BRIEF OF THE CASE

COMMUNICATION EQPT WITH INDIAN SECURITY PROTOCOLS

Case Reference: CF. No/AIR HQ/S.59101/26/ACQT (MAKE) BM-I

1. **Service.** Indian Air Force

2. **Nodal Dte at SHQ**: Directorate of Ops (CIT Security)

3. **Name of the Case**: Design and Development of Securer Communication Network Grid with Indian Security Protocols.

Case Brief

4. Indian Armed Forces intend to establish a secure communication grid to integrate its weapon systems, air-defence elements, data-centers and end-users using technology developed through indigenous industry.

5. The Secure communication Grid should have required components to establish a packet switching core using standardized protocols and interfaces to support routing and transport of IPv4/IPv6 packets between various elements in a reliable manner. In addition to the forwarding plane, the Grid should provide distributed computing infrastructure using open source cloud or containerization technology to run application stack, applications related to operations and various enterprise applications to handle techno-logistics and administrative requirements.

6. The network should have a secure wire-line and wireless access segment to provide connectivity to end users deployed at separate geographical locations. The end user connectivity must support digital voice as well as data services offered in an integrated or segregated manner.

7. With the evolution of Internet technology to Web 2.0 and to 3.0 in future, the connectivity and computing landscape will witness significant technology transition requiring support for high to ultra-high bandwidth in the access / core, low-latency network connectivity, near zero-loss of packet in the core, and integrated security at every stage. The technology development for the project is expected to comply to these requirements.

Operational Requirements

6. The secure communication grid is expected to achieve the following operational requirements:-

(a) Hardware and Software used to establish the network must be security certified by an agency nominated by the GoI.

(b) The grid must support integration of narrow band to ultra-high band IT assets and systems. Narrow band integration would be realized over 100/1000Mbps Optical/Copper interface. Data center computing assets and centralized assets would be integrated over 40G/100G interfaces to ensure adequate bandwidth.

(c) Network should offer low-latency to various services through high-performance routing/forwarding plane.

Indigenization Objectives

7. The program is expected to meet the indigenization objectives articulated by GoI in various forums and policy letters. Following are the few key indigenization objectives:-

(a) The hardware used for establishing the secure communication grid must be designed & developed in India. The grid hardware should make maximum possible use of components developed/ manufactured in India. For non-Indian components (where used), effort should be to avoid any OEM lock-in and the design must be adaptable to chips from different makes/manufacturers, with minimal changes.

(b) Open source initiatives must be leveraged to reduce dependency on FOEM and to make technology developed free from royalty.

(Note: Few examples of open source initiatives are Openstack, CNCF Kubernetes & OpenRAN)

(c) Developmental agencies are encouraged to create/develop “India Specific Standard”.

(d) Requirements to collaborate with Academia and/or other Govt/Private research bodies, to incubate critical technologies can be accommodated in the Project Definition Document.

Secure Grid Components

8. Secure Grid will be an evolving network to meet the communication requirement in the next decade. The grid may have the following components to meet operational and enterprise communication requirements:-

(a) **Wire-line Customer Edge Device**. In the next decade, using the open protocols and technologies, the customer edge device must meet network reachability requirement. Wireline customer edge device must aggregate '**X**' number of end users and uplink the traffic towards the network core to meet inter-site and intra-site communication requirement. While forwarding the packets, the device must maintain stated Quality of Service (QoS) objectives. All the customer edge devices must be centrally configurable for provisioning, policing and monitoring. The network components must support extreme automation to support zero-touch provisioning, rectification. The customer edge device would be packaged to meet port and environmental requirements. The single box SD WAN type solution is preferred to include following features like WAN Load Sharing, Auto-Link failover, Zero-Touch Provisioning (ZTP), Auto Quality of Service, Firewall, VPN, Automated Notification Events and Alerts, Centralize Policy Management Console, ISP Agnostic, Easy, scalable any-to-any (full mesh) configuration, Fast activation of new connections, Integrated IPsec, Special feature for Automated Key input and periodic key rotation.

Note: Some of above stated features, in today's technology parlance, are being offered under the Software Defined Access Network (SD-ACCESS).

(b) **Wireless End User Device.** The mobility needs of the end user are planned through handsets based on 5G/6G/6G+ technologies. These devices must support packet switched voice and data. Voice signaling must be complaint to SIP (will all the latest enhancements). Data throughput must be as per the Open standards defined by the ITU-T nominated forums.

(c) **Wireline Voice Handset**. For static subscribers, IP based wire-line fixed handsets are required to be implemented. These handsets must be complaint to the SIP standards and all its applicable extensions/enhancements. It must be PoE enabled to draw the power from Customer Edge Device. The handset must support clear and secure communication between caller and callee. Security to be implemented to meet the quality of service requirements.

(d) **Call Control Functionality**. A converged redundant call control network is required to be implemented using the SIP open standard to integrate Wireless and Wireline handsets. The call control functionality must be based on open source technologies and must provide REST/gRCP/SOAP interfaces to integrate various feature services. The Call control network must meet following high-level requirements:-

(i) Must be highly redundant in nature. Deployment must be distributed across various geographical nodes to meet the redundancy criteria.

(ii) Must be scalable to handle more than 200,000 wire-line and wireless end users.

(iii) Must provide all typical Enterprise call control features including CNID/CLID.

(iv) Must have distributed Trunk Gateways to connect to the outside world.

(d) **Core Network Components**. Core network components would aggregate Customer edge devices deployed at a base and establish inter site communication using Optical and Radio links. These Optical and radio links would be made available by IAF using Industry standard interfaces such as 1G/10G/40G, drawn from the underlying transmission infrastructure. Core component must meet following qualitative requirements:-

(i) Provide functionality to terminate uplinks of Customer edge devices, wireless nodes, weapon systems and voice end points. Core component must establish policy protected intra-site and inter-site communication path.

(ii) The core network solution and its constituent components must support extreme-automation by adapting SD-WAN or its equivalent standard based technology. The solution to gather intelligence about networks, and accordingly make intelligent routing decisions based on the performance of each path.

(iii) The solution needs to imbibe vendor agnostic orchestration and automation engine that can connect to any vendor routing and switching gear using REST/SSH/SNMP-based adapters to control them, thereby allowing for a smooth transition from current to proposed new network.

(iv) The core network must be capable of identifying traffic flows and would provide differential treatment.

(v) The core network must converge in milliseconds to reduce impact on the deployed applications.

(vi) The network must be capable of integrating various kind of media (For example, optical, radio, satellite, tropo, and microwave links). However, all the links would be made available on Ethernet interfaces.

(vii) The core network must be configured with all the applicable Open standards and technologies to establish inter-site and intra-site reachability.

(viii) It must be feasible to define constraints for flow types to implement security solutions.

(ix) The core network must provide network functions, which can be provisioned from distributed locations. These network functions would be provided through VMs/Containers.

(x) The network and its components must support both in-band and out-of-band monitoring capability to monitor logs/traps and metrics.

(xi) The core network must provide functionality to define various logical topologies such as Hub-Spoke, Mesh and Star.

(xii) The core network must meet Telecom related environmental requirements.

(f) **Computing Layer**. The computing layer must be provided using open source cloud and storage technologies. The computing layer must use generic hardware components and should be completely vendor agnostic. The cloud must be scalable to meet the computing requirements of IAF for the next decade. The computing layer must be capable of provisioning following services:-

(i) Virtual Machines for legacy applications.

(ii) Containers.

(iii) Object Storage buckets.

(iv) Block Storage solution which can be attached to VMs.

(v) Firewall as a Software Function.

(vi) Software defined network function.

(vii) GPU nodes for AI/ML functions.

(viii) Automation layer for provisioning of computing components.

(g) **Quantum Encryption**. Use of quantum technology to develop indigenous hardware token based authenticator.

(a) **Operating System.** Indigenously developed OS based on kernel separation technology. To enable secure transfer of files from internet to intranet facing system while preventing infiltration of data from intranet to internet.

Support of Application

9. The secure grid envisaged to be implemented through this program would support various applications. An illustrative and representative list is as follows:-

(a) Air Defence application using client-server architecture. These applications are designed to function in real-time mode.

(b) Enterprise applications using Web1.0/Web2.0 technologies following2Tier/3Tier distributed client-server architecture. These applications are essentially of near-real time nature.

(c) Any-to-Any Voice call.

(d) Collaboration application such as voice and audio conferencing solution.

(e) Integration of weapon systems with Command and Control Centers.

(f) Exchange of high volume Imagery data (Non-Real time).

(g) Real-time Transmission of Video between sensor and consumers.

(h) Exchange of short/busty real time traffic over the network.

(i) Inter computing node replication and management traffic.

Lifecycle Management

10. Components (Hardware and Software) that would be supplied under the program must be under Long Term product support. The Long term product support would cover the followings:-

(a) Hardware repair and replacement for the faulty/obsolete components.

(b) Complete logistic management to pick up the faulty components/hardware from the installation location and its replacement with serviceable components/hardware.

(c) Continuous upgradation of software to integrate new features and standards.

(d) Removal of vulnerable hardware/software components through upgradation and replacement.

Realization Strategy

11. Secure network would be implemented in a staggered manner based on the availability of technology and its maturity to support military applications.

Compliance to Standards

12. All the components supplied as part of the Secure Grid must be compliant to open standards such as ITU-T/ITU-R, IETF, ISO etc.

13. The solution should preferably aim at the following: -

(a) **Network elasticity.** The ability to upgrade or downgrade capacity with ease, so that the organization can respond quickly to changing needs.

(b) **Built-in protection.** Ability to embrace integrated security into network infrastructure, to avoid the pitfalls of layered-on security tools, like security gaps and reduced performance. The security functions built into the network should no longer need to funnel traffic through a series of security appliances. Aim should be to reduce hops and security inspections and improved application performance.

(c) **Cloud-ready.** Integrate cloud services into network architecture to avoid application performance bottlenecks.

(d) **Zero Trust security.** The solution offered should be Zero Trust solutions that could work across multiple connectivity options and protect users when working from anywhere. Zero Trust security should not only protect users from threats but also prevent the lateral spread of malware.

14. **Industry Attributes:**

(a) Should be an Indian entity (as per provisions of Para 20, Chapter I of DAP 2020, including additional conditions at sub paragraphs (a) and (b)). (**Essential**)

Note: A copy of DAP 2020 is available on website of Ministry of Defence.

(b) Experience in manufacturing, integration and supply of electronics, communication and IT eqpt including development of related software/firmware (**desirable**).

(c) Familiarity with QA processes of DGAQA (**desirable**).

15. Interested **Indian** vendors may send their proposals by **30 July 2022**.

It is requested that, answers to questions at **Appendix B** may also be dovetailed by the industry in their response.

Interested respondents are also urged to read the provisions of “Make–I” procedure at Chapter III of DAP 2020 as the project will be progressed as per these provisions.

16. **Contact Details.** Any queries/further details of the case may be obtained from the Nodal Dte at Air Headquarters (Vayu Bhavan). Interested Indian vendors may forward their responses through letter/fax/email to the Nodal Directorate as follows:-

Nodal Directorate

Gp Capt Ops (CIT Security)
Dte of CIT Security
Room No 456, Air HQ (VB)
Rafi Marg, New Delhi – 110 106
Tele: 23011827
Email: kamakaya.14@gov.in

A copy of all communication should also be addressed to:-

Make PMU (AF); Room No 413; Air HQ (VB);
Telefax: 011-23013225
Email: makeind.af@gov.in