

# **Annexure – I: Details of Requirements for Network Vulnerability Assessment and Network Performance Analysis - Audit**

## **Introduction**

This document outlines the requirement for Network Vulnerability Assessment and Network Performance Analysis - Audit. The goal of the project is two-fold:

- Assess all security vulnerabilities of the INFINET network and recommend solutions for identified vulnerabilities
- Assess INFINET’s ability to meet the performance requirements related to traffic and transactions carried over it and to recommend solutions for improving the performance

Information assurance is an integral part of the IDRBT ’s mission. Our challenge is to make needed services available to authorized users concurrently with minimizing both the amount of information we disclose to others as well as minimizing the attack profile we present to others. The current level of security can be identified by assessing the performance, identifying the vulnerabilities & then developing appropriate steps for mitigation.

## **Statement of purpose**

IDRBT invites suitably qualified vendor to submit proposals for Network Vulnerability Assessment and Network Performance Analysis - Audit.

## **Confidentiality**

This document, with all information disclosed, is given in confidence. Any part of this document shall not be disclosed to a third party other than the personnel involved in the preparation of the response, except for necessary inquires for information from vendor.

## **Liability**

IDRBT reserves the right to accept or reject any of the submitted responses. IDRBT also has the right to use any of the ideas and information submitted without incurring any liability. IDRBT is not obligated to pay any costs incurred during the preparation of the response. Furthermore this RFP does not commit IDRBT to make an offer or award a contract. IDRBT may reward contract fully or partially to vendors.

## **Vendor Response**

The vendor should respond to the Institute’s requirements, by providing details on-

- An introduction outlining the proposal's content and key points.
- List of deliverables of the vendor
- Methodology and tools used by the vendor

- Profiles of the project team members including experience, qualification and certification
- Detailed Project Plan
  - Timeline and milestones for delivery
  - Allocation of task across project members
  - Project management methodology
- Requirements from IDRBT for executing the project
- Company profile and qualifications

### **Scope**

The scope of this project is Network Vulnerability Assessment and Network Performance Analysis – Audit of INFINET Network.

### **Target environment**

The target environment consists of the network and systems of INFINET Network.

The INFINET, an acronym for the INdian FInancial Network, uses a blend of communication technologies such as VSATs and Terrestrial Leased Lines. The HUB of the VSAT network is situated at IDRBT, and consists of an 11-metre antenna and other satellite earth station equipments.

The INFINET is a Closed User Group [CUG] Network for the exclusive use of Member Banks and Financial Institutions. Presently, the network consists of over 2000 VSATs located in 300 cities of the country and utilizes one full transponder of 36 MHz on INSAT 3B.

The INFINET is primarily a TCP/IP based network. A detailed IP addressing scheme has been devised by IDRBT for all CUG members, which has to be strictly followed by all CUG members, while interacting via the communication backbone.

Initially IDRBT would like to carry out Network Vulnerability Assessment and Network Performance Analysis for the following locations:

- INFINET as a whole network
- IDRBT, Hyderabad network
- RBI, Mumbai Regional Office
- RBI, NCC, Mumbai
- RBI, Delhi Regional Office
- RBI, Kolkatta Regional Office
- RBI, Chennai Regional Office

## Network Vulnerability Assessment (VA)

The security vendor identified will conduct vulnerability assessment against computers and network infrastructure components to identify services in use and potential vulnerabilities present. Our requirements under VA of INFINET are-

- Provide accurate network discovery detail.
- Identify network risks and prioritize issues.
- Enable efficient network-wide remediation.

The assessment should check for various categories of threat to the network, including

- Unauthorized access into the network and extent of such access possible
- Unauthorized modifications to the network and the traffic flowing over network
- Extent of information disclosure from the network
- Spoofing of identity over the network
- Possibility of denial of services
- Possible threats from malicious codes (viruses and worms)
- Possibility of traffic route poisoning

The assessment will involve the following three phases-

1. Network Architecture review for security
  - Review the appropriate segregation of network into various trusted zones
  - Review the traffic flow in the network
  - Review of routing protocols and security controls therein
  - Review the security measures at the entry and exit points of the network
2. Automated & manual security tests for
  - Obtaining information about the architecture and address scheme of the network
  - Security of routers and network devices
    - Mis-configuration related to access lists, account settings
    - Unpatched holes in the operating system
  - Security of servers
    - Mis-configuration related to access lists, account settings
    - Unpatched holes in the operating system
  - Security Devices checks
    - Firewall & IDS configuration
  - These tests are to be carried out from
    - Internal points in respective locations
    - Sample entry points from Closed User Group
    - From Internet

3. Review of key processes related to the Network
  - Configuration management process
  - Change management process
  - Account management process
  - Logging & Auditing
  - Physical security
4. If any of the points not covered in the above, and it is required for identifying Vulnerability assessment, the same may be provided by the vendor.

Deliverables:

- Vulnerability assessment report detailing the vulnerabilities identified and the remediation steps
- List of tools and tests carried out

**Network Performance Analysis**

An analysis of the performance of the network needs to be carried out by the vendor to ascertain the ability of the network to meet current and future needs of users and to identify any bottlenecks. The performance analysis should include the following-

1. Network Architecture review for performance
  - Review extent of layering of the network and redundancies in critical layers
  - Review capacity and redundancy of network devices at multiple layers
  - Analysis of number of hops across various links
  - Analysis of load balancing mechanism
  - Analysis of latency in traffic across various links
2. Automated & manual security tests for
  - Bandwidth utilization at critical links
    - Availability of bandwidth
    - Current utilization levels (average and peak)
    - Scalability of bandwidth & utilization
  - Network device performance
    - Performance related to CPU and memory utilization of devices during peak traffic
  - Analysis of Traffic prioritization mechanism
    - Checking for QOS configurations against business requirements
  - Protocol Analysis
    - Analyse protocols used and traffic generated and means to optimize traffic

3. Review of key processes related to the Network
  - Network management and monitoring process
4. If any of the points not covered in the above, and it is required for identifying Performance analysis of the network, the same may be provided by the vendor.

Deliverables:

- Performance analysis report detailing the weaknesses in current network and recommendations to improve performance
- List of tools and tests carried out

**Documentation**

At the conclusion of the project, IDRBT requires written documentation of the approach, findings and recommendations associated with this project. A formal presentation of the findings and recommendations to senior management may also be required. The documentation should consist of the following:

- Executive Summary Report
  - A document developed to summarize the scope, approach, findings and recommendations, in a manner suitable for senior management.
- Detailed VA Technical Report
  - A document developed for the use of IDRBT's technical staff, which discusses:
    - The methodology employed
    - Tools used
    - Positive security aspects identified
    - Detailed technical vulnerability findings
    - An assignment of a risk rating for each vulnerability
    - Vulnerabilities, risk level, recommended remedy measures for each of the components such as Router, firewall and Server to be reported.
    - Supporting detailed exhibits for vulnerabilities when appropriate and
    - Detailed technical remediation steps.
    - Recommending IDRBT for overall implementation plan for remedial steps.
- Detailed performance analysis Technical Report
  - A document developed for the use of IDRBT's technical staff, which discusses:
    - The methodology employed
    - Tools used

- Positive performance aspects identified
- Detailed technical findings related to gaps in network performance
- Supporting detailed exhibits for such findings when appropriate
- Detailed technical remediation steps.
- Recommending IDRBT for overall implementation plan for remedial steps.

### **Vendor Qualification**

A brief profile of your company is required. The following questions must be answered:

- **Company profile**
  - What are the core business areas?
  - What are the key services offered?
  - What was the revenue of Indian operations on 2003-04?
  - What was the percentage of revenue generated from the professional security? Consulting services fees (initial & recurring) in 2003-04?
  - Number of years in information security business
- **Technical Capability**
  - Number of certified security professionals in the company (Number of CISSPs, CISA, BS7799, GIAC certified professionals).
  - Skill mix of employees in the company
  - Any research activities, international recognitions and alliances relevant to information security
- **Consulting services experience**
  - List of 5 references where similar service has been provided
  - List of 5 large customers where your security consulting services were offered and the size of such service in revenue terms.