REQUEST FOR TRAINING PROPOSALS

DESIGN & DEVELOPMENT OF A QUANTUM KEY DISTRIBUTION DEVICE

Submission Deadline: 13th March, 2023 (Monday)

▪ **Training Objective**. National Center for Cyber Security is now looking for a training program to enable participants to develop a **Quantum Key Distribution (QKD) System** capable of seamlessly generating, transmitting and receiving secure keys over optical fiber channel of up to 1 km (minimum).

▪ **Team Composition**. The training may be imparted to a team of 5x members with following composition. However, team composition can be changed. Vendor may also identify qualification and experience of the team to extract max benefit in min training time:
   o 1x Software developer (C/C++/C#/PYTHON/JAVA etc.) to undertake all programming tasks.
   o 2x Hardware engineers (FPGA/DSP/SBC/Microcontrollers etc.) to undertake hardware tasks.
   o 1x Network engineer to undertake network and fiber communication related tasks.
   o 1x Physicist (Optronics expert) for all theoretical aspects.

▪ **Training Modules**.

The training must *preferably* involve following modules:

   o *Quantum Key Generation Module.* Generate a quantum key to be shared.

   o *Secure Channel Establishment Module.* Establish a secure channel over optical fiber to enable sharing of quantum-secure information (i.e. text, image, two-way audio/video calling).

   o *Quantum Key Transmission Module.* Encrypt and transmit generated quantum key (QK) using QKD protocols (i.e. BB84, BBM92, E91, etc.) over optical fiber up to a certain distance (e.g. 100m, 200m, from one building to another building, etc.). *At the minimum, participants will be familiarized (with identification of COTS components) for developing a 1 km QKD device*.

   o *Quantum Key Reception Module.* Receive and decrypt QK using QKD protocol (i.e. BB84, BBM92, E91, etc.) over optical fiber up to certain distance (e.g. 100m, 200m, from one building to another building, etc.) at the receiving terminal in real-time. *At the minimum, participants will be familiarized (with identification of COTS components) for developing a 1 km QKD device*.

   o *QKD Network Module.* Establishment of a scalable QKD network with at least 3x quantum nodes based on trusted node network technique. *At the minimum, participants will be familiarized (with identification of available options) for single or multi-mode fiber based communication and associated aspects of switching, routing, terminating etc*. Provision of preliminary understanding for wireless based communication may also be considered.

- **Essential Components**. Essential components (deliverables) for the training include (but not limited to) are as below. *Training proposal may include essential hardware for the purpose or identify for self-procurement by NCCS*:

    - *Practical use* of Photon Source and Photon Detector for QK transmission/reception along with identification of COTS components and key points for selection based upon the need for secure channel establishment over 1 km or 10 km distance.
    - *Establishment* of **Quantum channel** over optical fiber (single or multi-mode) along with identification of COTS components and key points for selection based upon the need for secure channel establishment over 1 km or 10 km distance.
    - *Practical implementation* of **polarization compensation** techniques in established quantum channel.
    - *Practical implementation* of **transmission and receiving of QK** using QKD Protocols (e.g. BB84, E91, etc.) up to 1km (at the minimum) over quantum channel. o *Development* of a cryptographic application **software suite with integrated quantum security** for information (text, image, video) encryption/decryption.
    - *Development* of a **hardware transmitter** system integrated with all of the above modules/techniques for transmission of quantum secure information.
    - *Development* of a **hardware receiver** system integrated with all of the above modules/techniques for real-time receiving of quantum-secure information.
    - *Development and Integration* of **error correction** and **privacy amplification** modules in QKD hardware (transmitter and receiver).
    - *Establishment* of a scalable **QKD network** with preferably, 3x quantum nodes based on trusted node network technique.

- **Training Venue**. Islamabad.

- **Administrative Support**. Administrative facilitations, if requested, can be provided to reduce overall cost of the training solution.

- **Supporting Documents**.   The proposal must be submitted with supporting documents stating technical and financial details associated with each training module including but not limited to following:
    - Tentative schedule, duration and number of participants with pre-requisites
    - Clear timelines for deliverables
    - Hardware and software to be procured/made available for the training
    - COTS components required for training

- **Contact**.
National Center for Cyber Security, Alpha-9, National Aerospace Science & Technology Park (NASTP), Chaklala Cantt., Rawalpindi.

Email: bilal.afzal@nccs.pk