Annex A2.3. Technical requirements for Deployment services of Software Licenses, Server and Network Hardware for the cyber-resilient architecture (Backup & Restore System) of the Central Election Commission (CEC) of Ukraine

1. Preparations

Analyse the existing IT infrastructure and document the configurations of components (virtual machine, service, etc.), including hardware specifications, software versions and network connections.

Analysis of the current state of the server and network infrastructure:

- Assessment of the capacity and performance of existing network switches and servers, network connections, software versions etc;
- Checking the configuration of switches for compatibility with the requirements of the software to be implemented;
- Assessment of network security and availability of redundant channels.

Checking the availability of the current data backup:

- Assessment of the current state of data backup and restore systems;
- Determining the need for additional measures to ensure fault tolerance.

2. Deployment and configuration of the Backup and Restore System

- Installation and configuration of network equipment.
- Installation and configuration of server equipment.
- Deployment and configuration of isolated Authentication System.
- Deployment and configuration of Backup & Restore System (BRS) software.
- Configuration of the role model of access to the BRS management.
- Connection of backup objects.
- Testing of backup procedures.

3. Integration with IBM Qradar

- Analysis of existing SIEM infrastructure based on IBM Qradar.
- Designing the logic of interaction with IBM Qradar.
- Provide integration with IBM Qradar for centralised collection of logs for further analysis and detection of potential threats in real time.

4. Testing

- Development of comprehensive testing program.
- Testing of the Backup & Restore System.
- Development of the testing report.

5. Documentation

Following documentation must be provided:

1. Description of Backup and Restore System architecture, that include:

- Installation and configuration of BRS software
- Configuration of BRS network environment
- Configuration of access to BRS administrative interfaces
- Configuration of backup policies
- Configuration of data sources for backup.

2. Data backup procedures, that include:

- List of backup objects
- Data backup procedures
- Data recovery procedures
- Backup rotation
- Backup protection
- Review and modification of these procedures.

3. Testing program (developed by the Bidder and approved by the CEC).

4. Testing report.

6. Quality of services and oversight

The bidder must provide a copy of the authorization letter from the vendors – Fortinet, Commvault and Lenovo – or from the official representative office of the specified manufacturer in Ukraine, indicating the subject of the procurement, stating that the bidder is an active authorized partner of the vendor, and also confirming the right of the bidder to participate in the bidding in accordance with the subject of the procurement.

The bidder must provide a confirmation that the bidder has employees with appropriate qualifications who have the necessary knowledge and experience to provide the services stipulated in the Technical Requirements of the subject of procurement and will be involved during the performance of the contract (indicating full name, position, copy of the valid certificates).

- Availability of at least 2 (two) employees, with a valid Fortinet certificate.
- Availability of at least 2 (two) employees, with a valid Lenovo Certified Storage certificate.
- Availability of at least 2 (two) employees, with a valid Commvault certificate.

Hardware warranty/support (OEM/vendor) shall be provided for 3 years. Technical support, including the scheduled maintenance for 1 (one) year after deployment, should include the following services:

- Consultations of settings and refining for the Backup and Restore System
- Consultations on the update processes of the Backup and Restore System

Clear SLA should also be provided, in terms of response time and problem resolution, available support channels and a defined escalation process.