INTERNATIONAL INSTITUTE FOR DEMOCRACY AND ELECTORAL ASSISTANCE

TENDER REFERENCES NO: 2026-01-082

Terms of Reference (ToR) for Procurement and Delivery of Software Licenses, Server and Network Hardware and Deployment Services for the cyber-resilient architecture (Backup & Restore System) of the Central Election Commission (CEC) of Ukraine

1. Background

As Ukraine prepares for post-war elections, its Central Election Commission (CEC) faces acute technical challenges, including cyber threats, outdated infrastructure, and gaps in ICT systems.

Before the war, the CEC began deploying a Backup and Restore System based on CommVault software and using a tape library. Currently, the existing solution remains incomplete and does not provide a sufficient level of reliability and disaster recovery for the entire ICT system.

The digitalization of electoral processes involves the accumulation and processing of large volumes of data, including restricted-access information such as personal data. The loss of election-related data or the inability to restore information systems is particularly sensitive for society during the electoral process.

Building a highly available and efficient backup, archiving, and recovery system will protect the CEC's information systems from cyber threats and enhance readiness for emergency situations, which is crucial in the context of Russia's ongoing aggression.

This system is designed to:

- Ensure data security – Guarantee the preservation and confidentiality of critical data by utilizing modern backup and encryption technologies.
- Enhance disaster resilience – Enable rapid recovery of information systems in the event of failures, cyberattacks, or other force majeure circumstances.
- Ensure compliance with standards – Align backup and archiving processes with international cybersecurity standards and Ukraine's regulatory requirements.
- Strengthen resilience to attacks – Create an autonomous backup infrastructure independent of compromised authentication and authorization services.
- Support scalability – Allow for system adaptation to the organization's growing needs and infrastructure changes.

Without an effective and scalable backup system, risks related to resilience, data recoverability, and cybersecurity increase, leading to potentially catastrophic consequences for both critical public information and communication systems and the entire information infrastructure of the Commission.

The implementation of this project will result in a modern, scalable, and secure backup system that meets the CEC's needs and minimizes the risks of data loss and operational disruptions during electoral processes.

2. **Objectives of the Assignment**

IDEA requires a reliable Bidder to ensure effective, secure, and compliant procurement and delivery of Software Licenses, Server and Network Hardware and Deployment Services for a Backup & Restore System of the CEC of Ukraine in preparation for post-war elections.

3. **Scope of Work**

3.1 The selected Bidder will be expected to deliver Software Licenses, Server and Network Hardware and Deployment Services. Any other software or / and hardware products or related services that may be required by the CEC in the future and are relevant to this procurement may be procured under Framework Contract to be concluded as an outcome of this tender based on a separate quotation.

3.2 In general, the backup and restore system should provide the following functions:

- A single interface for managing backup processes and transferring data to the archive, according to specified policies across the entire organization.
- Centralized management of data protection policies.
- Peer-to-peer confirmation of destructive operations.
- Built-in support for Multifactor Authentication and FIDO2 protocol.
- Vertical and horizontal scaling (by adding additional servers and software licenses).
- End-to-end data encryption between the agent and the server.
- Data encryption in backups.
- Support for event logging in Syslog format for integration with the SIEM system.
- Setting up backup policies approved at the organization level.
- Role-based access model to backup storage resources.
- End-to-end reporting on used storage resources for productive data, backups, and archives.
- End-to-end monitoring and notification of backup and archiving processes.
- Interoperability with tape libraries without additional licensing (existing tape library provided by CEC).
- Full-featured web interface that allows you to configure, create, monitor data backup status, SLA compliance, and have a user self-service portal.
- Copy file systems of the following OS:
    - Windows
    - Linux (Oracle Linux, Red Hat Enterprise Linux, CentOS, Suse Linux (SLES))
    - FreeBSD
    - Solaris
- Copy data in "hot mode" of the following DBMS and applications:
    - Microsoft Active Directory / SQL Server / Exchange Server / SharePoint Server
    - Oracle Database
    - MySQL
    - PostgreSQL
- Create backups in "hot mode", as well as full and granular recovery of virtual machines in environments:
    - VMware
    - Microsoft Hyper-V
    - Open Stack
    - RHEV
- Object-by-object recovery of the MS Active Directory

- Object-by-object recovery of the MS Exchange directory
- Support for any devices for storing backups and archives, including disk systems (DAS, SAN, NAS, VTL), tape libraries (existing tape library provided by CEC)
- Multiplexing of data streams when working with tape drives (existing tape library provided by CEC)
- Creation of more than two additional backup and archive copies
- Limiting the available network bandwidth for backup
- Generation of reports on SLA performance, schedules and status of backup, accounts, permissions, inheritance of permissions
- Interaction of external systems with the backup system using REST API.

3.3 The backup and restore system should be implemented on a separate set of equipment with limited access to form an isolated fault domain and using an autonomous authentication domain (separated LDAP based on FreeIPA software, deployed under Red Hat Enterprise Linux with high availability, acting as the central identity manager for MFA), which should ensure the cyber resilience of the organization.

3.4 The backup and restore system should provide the ability to backup, archive and restore data for:

- Up to 100 virtual machines.
- Up to 5 TB uncompressed source data that needs protection (for data on hardware servers).
- Long term storage up to 100 TB of data at the implementation stage.·
- RTO (maximum allowable recovery time): no more than 4 hours.
- RPO (maximum allowable data loss): no more than 15 minutes.

3.5 General list of Software Licenses, Server and Network Hardware and Deployment Services that needed to be procured and delivered is provided below in Table 1.

Table 1 Cyber-resilient backup and recovery system architecture (Phase 1)

#	Item	Q-ty
1.	Next Generation Firewall (4x10GE, 4x25G, 18 x GE RJ45 ports, 8 x GE SFP slots, dual AC PS), 3 years support	2
2.	Network switch (2x10G, 48x25G, 8x100G, dual AC PS), 3 years support	2
3.	Backup Management Server (12-core CPU, 128 GB RAM, 2x480 GB SATA SSD, 2x1.92TB SATA SSD), Windows Server 2025 Standard (16 core) – MultiLang, 3 years support	1
4.	Data storage server, Commvault Data layer – HyperScale X (2x16-core CPU, 512 GB RAM, 2x960 GB SATA SSD, 2x480 GB SATA SSD, 2x3.2TB Mixed Use NVMe PCIe 4.0 x4 HS SSD, 12x16TB 7.2K SAS 12Gb), 3 years support	3
5.	Anti-Malware Server (2x12-core CPU, 128 GB RAM, 2x480 GB SATA SSD, 2x1.92TB SATA SSD), Windows Server 2025 Standard (16 core) – MultiLang, 3 years support	1
6.	Authentication System Server for FreeIPA (8-core CPU, 32 GB RAM, 2x480 GB SATA SSD), 3 years support	2
7.	Additional cables for existing equipment - 3m LC-LC OM4 MMF Cable	14
8.	Addition modules - 25GE SFP28 transceiver module, short range 25 GE / 10 GE SFP28 transceiver module, short range 100m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP28 slots	20
9.	Red Hat Enterprise Linux Server, with Standard Maintenance Support 3Y (for Authentication System Servers)	2

#	Item	Q-ty
10.	Commvault Cloud Cyber Resilience Software, Per Front-End Terabyte, Perpetual with Standard Maintenance Support 3Y	5
11.	Commvault Cloud Cyber Resilience Software for Virtual Machines, Per VM (10-Pack), Perpetual with Standard Maintenance Support 3Y	10
12.	Commvault Cloud Hyperscale X Reference Architecture 12-Drive Node, Per Node, Perpetual with Standard Maintenance Support 3Y	3
13.	Deployment services for the cyber-resilient architecture	1

3.6 The detailed technical specification of the Software Licenses, Server and Network Hardware that needed to be procured and delivered is provided in Annex 2.2 (Specification in Annex 2.2 takes precedence over the general list in Table 1 above).

3.7 Additional licenses may be procured from the successful Bidder if needed, and this (should the need arise) will be the subject of a separate quotation. As an outcome of this tender, the framework contract will be concluded with the bidder.

3.8 The detailed technical requirements for deployment of the Software Licenses, Server and Network Hardware that needed to be procured and delivered is provided in Annex 2.3 (Specification in Annex 2.3 takes precedence over the general list in Table 1 above).

4. **Timing and Work Plan**

Project implementation schedule should not exceed 180 calendar days starting from the contract signature. A detailed timeline of deliverables will be developed and agreed with the selected bidder.

5. **Deliverables and Reporting Requirements**

5.1 The deliverables for this assignment shall include:

- Software Licenses, Server and Network Hardware according to Annex 2.2
- CEC Acceptance Letter which proves the delivery of Software and Hardware
- Deployment Services for the cyber-resilient architecture according to Annex 2.3
- CEC Acceptance Letter which proves the acceptance of Deployment Services.

5.2 As the part of reporting the Bidder must submit:

- An initial delivery plan within 3 working days of contract signature
- Biweekly progress reports highlighting technical tasks completed, blockers, and next steps
- Final delivery report including:
    - List of delivered software licenses, hardware and deployment services
    - Documentation packages (see below in 7.2 and Annex 2.3).

The technical documentation of acceptance tests is provided for approval in electronic (PDF) and paper form in Ukrainian language.

6. **Management and Organization**

From International IDEA, a relevant Project Manager will be designated to provide relevant guidance for the achievement of the overall objective of the assignment and deliverables. All bidder communications shall be directed to the designated IDEA Project Manager. Final deliverables must be jointly confirmed by IDEA and the designated CEC technical contact.

All questions arising during the course of the project should be coordinated with Tetiana Bibik, International IDEA Project Manager (e-mail: t.bibik@idea.int).

7. Monitoring and Evaluation

This Monitoring and Evaluation section defines how International IDEA will track the progress, quality, and outcomes of the purchase and delivery of Software Licenses, Server and Network Hardware for the CEC of Ukraine. The aim is to ensure timely purchase and secure delivery, compliance with technical specifications.

7.1 Key Performance Indicators (KPIs):

- Delivery of all Software licenses within 30 calendar days of contract signature
- Delivery of all Server and Network Hardware within 120 calendar days of contract signature
- Compliance with the technical specifications outlined in Annex 2.2
- Provide deployment services for the cyber-resilient architecture within 180 calendar days of contract signature
- Compliance with the technical requirements for deployment services outlined in Annex 2.3
- Delivery of a valid Acceptance Letter from the CEC.

7.2 Monitoring Activities:

- Biweekly check-ins with the bidder to track progress against the delivery timeline
- Document verification: review of delivery reports, license documentation, and invoices
- Confirmation with the CEC of receipt, functionality, and usability of the cyber-resilient architecture.

7.3 Evaluation Framework

Evaluation Criteria:

- Adherence to timeline milestones
- Full compliance with architecture and integration requirements in Annex 2.2 and Annex 2.3.
- Absence of critical errors in new cyber-resilient architecture
- Quality and completeness of documentation (design, test protocols, architecture passport)

Evaluation Process:

- Baseline technical assessment at project launch
- Mid-term evaluation at completion of deployment
- Final evaluation after testing and integration
- Feedback survey from CEC technical staff

Annexes (to be provided)

Annex A2.2. Technical specifications of Software Licenses, Server and Network Hardware for the cyber-resilient architecture (Backup & Restore System) of the Central Election Commission (CEC) of Ukraine

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

Annex A2.4. Documentation provided by Bidder