CNCCCITC 中化建国际招标有限责任公司

CNCCC INTERNATIONAL TENDERING CO, LTD.

亚洲开发银行贷款湖南低碳城市试点建设项目

开发，提供安装和调试智能城市范围的 ICT 平台操作系统（合同号：G201-ICT）

招标文件的澄清和补遗 No.5

Development, Provision Installation and Commissioning of the Smart City-wide ICT Platform Operation System（Contract No.: G201-ICT）

Clarification and Addendum No.5 of the BD

本澄清和补遗文件以英文版为准，中文版仅供参考，如中英版本有冲突，以英文版为准：

The Clarification and Addendum is prepared in English and the Chinese serves as a reference ONLY. The English shall prevail if there is any discrepancy between English and Chinese.

投标人：

Dear Bidders,

根据需要，对招标文件做如下澄清和补遗：

The clarifications and addenda of the BD are as follows.

一、对招标文件修改如下：

The addenda of the BD are as follows:

1、 招标文件第六章增加如下内容：

1.Add the following content to Section 6 of the BD.

一、湘潭政务云现状

1、湘潭政务云鲲鹏资源池

一期鲲鹏资源池包括鲲鹏服务器，按照超融合架构部署，超融合节点同时提供计算跟存储能力，控制节点由服务器组成高可用集群，保证平台稳定性；存储集群节点组成独立的对象存储/共享文件存储集群；容器节点组成一个完整的容器云平台集群；一期鲲鹏资源池能提供的虚拟化计算存储资源总量为：vCPU 6144 核、内存 13598G、固态云盘（信创集群）

34T、普通云盘（信创集群）490T。

2、湘潭政务云飞腾资源池

二期飞腾资源池由飞腾服务器组成，同样采用超融合架构部署。超融合节点同时提供计算和存储能力，控制节点由服务器组成高可用集群，在保证平台稳定性的同时可扩容至更大规模集群；二期虚拟化资源池的整体技术架构与一期的架构保持一致，通过一套云管理平台确保一期的分布式存储后台管理、物理机监控、应用容器、运维管理、多云管理等云平台组件能直接接管二期虚拟化资源池。二期飞腾资源池能提供的虚拟化计算存储资源总量为：vCPU 8960核、内存 14300G、固态云盘 49T、普通云盘 308T。

3、湘潭政务云公共资源池

公共资源池负责提供整个基于ARM架构CPU的政务云业务系统需要用到的公共服务，如DNS服务、NTP服务、日志服务、堡垒机服务等。在保障高安全性的前提下，最大限度满足基于ARM架构CPU的政务云上业务系统的公共需求。

二、湘潭市电子政务外网网络现状

- **互联网接入**：三个运营商互联网出口线路通过负载均衡设备接入，下联IPS入侵防御、防火墙等安全设备接入核心交换区。网络设备和安全设备均为双机部署。
- **专网接入**：湘潭市党政内部工作专网是全市党政机关内部人员使用的网络，与互联网和外网均不相通，电子政务外网采用MPLS-VPN技术承载专网，实现专网与其他网络的逻辑隔离。
- **外网接入**：湘潭市各委办局租用光纤链路，通过河东、河西汇聚与电子政务外网核心交换机进行相连。湘潭市各单位终端可以通过该链路连通电子政务外网，再通过电子政务外网的互联网出口访问互联网。
- **政务云互联网区**：此区域主要是云平台中需要对互联网提供服务的业务系统部署在此，此区域边界有2台Web应用防火墙以及1台抗DDOS安全网关进行边界防护。本项目中的统一电子印章、人脸核身、视频会议调度等子系统部署在互联网区。
- **政务云政务外网区**：此区域主要是云平台中外网业务系统提供服务，边界有2台防火墙进行安全防护。本项目中的大多数子系统部署在外网区。
- **政务云政务专网区**：此区域主要是云平台中专网业务系统提供服务，边界有2台防火墙进行安全防护。专网区是为特殊应用服务的。

- **政务云政务公共区：**此区域主要是云平台中共用业务系统提供服务，公共区的网络与政务云外网区、互联网区、专网区的网络都是连通的。本项目中的运维平台、统一运营网关、统一认证等子系统部署在公共区。

三、密码服务平台现状

1） 密码机

密码机为可实现高速密码算法运算的专用硬件设备，采用支持全SM2、SM3、SM4、SM9系列国家商用密码算法的密码机。

2） 密钥管理系统

密钥管理系统实现SM2、SM3、SM4、SM9算法的密钥管理，对用户实体的身份标识、私钥生成、私钥分发进行综合管理。

3） 协同签名系统

协同签名系统是一款基用SM2和SM9标识密码算法技术为用户提供协同签名服务的系统，配合密码软件模块，完成数字签名运算，实现用户在无安全介质场景下的密码算法应用。

4） 时间戳服务器

支持北斗卫星时间源，基于PKI技术的时间戳权威系统，对外提供精确可信的时间戳服务。

5） 统一密码服务平台

统一密码服务平台为上层应用系统提供统一的密码服务，上接业务应用，下联密码基础设施，将密码基础设施统一管理并资源池化，对外提供统一服务接口和管理入口。

6） 密码安全中间件

安全中间件以SDK开发包形式集成在应用系统中，提供可方便调用的认证、加解密、签名验签接口。

7） VPN安全网关

VPN安全网关实现用户端与服务端之间、应用系统之间数据安全加密传输，采用国密算法实现对接入用户的身份认证，并支持基于IP、端口、账号等设置详细的访问控制。

8） 数据库加密系统

数据库加密系统，基于国密算法（支持SM2/3/4/9）和安全的密钥管理，实现安全可控、可管理的数据库敏感字段加密，支持特定字段加密、全库加密，支持密文查询检索，支持数据加密后的还原和安全共享交换。

9） 文件加密系统

文件加密系统实现对各类文档、音视频等非结构化文件本身的存储加密和读取时的解密。

10）智能密码钥匙

智能密码钥匙（Ukey）作为PC端密码模块，用于数字证书以及用户密钥的安全存储介质，并基于USB接口提供硬件算法运算能力。

11）LRA节点

湘潭市LRA节点主要是建立与电子政务建设相配套的数字证书发放系统受理点，该系统是湖南省RA节点的延伸，以国家电子政务外网CA体系为基础平台。

四、WAF设备参数

厂商：安恒信息

品牌及型号：安恒明御WAF

系统及版本：嵌入式Linux系统V3.0.4.3.3(18-10-23)

参数：标准2U硬件平台，含2*GE电管理口，4*GE电业务口(含2组硬件BYPASS模块)。4*SFP光业务口(标配多模SFP模块*2)，4个万兆光口。硬盘:1T，1*RS232串口标准，可热插拔电源模块*2，应用层吞吐量6Gbps，HTTP最大并发数35万，物理保护链路4路，最大保护站点无限制。WAF-V3系统引擎，含核心安全引擎及基于特征值的安全护模块。”

I. Xiangtan Government Cloud Status

1. Xiangtan Government Cloud Kunpeng Resource Pool

Phase I of the Kunpeng Resource Pool includes Kunpeng servers, deployed in accordance with the hyper-converged architecture, with hyper-converged nodes providing computing and storage capabilities at the same time, and control nodes consisting of servers in highly available clusters to ensure platform stability. The storage cluster nodes form an independent object storage/shared file storage cluster; the container nodes form a complete container cloud platform cluster; the total amount of virtualized computing and storage resources provided by Phase I of the Kunpeng Resource Pool is: vCPU 6144 cores, 13598G of memory, 34T of solid-state cloud disk (Information Innovation Cluster), and 490T of ordinary cloud disk (Information Innovation Cluster).

2. Xiangtan Government Cloud Phytium Resource Pool

Phase II Phytium Resource Pool consists of Phytium servers, also deployed with hyper-converged architecture. The hyper-converged nodes provide both computing and storage capabilities, and the control node consists of servers that form a highly available cluster, which can be scaled up to a larger cluster while ensuring the stability of the platform. The overall technical architecture of the Phase II virtualized resource pool is consistent with that of Phase I. A set of cloud management platforms ensures that the cloud platform components of Phase I, such as distributed storage background management, physical machine monitoring, application containers, operation and maintenance management, and multi-cloud management, can directly take over the Phase II virtualized resource pool. The total amount of virtualized computing and storage resources that the Phase II Phytium resource pool can provide is: 8960 vCPUs, 14300G memory, 49T solid-state cloud disk, and 308T regular cloud disk.

3. Xiangtan Government Cloud Public Resource Pool

The public resource pool is responsible for providing the public services required by the entire government cloud business system based on ARM architecture CPU, such as DNS service, NTP service, logging service, bastion service, etc. Under the premise of guaranteeing high security, it maximally meets the public needs of the business systems on the ARM architecture CPU-based government cloud.

II. Xiangtan E-government Extranet Network Status

- **Internet access**: Internet export lines of three carriers are accessed through load balancing equipment, and downlinked IPS intrusion prevention, firewall and other security equipment are accessed to the core switching area. Both network equipment and security equipment are deployed as dual-machine.
- **Private network access**: Xiangtan City Party and Government internal work network is the network used by the internal staff of the city's Party and

Government organs, which is not connected to the Internet and the extranet, and the e-government extranet adopts MPLS-VPN technology to carry the private network, so as to realize the logical isolation of the private network from the rest of the network.

- **Extranet access:** All commissions and offices in Xiangtan City rent fiber-optic links, which are connected to the core switches of the e-government extranet through Hedong and Hexi convergence. The terminals of Xiangtan Municipal units can connect to the e-government extranet through this link and then access the Internet through the Internet exit of the e-government extranet.
- **Government cloud Internet area:** This area is mainly where the business systems in the cloud platform that need to provide services to the Internet are deployed, and there are two Web application firewalls and one anti-DDOS security gateway for border protection at the border of this area. The unified electronic seal, face recognition, video conference scheduling and other sub-systems in this project are deployed in the Internet area.
- **Government cloud extranet area:** This area is mainly used for providing services for extranet business systems in the cloud platform, and there are two firewalls at the border for security protection. Most of The subsystems in this project are deployed in the extranet area.
- **Government cloud dedicated network area:** This area is mainly dedicated network business systems in the cloud platform to provide services, and there are two firewalls at the border for security protection. The private network area is for special application services.
- **Government cloud public area:** This area is mainly for common business systems in the cloud platform to provide services. The network in the public area is connected to the networks in the government cloud extranet area, Internet area and private network area. The operation and maintenance platform, unified operation gateway, unified authentication, and other subsystems in this project are deployed in the public area.

III. Password Service Platform Status

1) Cipher Machine

The cipher machine is a special hardware device that can realize high-speed cryptographic algorithm operation, and it adopts the cipher machine that supports the national commercial cipher algorithm of the whole SM2, SM3, SM4 and SM9 series.

2) Key Management System

The key management system realizes key management of SM2, SM3, SM4 and SM9 algorithms, and carries out comprehensive management of identity identification, private key generation and private key distribution of user entities.

3) Collaborative Signature System

Collaborative Signature System is a system based on SM2 and SM9 identification cryptographic algorithm technology to provide users with collaborative signature services, together with the cryptographic software module, to complete the digital signature operation, so as to realize the application of cryptographic algorithms for users in the scenario without secure media.

4) Time Stamp Server

It supports BeiDou satellite time source and PKI technology-based timestamp authoritative system to provide accurate and trustworthy timestamp service to the outside world.

5) Unified Password Service Platform

The unified password service platform provides unified password service for upper-level application systems, connects business applications upwards and password infrastructure downwards, manages and pools resources in password infrastructure, and provides unified service interface and management portal to the outside world.

6) Password Security Middleware

The security middleware is integrated into the application system in the form of SDK development kit, providing interfaces for authentication, encryption and decryption, as well as signature verification that can be easily invoked.

7) VPN Security Gateway

VPN security gateway realizes secure and encrypted transmission of data between user and server as well as between application systems. It adopts national cryptography algorithms to realize identity authentication of access users and supports detailed access control based on IP, port and account number.

8) Database Encryption System

Database encryption system, based on national cryptography algorithms (supporting SM2/3/4/9) and secure key management, realizes secure, controllable and manageable encryption of sensitive database fields, supports encryption of specific fields, encryption of the whole database, ciphertext query and retrieval, and supports restoration of encrypted data and secure sharing and exchange.

9) File Encryption System

File encryption system realizes storage encryption and decryption of unstructured files such as documents, audio and video.

10) Ukey

As a password module for PC, Ukey is used as a secure storage medium for digital certificates as well as user keys, and provides hardware algorithmic computing capability based on USB interface.

11) LRA node

Xiangtan LRA node mainly establishes the acceptance point of the digital certificate issuance system that is compatible with the construction of e-government affairs, which is an extension of the RA node in Hunan Province. The CA system of the national e-government affairs extranet is taken as the basic platform.

IV. WAF Equipment Parameters

Manufacturer: Dbappsecurity Co., Ltd

Brand and Model: WAF

System and Version: Embedded Linux System V3.0.4.3.3(18-10-23)

Parameters: Standard 2U hardware platform with 2*GE electrical management ports and 4*GE electrical service ports (including 2 sets of hardware BYPASS modules). 4*SFP optical service ports (standard multi-mode SFP module*2), 4 10Gb optical ports. Hard disk:1T, 1*RS232 serial port standard, hot-swappable power supply module*2, 6Gbps application layer throughput, 350,000 HTTP maximum concurrency, 4 physical protection links, unlimited maximum protection sites. WAF-V3 system engine, including the core security engine and feature value-based security protection module.”

2、招标文件第二章 投标资料表 “投标人须知”第24.1款：
原文件为：
“递交投标文件的截止时间是：
日期：2024年11月13日……”
修改为：
“递交投标文件的截止时间是：
日期：2024年11月21日……”
1. ITB 24.1, Section 2 of the BD (Bid Data Sheet):
The original is:
“The deadline for bid submission is:
Date: November 13, 2024.……”
Revised as:
“The deadline for bid submission is:
Date: November 21 2024.……”

3、招标文件第二章 投标资料表 “投标人须知”第27.1款：
原文件为：
“开标日期和时间：2024年11月13日上午10:00时……”
修改为：
“开标日期和时间：2024年11月21日上午10:00时……”
2. ITB 27.1, Section 2 of the BD (Bid Data Sheet):
The original is:
“The bid opening shall take place at:
Date and time: 10:00 a.m. on November 13, 2024.……”
Revised as:
“The bid opening shall take place at:
Date and time: 10:00 a.m. on November 21, 2024.……”

特此澄清和补遗。
The clarification and addendum are as above.

请投标人收到此函后在回执处签章，扫描回执到 cnooctj@qq.com、wuxiyu0722@163.com。

On receiving this Addendum, please send the photocopy of the receipt with signature and official stamp to cnooctj@qq.com、wuxiyu0722@163.com.

CNCCC International Tendering Co., Ltd.
November 4, 2024
中化建国际招标有限责任公司
2024年11月4日

中化建国际招标有限责任公司

回 执/Return Receipt

本公司已于 2024 年 11 月 4 日收到邮件发来的《开发，提供安装和调试智能城市范围的 ICT 平台操作系统（合同号：G201-ICT）招标文件的澄清和补遗 No. 5》共 11 页。

This is to confirm that we have received the Clarification and Addendum No.5 dated November 4, 2024 for Development, Provision Installation and Commissioning of the Smart City-wide ICT Platform Operation System (Contract No.: G201-ICT). 11 pages in total.

投标人名称：_________（公章）_________

Bidder name: _________（Official Stamp）_________

授权代表：_________（签字）_________

Authorized Representative: _________(Signature)_________

Date 日期：