	Available with insurance broker
41.	If answer to question 12 c in each of the RW questionnaire is not zero, then for each service account that is identified to have 'Domain Admin' privilege; details need to be collected in prescribed excel template titled '12c-Service Account-Data Collection' (please find attached a PDF which elaborates the importance of service accounts with DA privileges)	Will be provided to successful bidder
42.	List of Inventory of External IP(s) of the Insured, including subsidiaries. Also, all the entities being covered under the policy	Attached, may be changed during policy period
43.	List of Domains belonging to the Insured, including subsidiaries. Also, all the entities being covered under the policy	nabard.org, nabkisan.org, nabventures.in, nabcons.com, nabfoundation.in, nabsamruddhi.in, nabfins.org
44.	Are the systems of NABARD and its subsidiaries interconnected*, if yes, how?	Yes
45.	If connected how do they maintain network segregation and will contain a breach to one company only, in case it happens?	NABARD is hosting some applications of its subsidiaries in its Data Center.

Pre-Bid Replies - REQUEST FOR PROPOSAL (RFP) FOR CYBER INSURANCE POLICY OF NATIONAL BANK FOR AGRICULTURE AND RURAL DEVELOPMENT (NABARD) FOR 2022-		
S N	**Query**	**Response**
46.	*System interconnectivity includes sharing of:	
47.	1. Domain	Subsidiaries staff working in NABARD Premises are using same network and other resources as that of NABARD.
48.	2. Shared Folders	
49.	3. Active directory	
50.	4. Email systems	
51.	5. Security system	
52.	6. Network infrastructure	
53.	7. ERM or CRM type applications (e.g. SAP, Salesforce, etc.)	
54.	Common Datacenter / Cloud Tenancy (what about coincidence they use the same company but do not share the same resources - better way to be specific?)	
55.	Common IT team managing multiple IT environments of group companies (if common, could central team be bridge to incident from insured to none-insured?)	
56.	End user systems	
57.	Operational technology	
58.	Past claim exp for last 3 years	None
59.	Changes in terms from expiring policy	No
60.	Any dilution in security measures,. IT, accounting or audit etc, whish is more exposed to risk or frauds	No

Pre-Bid Replies - REQUEST FOR PROPOSAL (RFP) FOR CYBER INSURANCE POLICY OF NATIONAL BANK FOR AGRICULTURE AND RURAL DEVELOPMENT (NABARD) FOR 2022-		
S N	**Query**	**Response**
61.	Any improvement in security measures, IT, accounting or audit etc to prevent fraud / claims etc	NAC
62.	Completed proposal form with total turnover	Available with insurance broker
63.	How much% of your business is dependent on internet and machines which operate on Internet.	No dependency
64.	Do you have system back up ? If yes, kindly elaborate the type of backup and the periodicity of Back up.	Daily, weekly, monthly and yearly depending on applications
65.	Loss of Revenue, if there is a business interruption to the operation system, computer systems.	Yes
66.	Do you have Firewall// end point detection response (EDR)/Antivirus ?	Yes
67.	Is Multifactor Authentication	Only on VPN
68.	Besides traditional signature based detection, does your malware protection use advanced heuristic and behaviour based detection mechanisms to protect against new malware.	Yes
69.	Security Architecture of application	WAF + Perimeter Firewall, Internet Firewall, Port blocking on Core Switch, Server Antivirus, SOC and DMZ
	Supporting document are available with AIBIL (NABARD Insurance Banker)	