Corrigendum1

RFP for Cybersecurity Audit of Nagaland Department Websites Hosted in Nagaland State Data Centre

Sr. No	Clause /page number	As Per RFP	As per modified / to be read as
1	Annexure 1. Page number 17	As per RFP	Annexure1 is modified

ANNEXURE# 1

1 Background and Objective of the Assignment

NSEGS would like to engage a third-party firm to perform a cybersecurity audit. The overall purpose of the Cyber Security Audit exercise is to conform to the IT security needs of quality standard ISO 27001, with respect to CERT-IN guidelines:

- List of websites hosted on Nagaland state data centre as per annexure 3

a. The First Cyber Security Audit exercise needs to be commenced within 7 business days of issuing the Work Order. This needs to be done at NSDC Located in Kohima, Nagaland. Report of Cyber Security Gaps along with the recommendations needs to be provided by the Bidder and based on the same security Gap analysis, action would be taken at NSEGS end. The First Phase of the Cyber Security Audit and its Reporting need to be completed within 20 business days of commencement.

b. After the end of the First Phase of the Cyber Security Audit and Reporting thereof by the bidder, NSEGS would take some reasonable time to study the Gaps in Cyber Security and would attempt to bridge the gaps as much as possible. After the Gap bridging exercise by NSEGS has been completed, the bidder would be informed accordingly by the concerned NSEGS representative, and thereafter the bidder should commence the Second Phase of the Cyber Security Audit exercise. The time taken by NSEGS for bridging the Cyber Security Gap will not affect the bidder in any way as the bidder will not be held responsible for any delay in the same.

2 The scope of Work:

The Scope of work for Cyber Security Audit would be as per the Guidelines of CERT-IN and would be under the following broad categories:

2.1 Cyber Security Audit:

The audit has to be carried out as per the CERT-IN guidelines. The audit will include a compliance audit as per Cert-IN markers along with the technical sampling audit for evidence gathering.

The scope of work would cover the following areas:

- Assessment against Cert-IN markers and evidence collection
- Gap Analysis against CERT-IN Guidelines
- Documented evidence
- Audit Report

The audit will include the website vulnerability assessment and the latest cybersecurity assessment. The bidder is supposed to analyse and submit all vulnerability reports

The Bidder should provide the below-mentioned details at the starting of the Cyber Security Audit exercise:

a) The methodology in which the Cyber Security Audit activity to be done will include the time frame of each activity to organize the cyber audit activity.
b) Standards of Security and Quality that are to be followed during the Cyber Security Audit activity.

c) Tools and Software that may be used for the cybersecurity audit activity. All tools and software used by the bidder need to be licensed.
d) Any Additional and Mandatory standards of Cyber Audit regulation as required for CERT-IN Audit, should be made available and applicable by the Auditor.
e) The scope of the audit (in case of VA/PT) should not be limited to the few lists like OWASP top 10 or SANS Top 25 programming errors, it must include the discovery of all known vulnerabilities

2.2 Schedule of Conducting Cyber Security Audit:

Cyber Security Audit in NSEGS needs to be conducted Two Times for the sake of cross-checking the effective implementation of the recommendations provided during the first Audit exercise. The First Cyber Security Audit exercise needs to be commenced within 7 days of issuing the Work Order. The audit will include a compliance audit as per CERT-IN markers along with the technical sampling audit for evidence gathering. Report of vulnerability and corrective measure need to be provided by the Bidder and based on the same action would be taken at NSEGS end. The First Phase of the Cyber Security Audit and its Reporting need to be completed as per the scheduled timeline.

a. After the end of the First Phase of the Cyber Security Audit and Reporting thereof by the bidder, NSEGS would take some reasonable time to study the Gaps in Cyber Security and would attempt to bridge the gaps as much as possible. After the Gap bridging exercise by NSEGS has been completed, the bidder would be informed accordingly by the concerned NSEGS representative, and thereafter the bidder should commence the Second Phase of the Cyber Security Audit exercise. The time taken by NSEGS for bridging the vulnerability will not affect the bidder in any way as the bidder will not be held responsible for any delay in the same. The Report of the VA/PT Analysis of the First Phase of Cyber Security Audit should be made in such a way that it should help NSEGS in patching or updating of web/applications.
b. The Second phase Cyber Security Audit need to be completed within 7 days after the concerned NSEGS representative gives the go-ahead for the Second Phase exercise. The purpose of the Second Phase Audit exercise would be to identify and specify whether the Vulnerability Report Submitted in the First Phase exercise, still exists or the Cyber Security Gaps are plugged in to make the IT system of NSEGS as secure as possible. The Second phase audit exercise should also result in a Detailed Report and Analysis to be submitted for the current Cyber Security status of the websites hosted at the Nagaland State Data Centre.

2.3 Reports and Deliverables:

1. Audit Plan of the Cyber Audit exercise .
2. Dates and Locations of Proposed and Actual Cyber Audit exercise.
3. Summary of Cyber Audit findings, including identification tests and the results of the tests, need to be shared with concerned NSEGS officials.
4. Analysis of vulnerabilities and issues of concern of Cyber Security needs to be reported.
5. Recommendations in line with CERT-IN compliant.
6. Final Report of Cyber Security Audit in NSEGS across all departments to be submitted immediately after the completion of the Audit activity.
7. Presentations on the Cyber Security Audit Report, its findings, conclusions, and recommendations
8. Security Audit Certificate for all the audited websites.

The bidder will analyse all reports, which has to be shared with representatives to keep NSEGS informed about cyber threats at present and in future at NSEGS IT facilities. The bidder will identify current and future cyber threats to NSEGS IT facilities and propose to take actions to mitigate such upcoming cyber threats and vulnerabilities so identified.

Details of the Authorized Contact person for the Cyber Security Audit Exercise need to be provided by the Bidder, designated for NSEGS, to be the single point of contact for the Bidder

3. Schedule of Deliverables

Sr.no	Deliverable	Tentative Duration/Periodicity (T is the date of Work Order from DITC)
1	Inception report including an outline of IT/Cybersecurity and ISO 27001 requirements, audit Plan, Reporting Formats, work plan, documentation formats, dates and location of proposed IT/Cyber audit exercise	T1=T + 7 days
2	Summary of IT/Cyber Audit findings, including identification tests and the results of the tests, need to be shared with concerned NSeGS officials weekly and as and when required by NSeGS	Weekly/ As & when requested
3	Prepare and submit an a) Cybersecurity and IT audit report (VA/PT) of all websites and application b) Expert Recommendations on the identified gaps. c) Compliance and Regulatory requirements management **Phase 1 –** Share the reports and findings with NSEGS and relevant stakeholders only. Presentations on the IT/Cyber Security Audit Report, its findings, conclusions, and recommendations for Gap Analysis and Plugging, as per CERT-In guidelines.	T2=T1+30 Days
4	Submission of final reports with required guidelines and documents (Phase 2)	After NSeGS Patching and updating websites and application + 20 days.