浙江省动物疫病预防控制中心政府采购
网络安全升级服务项目

招标文件

采购方式：公开招标

项目编号：**CTZB-2021090194**

采购人：浙江省动物疫病预防控制中心（盖章）

采购代理机构：浙江省成套招标代理有限公司（盖章）

二〇二一年九月

目录

第一章　招标公告

项目概况

浙江省动物疫病预防控制中心网络安全升级服务项目的潜在投标人应在浙江政府采购网（http://zfcg.czt.zj.gov.cn/）获取（下载）招标文件，并于 2021 年 9 月 29 日 09 时 00 分（北京时间）前递交（上传）投标文件。

一、项目基本情况

项目编号：CTZB-2021090194

项目名称：网络安全升级服务项目

采购方式：公开招标

预算金额（元）：1080000

最高限价（元）：1080000

采购需求：

序号	标项名称	数量	单位	预算金额（元）	简要技术要求	备注
1	网络安全升级服务	1	项	1080000	网络安全升级服务，具体内容详见招标文件。	依据：【2021】58392 号、【2021】58393 号、【2021】58394 号、【2021】58395 号、【2021】58397 号； 最高限价：1080000 元； 类型：服务项目。

合同履行期限：按招标文件规定。

本项目（否）接受联合体投标。

二、申请人的资格要求：

1. 基本资格要求：

（1）满足《中华人民共和国政府采购法》第二十二条规定，未被“信用中国”（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单。

2. 落实政府采购政策需满足的资格要求：

本项目为服务项目，本项目服务属于**【软件和信息技术服务业】**，要求服务全部由中小企业承接，即提供服务的人员为中小企业依照《中华人民共和国劳动合同法》订立劳动合同的从业人员。中小企业是指满足《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）第二条规定的企业，监狱企业、残疾人福利性单位视为小型、微型企业；

3. 特定资格要求：

（1）单位负责人为同一人或者存在直接控股、管理关系的不同投标人，不得参加同一合同项下的政府采购活动；

（2）根据《关于规范政府采购供应商资格设定及资格审查的通知》（浙财采监[2013]24 号）第 6 条规定接受金融、保险、通讯等特定行业的全国性企业所设立的区域性分支机构（应依法办理了工商、税务和社保登记手续，获得总公司（总机构）授权或能够提供房产权证或其他有效财产证明材料，能证明其具备实际承担责任的能力和法定的缔结合同能力）、以及个体工商户、个人独资企业、合伙企业（应依法办理了工商、税务和社保登记手续，能够提供房产权证或其他有效财产证明材料，能证明其具备实际承担责任的能力和法定的缔结合同能力）；

（3）非联合体。

三、获取招标文件

时间：招标公告发布之日起至投标截止时间前；

地点：浙江政府采购网（http://zfcg.czt.zj.gov.cn/）；

方式：供应商通过“浙江政府采购网”在线获取（招标公告下方选取“潜在供应商”处“获取采购文件”），不提供纸制版招标文件；供应商只有在“浙江政府采购网”完成获取招标文件申请并下载了招标文件后才视作依法获取招标文件；

售价（元）：0。

四、提交投标文件截止时间、开标时间和地点

提交投标文件截止时间：2021 年 9 月 29 日 09 时 00 分（北京时间）；

投标地点（网址）：政府采购云平台（https://www.zcygov.cn）；

开标时间：2021 年 9 月 29 日 09 时 00 分；

开标地点（网址）：在政府采购云平台（https://www.zcygov.cn）上开启投标文件。

五、公告期限

自本公告发布之日起 5 个工作日。

六、其他补充事宜

1. 投标人认为招标文件使自己的权益受到损害的，可以自获取招标文件之日或者招标文件公告期限届满之日（在招标文件公告期限届满后获取招标文件的，以招标文件公告期限届满之日为准）起 7 个工作日内，以书面形式向采购人和采购代理机构提出质疑。提出质疑的投标人对采购人、采购代理机构的答复不满意或者采购人、采购代理机构未在规定的时间内作出答复的，可以在答复期满后十五个工作日内向同级政府采购监督管理部门投诉；质疑函范本、投诉书范本请到浙江政府采购网下载专区下载。

2. 其他事项

2.1 采购项目需要落实的政府采购政策：

本项目对符合《政府采购促进中小企业发展管理办法》规定的中小企业、监狱企业、残疾人福利性单位给予政策扶持，执行节能产品政府强制采购和优先采购政策，执行环境标志产品政府优先采购政策。

经采购人确认，本项目属于预留份额专门面向中小企业采购项目。

2.2 采购信息发布媒介：浙江政府采购网（http://zfcg.czt.zj.gov.cn/）。

2.3 未按招标公告规定获取招标文件的潜在投标人不得对招标文件提出质疑，其投标文件将被拒绝；通过本公告下方“游客，浏览采购文件”下载的招标文件仅供浏览，不视作依法获取招标文件。

2.4 在线投标响应（电子投标）说明：

（1）本项目采用政府采购电子化交易；

（2）投标人应在投标前完成 CA 数字证书办理。（办理流程详见 http://zfcg.czt.zj.gov.cn/bidClientTemplate/2019-05-27/12945.html）；

（3）投标人应安装“政采云投标客户端”，电子投标工具请投标人自行前往浙江政府采购网下载并安装，（下载网址：http://zfcg.czt.zj.gov.cn/bidClientTemplate/2019-09-24/12975.html）；

（4）电子交易具体流程详见操作指南：登录政府采购云平台（https://www.zcygov.cn/），从首页-服务中心-帮助文档-项目采购-电子招投标，查看文档和视频；

（5）如有疑问，可致电政府采购云平台技术支持热线咨询，联系方式：400-881-7190；

2.5 开标时间后 30 分钟内，投标人须登录政府采购云平台，用“项目采购-开标评标”功能解密投标文件（线上）。

2.6 中标人应在合同签订前完成政府采购云平台（https://www.zcygov.cn/）全部注册步骤并成为正式注册入库供应商，否则将导致合同款无法正常支付，责任由中标人承担。请投标人尽早完成注册。https://middle.zcygov.cn/settle-front/#/registry（供应商注册页面）。

七、对本次采购提出询问、质疑、投诉，请按以下方式联系。

1.采购人信息

名称：浙江省动物疫病预防控制中心

地址：杭州钱塘新区下沙街道十五堡南浙江牧业监测大楼

项目联系人（询问）：陈凯

项目联系方式（询问）：0571-56269718

质疑联系人：陈洁

质疑联系方式：0571-56269703

2.采购代理机构信息

名称：浙江省成套招标代理有限公司

地址：杭州市文晖路 42 号现代置业大厦西楼 18 层 1804 室

项目联系人（询问）：卢亚君

项目联系方式（询问）：0571-85830198、85830257

质疑联系人：冯东东

质疑联系方式：0571-85331293

3.同级政府采购监督管理部门

名称：浙江省财政厅政府采购监管处

地址：杭州市环城西路 37 号

联系人：倪文良、吴聪瑜

监督投诉电话：0571-87057615、87058489

第二章　采购需求总体要求

一、技术标准、规范（不限于以下）

1、国家规定的标准及规范，按最新的标准及规范执行；

2、行业标准及规范，按最新的标准及规范执行；

3、与服务有关的材料设备质量应符合中华人民共和国及产品品牌所在国的有关质量标准，上述标准如有不一致，执行两者中更严格的标准；

4、其它相关标准及规范，按最新的标准及规范执行。

二、采购内容及需求

具体要求详见招标文件的“第三章 采购需求”。

三、工作范围

各投标人须按国家有关标准及规范完成招标文件规定的所有工作内容：

1、履行所有规定服务；

2、服务成果须达到招标文件规定的质量标准及使用要求。

第三章　采购需求

第一部分 采购内容一览表

序号	标项名称	数量	单位	预算金额（元）	技术服务要求	备注
1	网络安全升级服务	1	项	1080000	网络安全升级服务，具体内容详见采购需求。	依据：【2021】58392 号、【2021】58393 号、【2021】58394 号、【2021】58395 号、【2021】58397 号；最高限价：1080000 元；类型：服务项目。

第二部分 采购需求

一、项目背景

为贯彻落实国家网络安全重大决策、重要部署和省政府“深化推进政府数字化转型”工作要求，按照《中华人民共和国网络安全法》《计算机信息系统安全保护条例》的相关要求，省动物疫病预防控制中心亟需推进网络安全建设。疫控中心内外网设备老旧，设备故障率高，性能也不能满足业务发展需求，机房基础建设存在密闭问题，基础设施欠缺环境监控相关设备，同时中心在用的有多个实验室信息管理系统，整体架构缺少必要的安全冗余机制。业务系统需要满足等级保护 2.0 标准要求，基于等保预测评整改建议对现网进行安全升级加固。

二、建设目标

为保障省动物疫病预防控制中心政务网络、核心设备及信息系统稳定运行，有效提升运维保障能力，促使省动物疫病预防控制中心的网络和信息化运维工作向提高应急响应能力、保障业务连续性、加强网络安全管理的方向迈进。

投标人需根据本项目的要求，提供网络系统维护保障及网络安全提升服务，提升网络系统、信息系统的安全防护能力，需通过等保评测。

三、服务内容

3.1 网络机房基础设施维护服务

服务方提供基础设施改造，机房区域窗户贴膜及石膏板封堵，原防火玻璃隔断破损，进行更换修复。机房线路整理将通信线缆铺设在隐蔽安全处。增加监控录制平台。

增加灭火消防配套设施，配置机房集中监控平台，在统一的平台上实现机房温湿度、烟雾，漏水，UPS，空调等监测，实现统一的报警管理。

3.2 网络系统维护服务

监控网络设备工作状态，监控重要运行信息，网络链路的连通状态，及时处理各类网络设备故障。建立完整的网络设备配置管理文档并及时更新发生变化的系统配置。及时处理各类网络设备故障和骨干网络链路故障。定期对网络设备监控记录和日志进行分析，发现系统存在的故障隐患和安全隐患，并提出解决建议。

服务方需对原有网络平台进行更新，更新全部数据接入交换平台，数据核心交换平台替换外网现有老旧平台，将该数据核心交换机部署到内网，和内网核心交换平台集群部署。

3.3 安全系统维护服务

检测安全设备工作状态和工作性能，及时升级系统软件，并记录备案，及时处理各类安全设备故障。实时监控各项数据和敏感信息，及时发现问题和安全隐患，并做出相应处理，保障网络通讯安全。

对安全设备的参数和配置进行动态的管理，维护配置文档和管理文档，并定期备案。

服务方需对原有安全平台进行更新，内外网部署下一代防火墙，具备 NAT 地址转换、出口链路负载均衡、安全边界隔离功能（避免安全事件影响到全局），同时开通 IPS、WAF、杀毒等功能模块，对数据流量做到 2-7 层的整体防护（实现快速的安全查杀防护等）。

外网配置上网行为管理平台，实现对出口访问审计、流控、认证等。满足公安部 82 号令和网络安全法的对内和对外审计合规要求。

内网配置入网规范管控系统，具有入网准入认证，避免非授权终端进入网络，避免非授权终端安全影响到网络内部。

3.4 数据备份服务

针对内网服务器等数据本地备份配置备份一体平台，避免逻辑错误（中病毒或误操作），造成数据丢失。保障数据安全，数据是核心资产，需要本地备份。对关键业务系统及生产数据采用备份方式进行数据保护，以保证当系统出现数据逻辑错误时，能够保证数据能够在短时间内进行恢复，符合等保要求。

3.5 统一安全审计服务

为内外网配置等保一体平台，需包含了日志审计系统、数据库审计系统、终端安全系统等功能，根据网络安全法的要求，日志可存留 180 天以上，对所有的数据库访问行为进行第三方的监控审计，对其中的敏感和异常访问事件（篡改数据、修改权限、敏感数据浏览等行为）进行告警，彻底扭转业务系统应用安全保障不利的局面。对 DBA、第三方运维及开发人员的 SQL 操作的审计，及时查询误操作、恶意操作及违规操作而导致数据破坏、篡改、泄露和业务中断。

3.6 其他

对现有网络中进行深度分析，评估平台的可用性水平。并通过应急保障预案、可用性评估报告的综合手段，提高系统的连续服务能力，降低业务中断的风险。进行平台级和应用级的可靠性和可维护性分析，建立安全管理计划和故障处理规范。

四、相关服务要求

下述内容为相关服务配置的最低要求，具体以供应商提供的服务方案为准；若有偏离则可能造成不利评审。

4.1 网络机房基础设施维护服务

4.1.1 基础设施改造

指标项	指标要求
功能要求	机房区域窗户贴膜及石膏板封堵。
	原防火玻璃隔断破损，在原有基础上进行更换修复。
	机房线路整理将通信线缆铺设在隐蔽安全处。
	设置机房监控、显示屏及录像平台。
	设置机房灭火消防配套设施。

4.1.2 机房安全集中监控系统

指标项	指标要求
系统架构	全 B/S 架构，中文管理界面，支持分布式部署，支持远程监控管理。
功能要求	在统一的平台上实现机房温湿度、漏水，UPS，精密空调等监测，实现统一的报警管理，形成综合监控告警平台。

	★监控平台内置 3D 建模功能：在平台内实现机房 3D 建模，系统应能提供机房建筑类如地板，墙，门，窗、柱子、环境监控传感器、UPS、配电柜、电源，空调、机柜、存储、交换机、服务器等部件，直接根据用户机房的实际布局通过拖拉组件的方式生成机房 3D 概览图，无需第三方软件建模导入，在平台内方便快捷快速建立真实的 3D 机房视图。（提供软件功能截图）
	★具有 3D 漫游巡检功能：系统可以按事先设定好的路线进行自动巡检。自动巡检时，虚拟人物会从设定好的起点出发，依次走到对应设备前面，打开设备监控页面。在自动巡检过程中，如发现设备有告警，系统将记录并发送告警信息给相关人员处理，巡检完成自动生成巡检报表。
	可视化大屏展示模块：采用先进的大数据展示技术，直观、美观的展示系统运行数据和状态，包括网络拓扑、设备运行状况统计、TOP 排名、具体监测设备数量、运行状态、告警信息、故障设备等，并且可根据用户关心的数据定制展示模块。
	辅助值班功能：用户可以按周或按日历两种方式进行设置。按周：用户选择周一到周五及周末的一天或多天值班，按日历即用户可配置一段时期内的值班时间，以日历的方式配置，方便直观，配置完成后，系统报警信息根据值班配置情况发送到值班员的手机或电子邮件中。
	自检功能：监测环境监控服务器运行状态：采集信息包括 CPU、内存、磁盘空间、进程、服务、流量、日志文件、文件系统等。
	自检功能：支持环境监控系统数据库监测；采集信息包括连接情况、命中率情况、内存情况、进程情况、会话数情况、连接数情况、死锁情况、表空间（数据库）情况等。
厂商资质	原厂商必须具有国家认证的软件企业证书
	软件必须具有省级及以上检验机构的检测报告（提供相关证明材料）。
远程管理软件	使用 B/S 模式，基于 TCP/IP 协议下的网络远程管理界面，便于操作人员以浏览 WEB 监控界面的形式，便捷完成远程管理机房的环境巡视和对各执行器的控制
短信告警模块	接口：具备短信发送功能，通过以太网共享，任何在网内的计算机都可以共享收发短信。支持 TCP、UDP 协议，支持 Socket 编程。 支持各种操作系统，可灵活设置各类指标报警阀值，可分多个报警等级。支持多种的告警方式，如手机短信、电子邮件等
智能数据集中采集器	组网方式：基于 IP 的局域网、广域网等，通过温、湿度传感器检测环境温度湿度值；通过温湿度传感器检测环境温度、湿度值；8 路 DI、DO 接口,4 路 RS485/RS232/RS422 三合一 12V 供电，连接浸水传感器，检测地面积水信息；RJ45 标准网络接口，符合 TCP/IP 及兼容协议；模块化电源设计，并考虑对过压与雷击的防护；硬件和软件上均采取先进的抗干扰措施，从而保障监控系统长期稳定的运行
温湿度传感器	供电电压：18-24VDC 输出信号：T：4-20mA liner 测量范围：T：0-60℃ H：0～100％RH 测量精度：T：±0.5℃（25℃，10%-90%RH）H：±3%RH（25℃，10%-90%RH）
线式漏水监测传感器	工作电压：DC 12V 供电电源：12-24VDC；输出形式：告警时蜂鸣器响；短路时阻抗<50Ω，负载电压＜60V，负载电流＜30mA；静态电流：<45mA；告警电流：<65mA；工作环境：-10~55°C，10~98%RH；含漏水监测软件模块。数量 2 个

烟雾传感器	光电探测方式、抗高频干扰、工作电压：DC12V、静态电流：≤8Ma 报警电流：≤35mA\工作温度：－10℃～55℃、环境湿度：≤95%RH、报警输出：继电器常开／常闭\探测灵敏度：Ⅱ、Ⅲ级。数量 2 个。
UPS 监测软件模块	对 UPS 内部整流器、逆变器、电池、旁路、负载等各部件的运行状态进行实时监视，一旦有部件发生故障，系统会自动报警。并且实时监视 UPS 的各种电压、电流、频率、功率等参数，直观图形界面显示。
空调检测模块	对于精密空调的监视，通过相关协议可实时采集监测的数据有：各模块压缩机、风机、加湿器、去湿器、加热器工作情况及设定温湿度、回风温湿度、控制状态（本机、远程、微机）和温湿度报警等。

4.2 网络系统维护服务

4.2.1 网络系统维护报告

指标项	指标要求
网络系统维护报告	报告至少包含：监控网络设备工作状态，监控重要运行信息，网络链路的连通状态，及时处理各类网络设备故障。建立完整的网络设备配置管理文档并及时更新发生变化的系统配置。及时处理各类网络设备故障和骨干网络链路故障。定期对网络设备监控记录和日志进行分析，发现系统存在的故障隐患和安全隐患，并提出解决建议。

4.2.2 数据接入交换平台

指标项	指标要求
性能	交换容量≥300Gbps；包转发率≥100Mpps
配置	48*10/100/1000TX 以太网端口+4 个 SFP+端口，交流电源，2 个千兆单模光模块。数量不少于 30 台。

4.2.3 数据核心交换平台

指标项	指标要求
交换容量	≥20Tbps
包转发率	≥4000Mpps
主控板槽位数	≥2 个
业务板槽位数	≥6 个
路由特性	支持静态路由、RIP、OSPF、IS-IS、BGP4、支持等价路由、支持策略路由、支持路由策略、支持 IPv6 静态路由、RIPng、OSPFv3、IS-ISv6、BGP4+、支持 VRRPv3 支持 Pingv6、Telnetv6、FTPv6、TFTPv6、DNSv6、ICMPv6、支持 IPv6 等价路由、支持 IPv6 策略路由、支持 IPv6 路由策略
配置	配置双主控，双电源，千兆电口≥48 个，万兆光口≥48 个

4.3 安全系统维护服务

4.3.1 安全系统维护报告

指标项	指标要求
安全系统维	针对本项目提供：安全系统维护报告，报告至少包含：检测安全设备工作状态和工

护报告	作性能，及时升级系统软件，并记录备案，及时处理各类安全设备故障。实时监控各项数据和敏感信息，及时发现问题和安全隐患，并做出相应处理，保障网络通讯安全。对安全设备的参数和配置进行动态的管理，维护配置文档和管理文档，并定期备案。

4.3.2 内网出口防火墙系统

指标项	指标要求
系统架构	原厂商要求参与第二代防火墙标准 GA/T1177-2014《信息安全技术 第二代防火墙安全技术要求》标准编制，要求提供相关证明复印件
	系统采用多核 AMP+架构架构，硬件设计采用高性能一体化智能安全处理引擎，要求提供计算机软件著作权登记证书，证书上要求有“高性能一体化智能安全处理引擎”字样
配置要求	性能要求：不低于 2U 机架设备，网络层吞吐量≥8G，应用层吞吐≥4G，并发连接≥280 万，每秒新建连接数≥13 万，
	配置≥6 个千兆电口，2 个千兆 SFP 光口，1 个 Console 口。
	扩展槽≥1 个；
	配置：5 年全功能模块升级订阅服务包（含应用识别库、URL 分类特征库、病毒防护特征库、入侵防御特征库升级服务及威胁情报订阅服务）
访问控制	支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN 等多种方式进行访问控制，并支持地理区域对象的导入以及重复策略的检查。
应用识别与控制	支持应用识别，应用特征库包含的应用数量（非应用协议的规则总数）大于 2800 种，支持配置基于 IP、用户、应用的流量管理规则，可深度识别每种应用的属性，
	为每种应用提供预定义的风险系数，并将应用基于类型、使用场景、数据传输、风险等级等特征分类。
病毒防护	能够对 HTTP/FTP/POP3/SMTP/IMAP/SMB 六种协议进行病毒查杀。
	支持对最多 6 级的压缩文件进行解压查杀。
	支持基于 MD5 的自定义病毒签名；支持设置例外特征，对特定的病毒特征不进行查杀。
入侵防御	支持漏洞防护功能，同时将漏洞防护特征库分类，至少包括缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL 注入、WEB 攻击等六种分类；漏洞防护支持日志、阻断、放行、重置等执行动作,可批量设置针对某一分类或全部攻击签名的执行动作；支持基于 FTP、HTTP、IMAP、OTHER_APP、POP3、SMB、SMTP 等应用协议的漏洞防护。
	★支持漏洞防护特征库包含高危漏洞攻击特征，至少包括“永恒之蓝”、“震网三代”、“暗云 3”、“Struts”、“Struts2”、“Xshell 后门代码”以及对应的攻击的名称、CVEID、CNNVDID、严重性、影响的平台、类型、描述等详细信息；（需要提供设备包含上述所有高危漏洞攻击的特征及对应详细信息的截图）。
	支持间谍软件防护功能，同时将间谍软件特征库分类，至少包括木马后门、病毒蠕虫、僵尸网络等三种分类;支持在防火墙间谍软件签名库直接查阅攻击的名称、严重性、描述等信息；间谍软件防护支持日志、阻断、放行、重置等执行动作,可批量设

	置针对某一分类或全部攻击签名的执行动作；支持基于 FTP、HTTP、IMAP、OTHER_APP、POP3、SMB、SMTP 等应用协议的间谍软件防护。
VPN 功能	支持支持 IPSec VPN 功能，支持基于主模式（Main Mode）、积极模式（Aggressive Mode）、国密三种协商模式建立的网关-网关加密隧道；支持本地 CA 并可为参与 IPSec VPN 隧道建立的设备颁发用于身份认证的证书。
	支持支持 GRE 隧道，支持 GRE over IPSec VPN。
	支持 L2TP、支持 L2TP over IPSec、支持 PPTP ，并支持本地认证以及 LDAP/Radius/证书/Active Directory/TACACS+/POP3 等第三方用户认证系统。支持客户端地址分配。
	支持 SSL VPN，支持使用 SSL VPN 客户端与防火墙建立 SSL VPN 加密隧道，支持对远程用户进行口令认证或证书认证，或证书认证+口令认证双因素；口令认证支持本地认证以及 LDAP/Radius/证书/Active Directory/TACACS+/POP3 等第三方用户认证系统；支持 USB-key 证书；支持本地 CA 并可为 SSL VPN 客户端颁发用于身份认证的证书。
网络异常感知	支持基于主机或威胁情报视图，统计网络中确认被入侵、攻破的主机数量，至少可查看被入侵、攻破的时间、威胁类别、情报来源、威胁简介、被入侵、攻破的主机 IP、用户名、资产等信息；并对威胁情报发现的恶意主机执行自动阻断（提供截图）。
	支持基于主机或威胁情报视图，统计网络中存在安全风险的主机数量以及对应的风险等级，至少可查看遭遇风险的时间、威胁类别、情报来源、威胁简介、失陷主机 IP、用户名、资产等信息（提供截图）。
	支持与威胁感知设备协同，实现主机状态检测及告警；（需提供包含云端配置的威胁感知设备的截图）。
	支持统计网络内威胁事件的数量及对应的风险等级；支持一键跳转查看详情并自动显示关联日志；可基于网络连接、应用名称、威胁事件处置威胁事件；（需提供能够体现以上功能的截图）。
	支持用户自定义重点 URL 分类和应用，并可基于定义的重点关注对象进行用户维度关联，并结合分析中心进行基于关联的用户/地址、URL 分类、应用进行二次递进式深度分析，挖掘异常用户及异常网络行为。
厂商资质	CCRC 信息安全服务资质-信息系统安全集成服务一级（一级为最高级）。
	CCRC 信息安全服务资质-安全运维服务资质一级（一级为最高级）。
	国测信息安全服务资质-安全开发类一级（一级为最高级）。
	提供产品《计算机信息系统安全专用产品销售许可证》，提供复印件；

4.3.3 内网数据中心防火墙系统

指标项	指标要求
性能要求	千兆电口≥6；万兆光口≥2；网络层吞吐量≥20G;应用层吞吐量≥8G;并发连接数≥220 万;新建连接数（CPS）≥15 万; IPSecVPN 最大接入数≥1000;IPSecVPN 加密速度≥400Mb;冗余电源; 开通 IPS、WAF、防病毒功能模块和对应的 5 年特征库升级服务。
产品架构要求	产品采用自主知识产权的专用操作系统，应用多核并行处理技术保障产品处理性能，需提供公安部计算机信息系统安全产品质量监督检验中心、中国信息安全测评中心、中华人民共和国国家版权局、公安部信息安全产品检测中心之中任意一家检测机构

	出具关于“多核并行安全操作系统”的证书或检测报告。
VPN 功能	产品支持 IPsec VPN 和 SSL VPN 功能。
	为满足组网兼容性，IPSec VPN 需支持 IKEv1 和 IKEv2 协议，支持基于主模式和野蛮模式建立加密隧道。
	产品支持 IPSec VPN 智能选路功能，根据线路质量实现自动链路切换。
	产品支持多种 SSL VPN 用户认证方式，至少包括本地密码认证、LADP 认证和硬件特征码认证。
地址转换	支持 IPv4 / IPv6 下 NAT 地址转换，包括支持源地址转换 SNAT，目的地址转换 DNAT 和双向地址转换双向 NAT，支持一对一、一对多、多对一等多种转换方式。
	支持 NAT64、NAT46 地址转换。
	支持 NATALG 功能，包括支持 FTP、、RTSP、SQLNET、PPTP、TFTP、H.323、SIP 应用协议的 NAT 穿越。
应用控制策略	支持基于区域、IP 地址、域名、端口、用户、应用、服务、时间等多个维度设置应用控制策略。
地域访问控制	支持基于对象、区域和地域维度设置安全访问控制策略，允许或拒绝特定国家或者地区的对象访问内部网络，保障业务重大时期安全可靠性。
应用识别	产品支持对不少于 9880 种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P 下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制。
流量控制	★产品支持基于地区维度设置流控策略，实现多区域流量批量快速管控功能。所投产品必须提供具备中国国家认证认可监督管理委员会认可的第三方检测机构关于“国家/地区的流量管理”功能项的产品检测报告（CMA）。
会话控制	产品支持基于 IP 对象的会话控制策略，实现并发连接数的合理限制。
DDoS 防御	支持 SYNFlood、ICMPFlood、UDPFlood、DNSFlood、ARPFlood 等泛洪类攻击防护，支持 IP 地址扫描和端口扫描攻击防护。
	支持 TearDrop 攻击、IP 数据块分片传输、Land 攻击、Smurf 攻击、WinNuke 攻击、超大 ICMP 数据攻击等异常报文攻击防护，支持 IP 协议异常报文和 TCP 协议异常报文攻击防护。
	支持 ARP 欺骗类攻击防护。
SSL 解密	支持对 HTTPS 协议加密会话进行解密分析，支持基于区域、对象、业务类型、服务器 IP/端口设置解密策略。
防病毒	支持对 HTTP、HTTPS、FTP、SMB、SMTP、POP3、IMAP 协议进行病毒检测和查杀，支持最大 10 层的压缩文件查杀。
	支持病毒排除设置，支持基于文件 MD5 值和文件下载 URL 设置病毒白名单；
	★支持防火墙内置蜜罐功能，定位内网感染僵尸网络病毒的真实主机 IP 地址；（需提供相关功能截图证明）
	★具备勒索软件通信防护功能，提供具备中国合格评定国家认可委员会认可的第三方检测机构关于“勒索软件通信防护”产品功能检测报告（CNAS）。
入侵防御	产品内置 IPS 检测引擎，支持口令暴力破解、僵尸网络、恶意软件、服务器与终端漏洞攻击等检测和防护，支持超过 5000 种特征规则。

	产品预定义漏洞特征数量超过 7650 种，支持在产品漏洞特征库中以漏洞名称、漏洞 ID、漏洞 CVE 标识、危险等级和漏洞描述等条件快速查询特定漏洞特征信息，支持用户自定义 IPS 规则。
	产品支持僵尸主机检测功能，产品预定义特征库超过 110 万种，可识别主机的异常外联行为。
Web 安全防护	产品支持对常见 Web 应用攻击防御，攻击类型至少支持跨站脚本（XSS）攻击、SQL 注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等类型，产品预定义 Web 应用漏洞特征库超过 3320 种。
	产品支持未知威胁检测能力，需提供公安部计算机信息系统安全产品质量监督检验中心、中国信息安全测评中心、中华人民共和国国家版权局、公安部信息安全产品检测中心之中任意一家检测机构出具关于“未知威胁检测”的证书或检测报告。
	产品支持对请求报文头的 X-Forward-For 字段检测，并对非法源 IP 进行日志记录和联动封锁。
	产品支持 CC 攻击防护功能，为保障勒 CC 攻击的检测效果，所投产品需提供具备中国国家认证认可监督管理委员会认可的第三方检测机构关于“CC 攻击防护”功能项的产品检测报告（CMA）。
蜜罐联动	产品支持与本地蜜罐联动，实现对 APT 攻击的防御功能。
	产品支持主动诱捕功能，通过伪装业务诱捕内外网的攻击行为，并联合云蜜罐获取黑客指纹信息，并自动封锁高危 IP。（需提供产品功能截图证明）
网端云联动	具备网端云协同联动功能
网端统一管控	本产品自带终端安全软件，通过防火墙产品界面实现中的终端安全软件的安全策略统一管控，实现安全事件进程级别取证以及一键安全事件处置。
资产识别	支持 Web 服务器自动侦测功能，根据 Web 服务器在线状态、端口使用状态、Web 服务器之间的互访关系生成业务资产列表，同时展示内网资产访问的风险等级。（需提供产品功能截图证明）
云端联动	支持将防火墙安全数据上报云端分析，提供云端独立平台用于安全人员进行安全分析和管理，云端平台需要包含但不限于资产安全、策略下发、安全事件自动处置等功能。
攻击事件风险分析	支持针对业务攻击事件汇总，展示攻击事件类型 TOP5 及当前业务命中的全网实时热点事件，支持通过地图区域颜色深浅展示攻击者的分布与数量。
安全运维	支持实时检测当前网络的整体安全状况，显示当前安全风险问题，并提供建议方案便于快速开展日常安全运维。
微信通告	支持通过微信方式，实现周期性发送安全报告，包括日报、周报、月报，报告包含但不限于业务态势得分，脆弱性概况、攻击防御、主机风险等
应急处置	支持发生紧急安全事件时，可通过微信的方式，实时通告给安全管理人员，安全人员可以在微信上一键下发策略至本地防火墙设备进行处置。
用户管理权限	支持三权分立功能，根据用户权限分为安全管理员、审计员、系统管理员三种角色；
双因素认证	支持管理员双因素认证，包含用户名/密码和 Key 等不同方式。
原厂商资质	要求所投产品的生产厂商为中国反网络病毒联盟 ANVA 成员单位，提供有效证书的

	复印件。
	要求所投产品的生产厂商具备中国网络安全审查技术与认证中心的信息安全软件开发服务资质，提供有效证书复印件。
	提供产品《计算机信息系统安全专用产品销售许可证》，提供复印件；

4.3.4 外网出口防火墙系统

指标项	指标要求
性能要求	千兆电口≥6；万兆光口≥2；网络层吞吐量≥20G;应用层吞吐量≥8G;并发连接数≥220万;新建连接数（CPS）≥15 万; IPSecVPN 最大接入数≥1000;IPSecVPN 加密速度≥400Mb; 冗余电源; 开通 IPS、WAF、防病毒功能模块和对应模块的 5 年特征库升级服务。
产品架构要求	产品采用自主知识产权的专用操作系统，应用多核并行处理技术保障产品处理性能，需提供公安部计算机信息系统安全产品质量监督检验中心、中国信息安全测评中心、中华人民共和国国家版权局、公安部信息安全产品检测中心之中任意一家检测机构出具关于“多核并行安全操作系统”的证书或检测报告。
部署方式	支持路由、透明、虚拟网线、旁路镜像、混合等多种部署方式，适应复杂使用环境的接入要求。
链路聚合	具备链路聚合功能，将 2 个或者更多物理链路组合成一个更高带宽的逻辑链路接口，提高链路带宽和链路可靠性。
路由功能	具备静态路由和多播路由，支持 RIP、OSPF、BGP 等动态路由协议。
	支持基于 IP 地址、端口、地域、协议、应用等维度配置策略路由策略，支持多种负载均衡算法，包括加权、带宽比例、轮询、线路排序等。
	产品支持策略路由负载，支持基于服务、ISP 地址、应用、地域等维度进行智能选路，保证关键业务流量通过优质链路转发，支持加权流量、带宽比例、线路优先等负载均衡调度算法。
网络服务	具备 ARP 代理功能，对指定地址的 ARP 请求使用指定接口的 MAC 地址应答，实现保护内网主机。
	具备标准 DHCP 服务功能，可为终端统一分配 IP 地址。
	具备 DNS 透明代理功能，避免单运营商 DNS 解析出现单一链路流量过载，平衡多条运营商线路的带宽利用率
VPN 功能	产品支持 IPsec VPN 和 SSL VPN 功能。
	为满足组网兼容性，IPSec VPN 需支持 IKEv1 和 IKEv2 协议，支持基于主模式和野蛮模式建立加密隧道。
	产品支持 IPSec VPN 智能选路功能，根据线路质量实现自动链路切换。
	产品支持多种 SSL VPN 用户认证方式，至少包括本地密码认证、LADP 认证和硬件特征码认证。
地址转换	支持 IPv4 / IPv6 下 NAT 地址转换，包括支持源地址转换 SNAT，目的地址转换 DNAT 和双向地址转换双向 NAT，支持一对一、一对多、多对一等多种转换方式。
	支持 NAT64、NAT46 地址转换。
	支持 NATALG 功能，包括支持 FTP、、RTSP、SQLNET、PPTP、TFTP、H.323、SIP 应用协

	议的 NAT 穿越。
IPv6	支持 IPv4/IPv6 双栈工作模式。
	支持 IPv6 环境的应用控制策略设置，能针对 IPv6 的 IP 地址、服务端口、区域、服务/应用、时间等条件进行应用访问规则的设置。
	支持 IPv6 环境的安全策略设置，实现入侵防御、防病毒、Web 应用防护等等安全功能。
应用控制策略	支持基于区域、IP 地址、域名、端口、用户、应用、服务、时间等多个维度设置应用控制策略。
地域访问控制	支持基于对象、区域和地域维度设置安全访问控制策略，允许或拒绝特定国家或者地区的对象访问内部网络，保障业务重大时期安全可靠性。
应用识别	产品支持对不少于 9880 种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P 下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制。
流量控制	产品支持基于地区维度设置流控策略，实现多区域流量批量快速管控功能。所投产品必须提供具备 CMA（中国国家认证认可监督管理委员会）认证的第三方权威机构关于“国家/地区的流量管理”功能项的产品检测报告。
会话控制	产品支持基于 IP 对象的会话控制策略，实现并发连接数的合理限制。
DDoS 防御	支持 SYNFlood、ICMPFlood、UDPFlood、DNSFlood、ARPFlood 等泛洪类攻击防护，支持 IP 地址扫描和端口扫描攻击防护。
	支持 TearDrop 攻击、IP 数据块分片传输、Land 攻击、Smurf 攻击、WinNuke 攻击、超大 ICMP 数据攻击等异常报文攻击防护，支持 IP 协议异常报文和 TCP 协议异常报文攻击防护。
	支持 ARP 欺骗类攻击防护。
SSL 解密	支持对 HTTPS 协议加密会话进行解密分析，支持基于区域、对象、业务类型、服务器 IP/端口设置解密策略。
防病毒	支持对 HTTP、HTTPS、FTP、SMB、SMTP、POP3、IMAP 协议进行病毒检测和查杀，支持最大 10 层的压缩文件查杀。
	支持病毒排除设置，支持基于文件 MD5 值和文件下载 URL 设置病毒白名单；
	支持防火墙内置蜜罐功能，定位内网感染僵尸网络病毒的真实主机 IP 地址；（需提供相关功能截图证明）
	具备勒索软件通信防护功能，提供具备 CNAS（中国合格评定国家认可委员会）资质的第三方权威机构关于“勒索软件通信防护”产品功能检测报告。
入侵防御	产品内置 IPS 检测引擎，支持口令暴力破解、僵尸网络、恶意软件、服务器与终端漏洞攻击等检测和防护，支持超过 5000 种特征规则。
	产品预定义漏洞特征数量超过 7650 种，支持在产品漏洞特征库中以漏洞名称、漏洞 ID、漏洞 CVE 标识、危险等级和漏洞描述等条件快速查询特定漏洞特征信息，支持用户自定义 IPS 规则。
	产品支持僵尸主机检测功能，产品预定义特征库超过 110 万种，可识别主机的异常外联行为。
Web 安全	产品支持对常见 Web 应用攻击防御，攻击类型至少支持跨站脚本（XSS）攻击、SQL 注

防护	入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等类型，产品预定义 Web 应用漏洞特征库超过 3320 种。
	★产品支持未知威胁检测能力，需提供公安部计算机信息系统安全产品质量监督检验中心、中国信息安全测评中心、中华人民共和国国家版权局、公安部信息安全产品检测中心之中任意一家检测机构出具关于“未知威胁检测”的证书或检测报告。
	产品支持对请求报文头的 X-Forward-For 字段检测，并对非法源 IP 进行日志记录和联动封锁。
	产品支持 CC 攻击防护功能，为保障勒 CC 攻击的检测效果，所投产品必须提供具备中国国家认证认可监督管理委员会认可的第三方检测机构关于“CC 攻击防护”功能项的产品检测报告（CMA）。
账号安全	产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生。
	产品支持文件目录防护功能，通过对用户账号进行认证，对网站内容的修改行为进行合法性控制。
蜜罐联动	产品支持与本地蜜罐联动，实现对 APT 攻击的防御功能。
	★产品支持主动诱捕功能，通过伪装业务诱捕内外网的攻击行为，并联合云蜜罐获取黑客指纹信息，并自动封锁高危 IP。（需提供产品功能截图证明）
网端云联动	具备网端云协同联动功能
网端统一管控	本产品自带终端安全软件，通过防火墙产品界面实现中的终端安全软件的安全策略统一管控，实现安全事件进程级别取证以及一键安全事件处置。
策略快速部署	支持在单条安全策略中可同时启用入侵防御、防病毒、URL 过滤、文件过滤、Web 应用防护等安全功能。
策略有效性检测	支持应用控制策略有效性检测，保障策略持续优化。
策略生命周期管理	支持应用控制策略生命周期管理，包含安全策略的变更时间、变更类型和策略变更用户，并对变更内容记录日志，方便策略的管理和运维。
策略优化	支持对当前应用控制策略异常分析，包括策略风险访问、策略冗余、策略冲突、策略重合、端口放通过大等问题，并提供相关解决方案便于用户快速调优。
原厂商资质	要求所投产品的生产厂商为中国反网络病毒联盟 ANVA 成员单位，提供有效证书的复印件。
	要求所投产品的生产厂商具备中国网络安全审查技术与认证中心的信息安全软件开发服务资质，提供有效证书复印件。
	提供产品《计算机信息系统安全专用产品销售许可证》，提供复印件；

4.3.5 上网行为管控平台

指标项	指标要求
性能配置	产品为标准 1U 机架式设备，需满足多核 X86 架构。标配千兆电口≥4 个；并含 2 个高速 USB2.0 接口，1 个 RJ45 串口，性能配置：最大并发连接数≥6w；用户规模≥300 人；每秒新建连接数≥1200；吞吐量≥2.4Gb；硬盘≥128GminiSATA；支持 BYPSS，包

	含 3 年 URL&应用识别规则库升级，3 年产品质保及软件升级。
链路负载	为了提高出口多链路利用率，要求支持按剩余带宽、带宽比例、平均分配、前面优先的方式进行多链路负载。支持使用 VPN 做专线备份，支持链路故障检测；
接入认证	支持多种接入认证； 1）多种认证方式，支持触发式 WEB 认证，支持用户名密码认证、IP 和 mac 认证、短信认证、微信认证、二维码认证、单点登录认证等多种认证方式； 2）用户身份源：支持对接多种用户源，包含内置账户、AD 域用户、LDAP 服务器用户验证、RADIUS 服务器、数据库服务器、POP3 服务器、第三方认证系统（cas）； 3）支持基于 802.1x 的外部 CA 证书认证，同时支持在线证书状态查询（OCSP）;
业务需要	为减少短信费用投入，要求设备支持微信身份验证，用户可以通过微信“扫一扫”、关注公众号等操作获取上网权限，后台能够记录下用户微信的 ID，支持与第三方微信平台对接，无需修改第三方平台代码；
	终端资产业务可视管理 1）支持图形化查看当前内网 IP 使用情况，帮助管理员减少人工维护 IP 表的工作量； 2）对网络接入的终端进行可视化管理，展示终端详细信息、异常状态等 3）支持查看终端类型，以及终端详细信息（厂商，系统，端口等）； 4）支持查看终端类型分布;
	支持非法外联行为检查阻断，包括拨号、双网卡、有 4G 网卡、有无线网卡、连接非法 wifi、使用非法网关、私连外网、自定义外联等行为，对不满足检查要求的终端强制断网，向管理员告警，并弹窗提示用户；
	为满足访客 PC 的简易接入授权，访客终端接入无线网络后，终端自动弹出二维码页面，审核人通过手机扫描访客终端二维码，添加备注信息，访客即可完成上网，同时设备记录访客备注信息、接入终端 MAC 以及审核人帐号。
	为满足公司内部实名认证，要求产品支持通过 OAuth 认证协议对接，支持阿里钉钉，企业微信第三方账号授权认证；
	为保证会议认证接入，支持提供二维码和会议号，用户扫码或输入会议号认证上网；支持通过验证手机号码实名认证;
	为确保我单位不会通过 SSL 加密内容发生通过互联网出口泄密事件，要求设备必须能够识别并过滤 SSL 加密的钓鱼网站、金融购物网站；识别和审计加密的邮箱（如 GMAIL）等；
	★针对内网用户的 web 访问质量进行检测，对整体网络提供清晰的整体网络质量评级，支持以列表形式展示访问质量差的用户名单，支持对单用户进行定向 web 访问质量检测（提供产品功能证明材料）
终端安全检查	★无需安装客户端，通过流量状况检查 10 款以上主流杀毒软件的运行情况，对不满足检查要求的终端可重定向页面修复;（提供截图证明文件）
应用识别规则库	支持根据标签选择应用，标签分类至少包含安全风险、高带宽消耗、发送电子邮件、降低工作效率、外发文件泄密风险、主流论坛和微博发帖 6 大类；此外可根据我单位需求自定义标签，根据标签做应用控制。
应用控制	设备内置应用识别规则库，支持超过 6700 条应用规则数，支持超过 2900 种以上的应用，1000 种以上移动应用，并保持每两个星期更新一次，保证应用识别的准确率；

流控黑名单	基于“流量”、“流速”、“时长”设置配额，当配额耗尽后，将用户加入到指定的流控黑名单惩罚通道中
P2P 智能流控	要求设备有效抑制如迅雷、ppstream 等 P2P 应用带宽，通过抑制可看到出口上下行带宽的明显改善。
IM 审计	支持对 QQ（客户端版本）、阿里旺旺、万德（Wind）、路透等应用的聊天，群聊天等内容的审计
杀软流量检查	无需安装客户端，通过流量状况检查 10 款以上主流杀毒软件的运行情况，对不满足检查要求的终端可重定向页面修复;（提供截图证明文件）
离线上网审计和管控	在非内网环境下通过客户端引流实现网页审计、邮件审计、应用审计、流量和时长审计，引流实现上网权限策略控制、上网时长控制、上网流量控制，支持 windows 终端，支持 windows 终端。
离线终端审计和管控	在非内网环境下实现客户端应用审计、U 盘审计、IM 审计，外发行为日志留存在终端本地，已配置的外设管控、外联管控、访问控制策略保持生效，终端接入内网后同步到设备日志中心。
SSL 加密内容审计和过滤	支持识别并过滤 SSL 加密的钓鱼网站、金融购物网站、非法网站等，同时支持 SSL 硬件加速卡解密，从而可提高 SSL 全流量解密性能；
单用户行为分析	针对单用户的行为分析（包括：应用流速趋势、应用流量排行、域名流量排行、应用时长排行、域名时长排行、行为汇总排行等）
数据中心	要求设备必须支持将审计数据备份到外置数据中心，实现海量存储；必须支持通过 USBKEY 方式对数据中心管理员进行身份验证，确保我单位核心数据不会外泄
产品联动	★能够与外网出口防火墙实现认证联动，同时部署产品后，可以实现认证同步机制，实现单点登录；（提供产品证明材料）
	★能够与等保一体平台实现联动，当检测到终端未安装“终端安全客户端”时，禁止上网并提示需要安装终端软件；（提供产品证明材料）
产品资质	提供产品《计算机信息系统安全专用产品销售许可证》，提供复印件；

4.3.6 入网规范管控系统

指标项	指标要求
系统要求	★标准机架式硬件产品，除自身硬件设备外，产品功能的实现无需额外增加服务器等设备；具有独立自主知识产权，符合公安部终端接入控制标准（GA/T 1105-2013）起草厂商（提供相关证明材料），产品核心功能必须是准入控制相关功能，如以类似模块形式体现，一律否决；所有功能的实现基于一套系统，不得多个管理页面(含通过跳转等多 ip 管理地址)，一个客户端（只有 2 个或 2 个以下进程）占用资源。
性能要求	标准配置 6 个 1000MBASE-T 接口；每秒事务数（TPS)：≥800（次/秒），最大吞吐量：≥500Mbps，最大并发连接数：1000（条）；支持 200 点终端规模。
IPv6 支持	支持在 IPv4 和 IPv6 双栈环境下的终端准入控制、重定向、认证、安检、修复等。
高可用性	准入设备必须具备 HA 模式，HA 须支持主备机心跳 IP 检测及虚地址管理模式。
	提供第三方监控平台，在出现重大异常情况时能及时通知网络设备放开网络。
终端部署	准入设备应至少提供安全客户端（Agent）、安全控件、无客户端等多种可供自定义

	部署和管理的模式。
	使用安全客户端模式部署时，客户端程序应支持功能定制，以降低系统资源耗用，提升客户端兼容性。
终端发现	能够实时监测并发现接入内网的 PC、移动终端、其他 IP 设备等终端。
	对自动发现的终端能够按照类别自动归类，以方便网络终端的统计管理。
准入技术	准入设备须支持 802.1x 协议准入方式，无需第三方 RADIUS 服务器支持。
	准入设备支持基于多厂商 Virtual Gateway 的 VLAN 隔离技术，实现无客户端下端口级准入控制。（功能截图）
	准入设备支持基于策略路由技术的准入控制模式，入网设备在访问网内关键资源时，将被强制隔离、引导至认证管理页面；
	支持交换机接口动态 VLAN 下发、端口隔离模式的网络边界管理。
	支持通过 MAC 旁路认证进行 ACL 下发的准入控制。
多路支持	单台准入设备可支持至少 4 路策略路由准入控制。
	单台准入设备可支持至少 4 个镜像口进行准入控制。
	单台准入控制设备支持至少 2 种准入技术组合使用，以增强环境的兼容性。
定向引导	支持终端入网 IE 浏览器重定向引导，当用户访问网页时能够自动转向到指定的页面或地址，并支持 http 代理及多重重定向引导。
	可根据用户的实际环境自定义非 80 端口的 Web 服务端口号及用户重定向引导。
	能通过浏览器完成身份认证、控件安装、设备注册、安全检查、检查结果展现等全流程引导管理。
	具有 Mac OS、Linux、iOS、Android 等系统专属客户端，支持认证引导和准入管理。
IP/MAC 绑定	具有入网设备自动学习功能，支持 IP/MAC/端口三者强制绑定，以及违规终端切换到断网 VLAN，防止终端仿冒 IP 接入网络或移动设备位置。
	支持在 DHCP 环境下的 IP、MAC 绑定功能
NAT 设备	具有 NAT 识别和检测机制能够及时发现网内私接的小路由器、无线 AP、随身 WIFI 等 NAT 设备，帮助清查通过网中网隐藏的真实网络终端。（功能截图）
	对通过 NAT 入网的计算机可以实现准入控制、安全评估和修复等流程化管理
Hub 管理	能够发现内网私接的 Hub、傻瓜交换机等非网管设备，当多台计算机通过 Hub 接入网络时，能够及时产生告警通知管理员。
	支持对连接 HUB 的交换机端口采用多种策略进行 VLAN 切换（功能截图）
网络设备管理	支持对：交换机、路由器、防火墙等，按照类别进行添加归类管理和展示。
	支持设备管理模板的定义功能，能够通过 SNMP、SSH、TELNET 等方式自动、批量添加网络设备。
终端网络拓扑	★能够在拓扑图上选取设备查看其基本状态信息、设备型号、所处位置、子节点、路由表、ARP 表等信息；支持在界面上提供对该网络设备进行 TELNET、SSH 等管理。；能够在网络拓扑图上由用户自定义显示的节点类型，方便用户通过不同方式

	查看拓扑连接。（提供以上功能截图）
交换机状态展现	支持可网管型交换机面板图形化展现各接口状态（up、down、trunk、单/多 MAC 等），以及各接口下联的终端详细信息（IP、地址、MAC 地址等）。
	能够支持自上而下逐级查找终端的具体位置、安全状态、认证用户、上下线时间等信息。
DHCP	提供 DHCP 服务。
	能够根据用户、IP/MAC 绑定信息等条件，为指定终端设备分配特定的 IP 地址。
DHCP 地址释放	支持 DHCP 通过管理服务器手动操作，主动进行某台主机的 IP 地址释放。实现 IP 地址充分利用。
终端识别	支持当前主流智能终端设备的安全准入控制，能够自动识别主流手机、智能终端等设备，并自动进行分类。
移动终端入网	提供独立的智能终端入网引导界面的自主定制功能，至少包括界面标题、界面 LOGO、界面说明文字等。
	能够提供移动终端入网的设备注册功能。
	支持指纹入网认证
联动认证	能够全面结合用户已有的认证或业务系统，可以与 RADIUS、LDAP、邮件、AD、WEB 系统做联动认证。
AD 域单点登录	能够与用户现有的 AD 域相结合，当用户登录到 AD 域后，无需二次认证即可入网，避免多次认证的繁琐流程。
	可对用户入网后进行是否 AD 域登录进行检查。
证书认证	在进行 Ukey 认证时，支持多个合法的根证书。终端用户认证时，自动进行根证书的匹配。
	支持采用软证书认证。
短信认证	支持短信认证模式，用户在登记入网手机号码后，能够在手机上接收到入网的短信验证码，并在浏览器页面上利用短信验证码认证入网。
微信认证	能够通过关注微信公众号放行移动终端入网（功能截图）
指纹认证	移动终端可以支持通过将指纹和用户账户绑定的方法，实现移动终端用户按压指纹认证入网。
接入审核	能够针对不同的角色或设备状态有选择的开启入网审核功能，待审核的用户或设备必须经过管理员审批才能入网。
	还可以进行审核流程调整。
认证控制	支持某类（角色）账户只能在指定的时间段、IP 段认证入网。
自助账号申请	支持用户在认证页面自行进行账号的申请。用户可自行提交用户名、密码、姓名、电话、部门、E-Mail 等信息。管理员审核通过后，用户即可使用该账号进行认证。有效解决用户账号和密码创建和分发的困难。
来宾角色	能够提供来宾角色选择，能够设定来宾设备的访问权限和入网时长

来宾码	员工可以为来宾申请来宾码，来宾使用来宾码可以接入网络；
	能够设定那些角色的用户能够申请来宾码。
二维码认证	★已入网员工可以通过扫描来宾终端上二维码，放行来宾用户入网（功能截图）
安全检查库	准入设备须提供系统安全配置、用户行为规范等类别检查项，至少提供 30 种以上安全检查项。
系统补丁	准入设备具有完整的补丁管理子系统，无需第三方补丁服务器支持，自身即可以提供完整的流程化补丁管理，包括同步更新、补丁分发表等功能。
	准入设备能够对补丁进行分级，分为：严重、重要、中等的类别。
	能够在终端的浏览器页面显示入网终端的补丁检查情况。
防病毒软件	支持主流的 20 种以上的杀毒软件检查，包括微软 MSE、可牛、Avast 等，支持杀毒软件版本、病毒库和运行情况的检查，能够在页面显示出检查结果。
终端安全加固	支持 Guest 来宾帐户、WSUS 更新配置、密码策略设置、屏幕保护设置、弱口令帐户、网卡绑定、系统共享资源进行检查加固
计算机健康性检测	支持对终端的磁盘使用率、垃圾文件、IE 主页、网络监听端口等安全性配置进行检查和修复
自定义安全检查	通过检测终端文件、指定文件版本、大小、MD5，注册表的项、注册表值，进程、服务状态进行检查。通过安装包运行、访问站点、开关服务、关闭进程、执行文件、删除文件、修改注册表进行修复。可以灵活的对终端进行安全检查和修复。
终端安全修复	能够提供多种修复方式，用户自行修复、自动修复。
移动终端管理	支持移动终端专用平台管理页面，方便使用平板、智能手机进行准入设备基本操作。
	可实现设备快速定位、设备审核、实时报警监控、小助手确认码生成、准入控制器管理、平台基本信息、关机与重启（功能截图）
管理角色控制	准入设备须采用系统管理员、安全管理员、审计员三权分立机制，防止单个角色管理者权限滥用。
网络诊断工具	支持通过 Web 管理界面进行 ping、抓包、traceroute、nslookup 等功能，并可以设置命令参数进行相关调试。
软件分发	准入设备应具有软件分发和部署功能，管理员可以预定义软件分发的路径、运行参数、是否执行等任务策略，以提升软件部署效率。
	能够自动判断并统计软件分发、部署的成功率，支持进程、注册表、文件等多种参数的组合判断。
虚拟监控台	为了方便管理员从整体上把握网络安全态势，系统提供虚拟监控台功能。通过集中的仪表、数值显示快速进行安全态势的把握，主要包括：报警、安全风险等级、全网终端数、清理终端数、安检合规率、安检项状态分布。
原厂商资质	公安部《计算机信息系统安全专用产品销售许可证》
	国家保密局《涉密信息系统产品检测证书（接入控制系统）》
	中国国家信息安全产品认证证书

4.4 数据备份服务

4.4.1 备份容灾系统

指标项	指标要求
设备基础要求	64 位多核处理器，内存≥16GB，热插拔盘位≥4 个，硬盘容量（配备≥3 块 2TB 企业级磁盘，7200 转，裸容量 6TB）；提供≥2 个千兆以太网接口。
	★设备系统基于存储专用的 64 位 UNIX 嵌入式系统(提供操作系统截图），存储系统及软件功能预装在独立的存储介质中，不占用 RAID 硬盘组的存储空间。
	★支持通用 RAID 0、1、5、6、50、60 等多种 RAID 方式，同时要求具备三重数据校验技术，即三块硬盘同时损坏数据不丢。(提供三重校验技术功能管理界面截图有厂商公章)
	备份容灾一体化设备，应支持备份、持续数据保护、存储、NAS、虚拟带库、虚拟主机等功能。(提供功能截图）
	支持的数据本地复制，以及到任一台备份设备的远程复制；支持接收 NAS 设备远程复制过来的数据。
	支持目标端在线重复数据删除功能，在数据存储时实时完成重复数据删除处理，不占用额外硬盘空间，不增加后期处理操作。不占用数据源端服务器处理资源，开启重删后，对设备本身的 CPU 资源占用要小于 10%，可随时开启或关闭重删功能。为保证数据源端的资源安全，不接受数据源端、服务器端的的重删方式。
备份功能支持	支持 Windows、Linux 及 Unix 操作系统下的文件或数据库在线备份。
	客户端必须支持纯国产环境，包括国产处理器构建的国产服务器、国产操作系统等；
	支持不同平台下 Oracle、Oracle RAC、Sybase ASE、Sybase IQ、SQL Server、DB2、Exchange Server、Lotus、MySQL 等国外数据库备份及恢复。
	★支持人大金仓、武汉达梦、南大通用、神州通用等国产数据库备份及恢复功能，并能够提供数据库厂商的兼容报告(提供管理界面截图并有厂商公章)
	支持 HP 安腾平台下的文件及数据库备份与恢复
	★支持打包备份功能、备份任务自动拆分处理功能，可针对细碎文件进行有效的备份处理，并支持对各种数据库进行脚本备份功能；（提供功能截图）
	支持 Oracle、Oracle RAC 的备份，在数据库服务器上无需安装任何客户端程序，即可实现数据备份。支持采用多通道备份方式，实现单一备份任务可并行多条备份通道进行数据备份，最大发挥高速网络（如万兆）和存储性能。备份工作支持完全、增量、差异等策略，最短备份间隔可缩短到每分钟进行一次数据备份。备份脚本可自动生成，必须支持按照实际需求手动编写备份脚本功能。
	支持对 VMware 的备份恢复，通过 vSphere API 进行 VMware 虚拟机的完全和增量备份恢复，无需在 Vcenter 服务器或中转服务器上安装任何代理，即可实现数据备份工作。必须支持多种级别的备份，包括：数据中心、ESXI/Cluster、vApp、虚拟机、虚拟磁盘等方式，能够支持数据并发备份，并发方式按照 ESXI 与虚拟主机的数量进行并发，支持备份完成后自动删除快照功能。不接受在虚拟机内部安装代理方式。
	能够灵活定制备份策略，如具有定时备份功能，能够自主地设定数据库、文件备份的策略，具有完全备份、增量备份、差分备份功能；提供时间和多种计划触发机制，实现任务计划的灵活性。
	支持远程备份，采用多主控模式，各主控能独立工作；支持断点续传、脱机备份、双向缓冲、流量控制等有效的广域网数据备份技术，减少网络通信流量，提高数据传输的稳

	定性和高效性；并可实现一对一、一对多、多对一、多对多的备份方式；（提供功能截图）
	能够提供操作系统的裸机恢复功能，能够对业务系统的操作系统进行手动备份和计划性在线增量备份，备份时不需要关机或重起，当操作系统意外损坏时，能够通过将 Window/linux 操作系统迅速恢复到之前备份的状态，而不需要重新安装操作系统。
	★支持 FC SAN 网络中异构平台下的多台服务器 LAN-Free 备份功能，支持以虚拟磁带库（VTL）或者物理磁带库作为 LAN-Free 的备份目标，不接受采用基于磁盘预先划分固定分区方式实现。支持同一存储空间（虚拟/物理磁带介质）被 Windows、Linux 和 Unix 主机共享使用。（提供基于磁带的 LAN-Free 功能截图，否则无效）（可根据用户要求提供测试）
虚拟带库功能	须拥有和备份功能为同一制造商的品牌，拥有自主知识产权，不接受 OEM 方式。（应提供软件产品登记证书）
	可虚拟出多种品牌的磁带库。包括：Oracle/SUN/STK、IBM、Quantum、Spectra Logic 等主流磁带库。
	可虚拟磁带库数量≥128、虚拟磁带机数量≥1024、虚拟磁带数量≥65536。支持 HP LTO-4 LTO-5 磁带机、支持 IBM LTO-4 LTO-5 磁带机。最大连接备份主机数:无限制;
虚拟化保护	★支持华为、华三等云平台实现无代理备份，支持深信服云平台、超融合平台实现容灾备份（提供兼容性证书复印件）
	支持 Vmware vSphere ESX/ESXi、Microsoft Hyper-V、KVM、CAS、FusionSphere 等主流虚拟化应用保护
	支持对 Vmware vSphere ESX/ESXi 虚拟化的保护，且在保护过程中，无需在任意虚拟机中安装任何客户端代理
	在对 VMWare 的保护过程中，支持 CBT、SDK、CDP 等多种备份方式。
	必须支持 SAN/vSAN 环境下的 Lan-Free 备份，减少备份过程中对于业务网的占用。
	支持备份任务并发，能够同时备份多个 ESXI 上的各自的虚拟机，或单台 ESXi 上的多个虚拟机，在单个任务下实现多个 ESXI 或多个虚拟机同时发起备份。
	支持永久增量备份，只需要进行一次初始化的全备份，其余备份全部采用增量备份方式；并且要求，在进行了多次备份作业后，VMWare 的性能不降低
	支持备份集的自动合并功能，要求在一份完整备份基础之上，将后续每次的增量数据与完整数据自动合并，合并成一份最新的完整数据，节省存储空间占用。在备份集合并之后，要求保留历史时间点的数据
	要求为保证 VMware 虚拟机的性能稳定，在 VMware 虚拟机快照记录中最多保留 2 个快照点
	能够从备份设备的备份文件快速启动虚拟机用于生产，而无需将备份文件先恢复到生产存储
	★支持 VMware 虚拟机的挂载功能，在原有虚拟机故障后，无需数据恢复过程，可将任意备份快照点挂载启动。支持单虚拟机粒度挂载，并支持虚拟机挂载后是否自动开机和联网，要求截图并具有厂商公章。
	支持瘦模式和厚模式磁盘分配的虚拟机
	根据不同的网络环境(SAN, LAN, WAN)可自定义数据去重的块大小

	提供无限数量的历史恢复点，可供 ESXi 进行恢复选择
	★支持以数据中心模式、VMware 集群模式、vAPP 模式、/虚拟机模式以及虚拟磁盘模式提供 VMware 数据备份，实现针对 VMware 环境更加准确的保护。(提供管理界面截图并具有厂商公章)
	支持多种备份介质，包括磁盘阵列、虚拟磁带库、NAS、物理磁带库等。
	管理控制台的可完全独立于备份服务器之外，用于在笔记本电脑和台式机上，而无需与备份服务器之间建立远程桌面协议 (RDP) 会话
	支持永久增量备份，只需要进行一次初始化的全备份，其余备份全部采用增量备份方式；并且要求，在进行了多次备份作业后，CAS 的性能不降低
	支持备份集的自动合并功能，要求在一份完整备份基础之上，将后续每次的增量数据与完整数据自动合并，合并成一份最新的完整数据，节省存储空间占用。在备份集合并之后，要求保留历史时间点的数据
	支持 CAS 虚拟机的挂载功能，在原有虚拟机故障后，无需数据恢复过程，可将任意备份快照点挂载启动。
	提供无限数量的历史恢复点，可供 ESXi 进行恢复选择
	支持备份任务并发，能够同时备份多个物理主机上的各自的虚拟机，在单个任务下实现多个物理主机同时发起备份。
数据保护 CDM 备份方式	支持 Oracle、Oracle-rac、SQLserver、MySQL、Sybase8T、PostgreSQL、恒辉等数据库的定时备份
	支持采用多通道备份方式，实现单一备份任务可并行多条备份通道进行数据备份，最大发挥高速网络（如万兆）和存储性能。
	针对 Oracle RAC 的备份，支持多节点、多通道并发备份方式，不接受单一节点备份方式，最大发挥高速网络（如万兆）和存储性能。
	支持 VMware、华为、H3C、KVM、Xen 等虚拟化平台的永久增量备份
	支持 VMware、华为、H3C、KVM、Xen 等虚拟化平台任意备份时刻的 5 分钟内快速挂载恢复，且挂载恢复的虚拟机文件应为完整的不含历史快照的文件集
	支持 VMware、华为、H3C、KVM、Xen 等虚拟化平台同一备份时刻可生成无限制数量的快照副本，且所有快照副本可同时挂载给不同或相同的生产系统满足使用需求。
	支持 VMware 多种级别的备份，包括：数据中心、ESXi/Cluster、vApp、文件夹、虚拟机、虚拟磁盘等方式，能够支持数据并发备份。(提供管理界面截图并加盖厂商公章)
	支持 Oracle、Oracle-rac、SQLserver、MySQL 等主流数据库同一备份时刻可生成无限制数量的快照副本，且所有快照副本可同时挂载给不同或相同的生产系统满足使用需求。
	支持文件及操作系统的永久增量备份
	★支持文件备份的过滤功能，提高备份效率，节省备份空间（提供功能截图）
	支持 Oracle 数据库 BCT （Block Change Tracking）数据保护模式，且支持用户自定义快照合并周期（提供产品功能截图）
	★可将设备中的 CDM 备份数据，归档至光盘库中进行离线保存，并能够将备份集中元数据信息同步至光盘库系统，实现脱离备份系统后，光盘库可直接对源主机进行数据恢复。(提供备份到光盘库功能截图)。

	支持 1 对多，多对 1，多对多的远程灾备功能，且所有节点的远程灾备计划任务在同一界面即可配置完成
权限管理	设备支持三权分立管理，可分为系统管理员、安全保密管理员和安全审计员，系统管理员负责创建和删除用户，进行系统维护；安全保密管理员负责设置所有用户的密码保存周期，重置用户密码，对普通用户进行授权，能够查看系统日志、用户日志和安全审计员日志；安全审计员用户名负责对系统管理员日志和安全保密管理员日志进行审计。
	具有国家信息安全产品认证（ISCCC），级别必须为增强级，提供证书复印件
授权许可	内嵌备份功能主模块； 配置 8 个 Windows、Linux 版本的文件代理模块、5 个操作系统代理模块和 5 个数据库代理模块； 配置远程备份代理模块，配置备份对象复制选件。 内嵌 Windows、Linux 环境下高级备份模块。
技术支持与服务	提供的软件应为最新版本，且不同时期软件版本应能兼容，同时要保证安全可靠及扩容和版本升级方便。
服务	提供产品《计算机信息系统安全专用产品销售许可证》，提供复印件；

4.5 统一安全审计服务

4.5.1 等保一体平台（内网）

指标项	指标要求
硬件参数	规格≥2U;CPU:不低于 Silver 4214R*2；内存≥128G;硬盘≥2*2TB SATA;网口≥千兆电口*6+万兆光口*2;电源≥冗余电源；
产品形态	产品支持软、硬件一体化与软硬件解耦两种部署方式
部署模式	支持网桥、路由、旁路模式部署
平台要求	平台包含数据库审计组件、运维审计组件、日志审计组件、主机杀毒安全功能组件
	平台可根据实际业务环境定义业务安全区域，简化运维管理；（提供界面截图证明）
	★在管理平台上可以通过拖拽虚拟设备图标和连线就能完成网络拓扑的构建，快速的实现整个业务逻辑的编排，并且可以连接、开启、关闭虚拟网络设备。（提供界面截图证明）
	平台首页可以展示详细主机状态、磁盘状态及应用状态，以及业务和用户遭受的安全风险、待处理的系统事件等相关安全信息；
	平台支持模板化的组件部署模式，至少支持出口边界安全模板、等保合规安全模板
	支持内置的安全市场，可根据业务需要灵活选择所需要的安全产品，且安全市场产品至少提供内置的 3 个月测试授权使用期限；
	支持故障迁移功能，当主机发生故障迁移后，可自动将组件迁移到其他主机上运行；
	★为了提供更好的排障手段，支持在平台内节点抓包分析分析功能，能够设置抓包的网口、过滤条件、文件大小等参数（提供界面截图证明）
	平台支持关键安全组件双机功能，保障安全组件高可用；在双机场景下，管理平台要支持双机配置同步，在硬件故障时保障无感知切换。
	支持基于一体化平台的安全运营中心功能，至少能够提供业务、用户视角的安全风险

	展示。
	业务、用户风险界面，支持针对业务、用户的风险事件进行分类，至少包含已经明确失陷的业务以及业务的威胁、脆弱性分析。同时能够针对已经实现、具备威胁与脆弱性不同阶段的安全事件进行等级描述、定位事件从何种安全组件上报，是否处理以及安全事件详情。（提供界面截图证明）
	至少支持业务维度与攻击维度的大屏展示功能。
	支持双因素认证功能，用户需在登录时进行双重认证，以此提高用户的安全性。
	支持禁用默认超级管理员账号，防止特权账号被滥用。
	支持针对安全组件账号的三权分立管理，实现平台管理员账号与安全组件账号权限的对应，防止平台管理员对安全组件进行越权操作。
主机杀毒功能要求	产品包含管理控制中心和终端 Agent 软件； 终端 Agent 软件支持 32 位和 64 位的 Windows 系统和 64 位的 Linux 系统。本次包含 Windows Server 客户端授权≥5 个；
	支持展示跟同品牌下一代防火墙、安全感知平台、上网行为管理，云端 SOC 平台，SAAS 化管理平台的联动状态
	支持管理员在同厂商的下一代防火墙管理界面下发快速查杀任务，并查看任务状态，结果并进行处置
	支持全网统一自动升级，不需要人为干涉，支持病毒库无缝主动式智能升级，增量升级，以减少升级时带来的网络流量；
	支持多种病毒报警方式，包括发送到管理控制台、声音报警、发送邮件、显示消息框、报告给上级系统中心等；
	支持跳转链接至云端安全威胁响应系统，针对已发生的病毒的基本信息，影响分析（客户情况、影响行业、区域分布）、威胁分析和处理建议等（需提供产品截图证明并加盖原厂公章）
	支持日志上报到云端 SOC 平台，包括 WEBSHELL 日志，暴力破解日志，杀毒日志，实现端网安全溯源分析。
数据库审计功能要求	纯 SQL 流量≥600Mb/s;业务流量吞吐≥4G;SOL 吞吐≥20000 条/s；日志条数≥20 亿条/天；存储天数≥180 天；日志检索≥40000 条/秒；
	采用 B/S 管理方式；
	支持多种数据库类型的审计，支持 Oracle 数据库审计、SQL-Server 数据库审计、DB2 数据库审计、MySQL 数据库审计、Informix 数据库审计、达梦数据库审计、人大金仓数据库审计、postgresql 数据库审计、sysbase 数据库审计、cache 数据库；
	支持白名单审计，系统使用审计白名单将非关注的内容进行过滤，不进行记录，降低了存储空间和无用信息的堆砌，白名单内容包括以下 4 个维度:SQL 模板、业务系统、URL 地址及数据库条件；（提供界面截图证明）
	支持自动基线学习数据库语义语法，并支持提取参数自动生成 SQL 模板，可以减少审计日志的重复写入和节省磁盘的存储空间；
	支持基于 SQL 命令的 webshell 检测，提供 webshell 日志查询； 可通过查看 webshell 攻击的时间、源 IP、业务系统、webshell 规则发现威；

日志审计功能要求	提供不少于 50 个审计许可。
	系统从不同设备或系统中所获得的各类日志、事件中抽取相关片段准确和完整地映射至安全事件的标准字段
	对安全事件重新定级。能根据统一的安全策略，按照安全设备识别名、事件类别、事件级别等所有可能的条件及各种条件的组合对事件严重级别进行重定义
	系统既可以完全收集采集对象上的日志信息，也支持在安全事件收集引擎上设置过滤条件，可过滤出无关安全事件，满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数，从而减少对网络带宽和数据库存储空间地占用。
运维堡垒机功能要求	提供不少于 50 个许可，内置配置管理员、密码管理员、审计管理员、系统管理员、系统审计员、普通运维用户等管理角色；针对 RDP、VNC、X11 等图形终端操作的连接情况进行记录及审计；记录发生时间、发生地址、服务端 IP、客户端 IP、操作指令、返回信息、操作备注、客户端端口、服务器端口、运维用户帐号、运维用户姓名、审批用户帐号、审批用户姓名、服务器用户名等信息；能够记录 RDP 协议中的活动窗口名称、删除文件等动作，并能记录 RDP 会话中的键盘输入信息；
原厂资质要求	★提供产品《计算机信息系统安全专用产品销售许可证》，提供复印件。

4.5.2 等保一体平台（外网）

指标项	指标要求
性能参数	规格≥2U;CPU:不低于 Silver 4214R*2；内存≥128G;硬盘≥2*2TB SATA;网口≥千兆电口*6+万兆光口*2;电源≥冗余电源；
产品形态	产品支持软、硬件一体化与软硬件解耦两种部署方式
部署模式	支持网桥、路由、旁路模式部署
平台要求	平台包含数据库审计组件、运维审计组件、日志审计组件、主机杀毒安全功能组件
	平台可根据实际业务环境定义业务安全区域，简化运维管理；（提供界面截图证明）
	★在管理平台上可以通过拖拽虚拟设备图标和连线就能完成网络拓扑的构建，快速的实现整个业务逻辑的编排，并且可以连接、开启、关闭虚拟网络设备。（提供界面截图证明）
	平台首页可以展示详细主机状态、磁盘状态及应用状态，以及业务和用户遭受的安全风险、待处理的系统事件等相关安全信息；
	平台支持模板化的组件部署模式，至少支持出口边界安全模板、等保合规安全模板
	支持内置的安全市场，可根据业务需要灵活选择所需要的安全产品，且安全市场产品至少提供内置的 3 个月测试授权使用期限；
	支持故障迁移功能，当主机发生故障迁移后，可自动将组件迁移到其他主机上运行；
	★为了提供更好的排障手段，支持在平台内节点抓包分析分析功能，能够设置抓包的网口、过滤条件、文件大小等参数（提供界面截图证明）
	平台支持关键安全组件双机功能，保障安全组件高可用；在双机场景下，管理平台要支持双机配置同步，在硬件故障时保障无感知切换。
	支持基于一体化平台的安全运营中心功能，至少能够提供业务、用户视角的安全风险

	展示。
	业务、用户风险界面，支持针对业务、用户的风险事件进行分类，至少包含已经明确失陷的业务以及业务的威胁、脆弱性分析。同时能够针对已经实现、具备威胁与脆弱性不同阶段的安全事件进行等级描述、定位事件从何种安全组件上报，是否处理以及安全事件详情。（提供界面截图证明）
	至少支持业务维度与攻击维度的大屏展示功能。
	支持双因素认证功能，用户需在登录时进行双重认证，以此提高用户的安全性。
	支持禁用默认超级管理员账号，防止特权账号被滥用。
	支持针对安全组件账号的三权分立管理，实现平台管理员账号与安全组件账号权限的对应，防止平台管理员对安全组件进行越权操作。
主机杀毒功能要求	产品包含管理控制中心和终端 Agent 软件； 终端 Agent 软件支持 32 位和 64 位的 Windows 系统和 64 位的 Linux 系统。本次包含 Windows Server 客户端授权≥5 个；
	支持展示跟同品牌下一代防火墙、安全感知平台、上网行为管理，云端 SOC 平台，SAAS 化管理平台的联动状态
	支持管理员在同厂商的下一代防火墙管理界面下发快速查杀任务，并查看任务状态，结果并进行处置
	支持全网统一自动升级，不需要人为干涉，支持病毒库无缝主动式智能升级，增量升级，以减少升级时带来的网络流量；
	支持多种病毒报警方式，包括发送到管理控制台、声音报警、发送邮件、显示消息框、报告给上级系统中心等；
	支持跳转链接至云端安全威胁响应系统，针对已发生的病毒的基本信息，影响分析（客户情况、影响行业、区域分布）、威胁分析和处理建议等（需提供产品截图证明并加盖原厂公章）
	支持日志上报到云端 SOC 平台，包括 WEBSHELL 日志，暴力破解日志，杀毒日志，实现端网安全溯源分析。
数据库审计功能要求	纯 SQL 流量≥600Mb/s;业务流量吞吐≥4G;SOL 吞吐≥20000 条/s；日志条数≥20 亿条/天；存储天数≥180 天；日志检索≥40000 条/秒；
	采用 B/S 管理方式；
	支持多种数据库类型的审计，支持 Oracle 数据库审计、SQL-Server 数据库审计、DB2 数据库审计、MySQL 数据库审计、Informix 数据库审计、达梦数据库审计、人大金仓数据库审计、postgresql 数据库审计、sysbase 数据库审计、cache 数据库；
	支持白名单审计，系统使用审计白名单将非关注的内容进行过滤，不进行记录，降低了存储空间和无用信息的堆砌，白名单内容包括以下 4 个维度:SQL 模板、业务系统、URL 地址及数据库条件；（提供界面截图证明）
	支持自动基线学习数据库语义语法，并支持提取参数自动生成 SQL 模板，可以减少审计日志的重复写入和节省磁盘的存储空间；
	支持基于 SQL 命令的 webshell 检测，提供 webshell 日志查询； 可通过查看 webshell 攻击的时间、源 IP、业务系统、webshell 规则发现威；

日志审计功能要求	提供不少于 50 个审计许可。
	系统从不同设备或系统中所获得的各类日志、事件中抽取相关片段准确和完整地映射至安全事件的标准字段
	对安全事件重新定级。能根据统一的安全策略，按照安全设备识别名、事件类别、事件级别等所有可能的条件及各种条件的组合对事件严重级别进行重定义
	系统既可以完全收集采集对象上的日志信息，也支持在安全事件收集引擎上设置过滤条件，可过滤出无关安全事件，满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数，从而减少对网络带宽和数据库存储空间地占用。
运维堡垒机功能要求	提供不少于 50 个许可，内置配置管理员、密码管理员、审计管理员、系统管理员、系统审计员、普通运维用户等管理角色；针对 RDP、VNC、X11 等图形终端操作的连接情况进行记录及审计；记录发生时间、发生地址、服务端 IP、客户端 IP、操作指令、返回信息、操作备注、客户端端口、服务器端口、运维用户帐号、运维用户姓名、审批用户帐号、审批用户姓名、服务器用户名等信息；能够记录 RDP 协议中的活动窗口名称、删除文件等动作，并能记录 RDP 会话中的键盘输入信息；
原厂商资质	★提供产品《计算机信息系统安全专用产品销售许可证》，提供复印件；
	厂商具备云安全成熟度成熟度模型 CS-CMMI 5 认证，提供证书复印件；

4.5.3 运维管控系统

指标项	指标要求
部署	云端 SaaS 化平台，免部署。无需硬件设备或者部署软件。
安全资产态势	支持以拓扑大屏形式展示整体网络安全态势，以失陷、风险或者正常等多个维度对资产安全情况进行统一展示；支持以轮播或者弹窗等方式推送待处理事件的告警；支持整体攻击态势和内部漏洞的统计展示；支持同步全网最新威胁情报信息；
分支详情展示	支持展示所有在线网点的网络吞吐带宽展示、当前用户流量信息、分支设备版本信息；
分支资源概况	支持即时查看受控设备状态，包括 CPU、内存、磁盘占用等。
分支版本监控	平台智能监控分支端设备 URL、应用识别库，若不是最新版本智能提醒升级。
日志查看	内置日志中心，详细记录管理员操作日志，管理员也可自行设定过滤规则来查看所需日志信息。
受控端设备日志查看	管理员通过远程接入可以查看任何一台受控设备的实时及历史日志信息 。
丰富的报表分析	支持展示分支资源利用率排行 TOPN、分支带宽利用率 TOP 排行、分支告警问题总数趋势、分支告警排行 TOP5、分支告警数量分布、分支离线市场 TOP5 等报表。
全网安全可视	收集网关、端点设备的安全日志，对全网的安全日志进行统一分析以及展示。
云网端联动	支持与网关、端点安全设备的命令下发、以及结果反馈（包括但不限于一键封堵 IP，一键断网，一键杀毒 ）。
实时微信告	支持通过微信推送安全事件（包括但不限于黑链，WEBSHELL，僵尸网络 ）

警	
高级威胁对抗	云端大数据分析，识别恶意攻击源，给出黑客画像，识别高风险攻击。

4.6 其他

4.6.1 安全评估

指标项	指标要求
安全评估	针对本项目提供： 漏洞扫描：对客户环境进行漏洞扫描及复检，发现系统环境潜在风险隐患，提供专业安全测评报告并提出整改建议及措施； 基线核查：避免人为疏忽或错误，或使用默认的安全配置，给业务系统安全造成风险，对重要服务器、应用系统、网络设备、安全设备等基于信息安全风险的角度进行安全配置检查，使业务系统的风险维持在可控范围内。

4.6.2 线缆辅材

指标项	指标要求
线缆辅材	项目服务过程中所需的跳线、电缆等

五、其他要求

5.1 进度要求

合同签订之日起 30 天内完成升级。

5.2 第三方评测

在系统验收前，由采购人委托第三方等保评测机构，需通过等保 2.0 评测。本项要求为系统验收的一个重要依据。

5.3 技术培训

供应商应根据项目实施的进度要求，及时安排有关培训，针对用户提供相关技术培训。

供应商负责编制有关培训方案、培训教材及其相关费用，提供具有技术能力和表达能力的培训讲师和辅导老师，提供培训所需的操作环境，以及培训讲师和辅导老师的差旅和食宿费用。

5.4服务要求

供应商需提供 7*24 小时的技术支持服务，采购人系统一旦出现故障，立即响应，先由工程师判断，无法解决情况下须有资深团队第一时间到达现场并作出处置，须在规定时间内作出故障原因判断并积极采取解决措施。4 小时解决问题，无法解决问题的，需在 8 小时内提供备品备件。

供应商的服务团队配置高级信息系统项目管理师、注册信息安全专业人员、CISAW 信息安全保障人员、备份容灾系统设备原厂认证工程师、HCIE/H3CTE/CCIE 等同级别能力的路由交换或安全方向认证工程师、VCP-Cloud 认证工程师认证等。

▲服务中所涉及到的软硬件设施设备保修期为三年，设备软件升级服务为五年。

第三部分 商务要求

一、报价要求

▲报价应包括完成本项目工作所需的人力物力成本、管理费、其他费用、利润、税金等所有费用。

▲本次报价为人民币价。

▲填报单价及总价。

二、签订合同

▲本项目合同甲方为浙江省动物疫病预防控制中心，乙方为中标人，合同款支付给乙方。

三、履约保证金交纳

▲按《第四章 采购合同》规定。

四、付款条件

▲按《第四章 采购合同》规定。

五、其他内容

详见招标文件的**《第四章 采购合同》**，投标人应对合同内容进行审核，如有偏离，请在投标文件的“偏离表”中反映。

六、分包和转包

▲本项目内容不得转包：供应商不得将本合同标的转包由其他单位承担；

▲本项目内容不得分包：供应商不得擅自将部分合同标的分包给其他单位承担；

▲享受《政府采购促进中小企业发展管理办法》的通知（财库〔2020〕46 号）的规定扶持政策获得政府采购合同的，小微企业不得将合同分包给大中型企业，中型企业不得将合同分包给大型企业；

▲如有违反以上情形，采购人有权解除合同，并追究中标人的违约责任。

第四部分 落实政府采购政策要求

一、政府采购扶持政策

（一）根据财政部 工业和信息化部关于印发《政府采购促进中小企业发展管理办法》的通知（财库〔2020〕46 号）的规定，本项目属于预留份额专门面向中小企业采购项目；

采购标的对应的中小企业划分标准所属行业：**【软件和信息技术服务业】**；

中小企业划分标准：《中小企业划分标准》（工信部联企业[2011]300 号）。

（二）根据财政部 司法部关于政府采购支持监狱企业发展有关问题的通知（财库〔2014〕68 号）的规定，监狱企业视同小型、微型企业。

（三）根据财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知（财库〔2017〕141 号）的规定，残疾人福利性单位视同小型、微型企业。

二、节能产品的强制采购政策

【本项目不涉及强制节能产品】

三、节能产品、环境标志产品的优先采购政策

根据财政部、国家发展改革委、生态环境部、国家市场监管总局《关于调整优化节能产品、环境标志产品政府采购执行机制的通知》财库〔2019〕9 号文件规定，对政府采购节能产品、环境标志产品实施品目清单管理，依据品目清单和认证证书实施政府优先采购。采购人拟采购的产品属于品目清单范围内的优先采购品目的，供应商提供的产品应具有国家确定的认证机构出具的、处于有效期之内的节能产品、环境标志产品认证证书，并在投标文件中提供该产品的节能产品认证证书或环境标志产品认证证书、产品所属节能环保品目清单中对应产品名称。

本项目执行：

【节能产品品目清单财政部、国家发展和改革委员会关于印发节能产品政府采购品目清单的通知（财库〔2019〕19 号），http://www.ccgp.gov.cn/zcfg/mof/201902/t20190213_11628855.htm】

【环境标志产品品目清单财政部、生态环境部关于印发环境标志产品政府采购品目清单的通知（财库〔2019〕18 号），http://www.ccgp.gov.cn/zcfg/mof/201903/t20190330_11833800.htm】

【产品认证机构详见市场监管总局关于发布参与实施政府采购节能产品、环境标志产品认证机构名录的公告（2019 年第 16 号），http://www.ccgp.gov.cn/zcfg/bwfile/201904/t20190403_11853998.htm】

第五部分 实质性要求

本章中所有带▲的内容是采购人提出的实质性要求，投标文件响应内容若不满足实质性要求，该投标文件将被评标委员会认定为无效。

第四章　采购合同

采 购 合 同

（甲乙双方应按招标文件确定的事项及投标文件响应内容签订本合同，不得对招标文件确定的事项和中标人投标文件作实质性修改）

合同编号：【　　】

项目名称：网络安全升级服务项目
合同内容：网络安全升级服务

甲方：浙江省动物疫病预防控制中心
乙方：**【　　】**

签署日期：二〇二一年【】月【】日

浙江省动物疫病预防控制中心（甲方）网络安全升级服务项目（项目名称）中所需网络安全升级服务（标项内容）经浙江省动物疫病预防控制中心（采购人）以招标文件（项目编号：CTZB-2021090194）进行公开招标。甲方确定【　　】（乙方）为中标人。甲、乙双方依据《中华人民共和国政府采购法》、《中华人民共和国民法典》，在平等自愿的基础上，同意按照下面的条款和条件，签署本合同。

一、项目采购依据

政府采购预算执行确认书：【　　】

二、下列文件构成本合同的组成部分

以下文件为本合同的组成部分，应该认为是一个整体，彼此相互解释，相互补充。组成合同的多个文件的优先支配地位的次序如下：

a. 本合同书

b. 中标通知书

c. 询标承诺

d. 投标文件

e. 招标文件

三、合同标的物

本合同标的物名称及数量：（服务内容可附后）

四、合同总价

本合同总价为【　　】元人民币。

分项价格：【　　】

五、合同价款的支付

1、本合同中甲乙双方之间所发生的一切费用以人民币进行结算。

2、支付方式：

付款次数	约定支付条件	付款条件	金额（元）	对应预算执行确认书
第一次付款	合同生效之日	满足合同约定支付条件，甲方向乙方支付合同总价35%的合同款。		
第二次付款	项目验收合格后	服务期满后，并通过验收，甲方向乙方支付剩余合同款。		

每次合同款项支付，乙方需提供同等金额的正规票据（发票或收据，应符合甲方财务管理要求））给甲方，甲方收到正规票据后15天内向财政部门申请支付。

以上付款时间是指甲方完成向财政部门申报支付手续的时间，财政部门审查及实际支付可能造成的时间延误不视为甲方违约。

发票类型：增值税发票。

3、甲方应付合同款至以下乙方指定的银行账户：

开户名称：【　　】

开户银行：【　　】

账　　号：【　　】

六、履约保证金

1、乙方应在合同签订后5个工作日内向甲方提交履约保证金为【/】元。【不需提交】

2、履约保证金用于补偿甲方因乙方不能履行其合同义务而蒙受的损失。

3、履约保证金应使用本合同货币，按下述方式中【/】形式提交：

A. 在中华人民共和国注册和营业的银行出具的保函，或保险公司出具的保函。

B. 支票。

C.汇票。

D.其他非现金形式。

4、如果乙方未能按合同规定履行其义务，甲方有权从履约保证金中取得补偿。

5、履约保证金有效期限：合同签订之日起至项目通过甲方验收后结束。

6、履约保证金退还：有效期限满后，按合同约定扣除相关款项（如有）后无息退还。

七、本合同履行期限、地点

1、服务期内，乙方应在充分了解甲方现有环境基础上，提供规范化、高质量的服务，具体服务内容与要求详见合同附件。

2、除合同约定内容外，乙方不得向第三方外包其服务。

3、履行期限：【　　】

4、履行地点：【　　】

八、服务人员

乙方应派遣一名具有专业知识的资深管理人员负责与甲方对接，负责本项目的项目管理，统筹相关工作，监督项目执行与情况汇报，控制工作质量，执行变更和应急情况管理，并根据实际状况调整乙方人员安排，以保证项目的正常高效运作。

乙方应派出投标文件中指定资历和经验的专业服务人员提供服务，负责对其人员进行监督、指导和管理，甲方有权要求撤换不合格的服务人员。若乙方原因，未经甲方书面同意，乙方不得擅自更换指定的服务人员，否则甲方有权解除合同，另行安排服务商，由此造成的损失由乙方承担。

甲乙双方指定代表，作为履行本合同服务事宜的主要联系人。

甲方代表：【　　】电话：【　　】

乙方代表：【　　】电话：【　　】

九、服务考核

甲方对乙方服务质量进行客观评估，具体考核办法（如有）作为合同附件。

项目完成后，乙方应及时向甲方发出书面履约完成通知，甲方在收到乙方履约完成通知后，应及时做好组织验收的准备工作，制定验收方案，成立验收小组，组织实施验收和履约评价。

验收小组完成验收后应出具验收书，验收书应包括每一项技术、服务、安全等标准的履约情况。

十、合同变更

1、甲方和乙方都不得擅自变更本合同，但合同继续履行将损害国家和社会公共利益的除外。如必须对合同条款进行改动时，当事人双方须共同签署书面文件，作为合同的补充，并报同级政府采购监督管理部门备案。

2、有下列情形之一的，双方协商一致可以变更合同：

（1）发生不可预见的紧急情况，继续按照原合同履行不能实现采购目的，又不能从其他供应商处采购；

（2）因甲方的过错导致不能实现采购目的，重新采购费用和违约金、违约损失赔偿金额占合同金额比例过大，但违背社会公共利益的除外；

（3）属于合同主要条款确定的事项，但变更不改变合同实质性内容；

（4）合同主要条款以外的内容；

（5）法律、法规规定可以变更合同的其他情形。

3、当事人协商一致变更合同的，应当报同级财政部门备案。

十一、转让和分包

1、政府采购合同不能转让。

2、经甲方事先书面同意乙方可以将合同项下非主体、非关键性工作分包给他人完成。接受分包的人应当具备相应的资格条件，并不得再次分包。分包后不能解除乙方履行本合同的责任和义务，接受分包的人与乙方共同对甲方连带承担合同的责任和义务。

十二、通知

本合同任何一方给另一方的通知，都应以书面形式发送，而另一方也应以书面形式确认并发送到对方明确的地址。

十三、计量单位

除技术规范中另有规定外，计量单位均使用国家法定计量单位。

十四、不可抗力

1、如果双方中任何一方遭遇法律规定的不可抗力，致使合同履行受阻时，履行合同的期限应予延长，延长的期限应相当于不可抗力所影响的时间。

2、受事故影响的一方应在不可抗力的事故发生后尽快书面形式通知另一方，并在事故发生后合同规定时间内，将有关部门出具的证明文件送达另一方。

3、不可抗力使合同的某些内容有变更必要的，双方应通过协商达成进一步履行合同的协议，因不可抗力致使合同不能履行的，合同终止。

十五、违约责任

除合同规定的不可抗力外，如果乙方没有按照合同规定的时间提供服务，甲方可要求乙方支付违约金。违约金按每周合同款的0.5%计收。但违约金的最高限额为合同价的5%。一周按7天计算，不足7天按一周计算。如果达到最高限额，甲方有权解除合同。

项目结束时验收不合格，乙方应在收到甲方通知后 10 日内退还甲方已支付的合同款，逾期退还合同款的，每日按未退还金额的 1 %支付违约金。

其他违约条款双方协商确定：【　　】

十六、违约解除合同

1、在乙方违约的情况下，甲方可向乙方发出书面通知，部分或全部终止合同。同时保留向乙方追诉的权利。

1.1 因不可抗力致使不能实现合同目的；

1.2 在履行期限届满之前，乙方明确表示或者以自己的行为表示不履行主要义务；

1.3 乙方迟延履行主要义务，经催告后在合理期限内仍未履行；

1.4 乙方迟延履行义务或者有其他违约行为致使不能实现合同目的；

1.5 乙方转包，或者未经甲方同意采取分包方式履行合同；

1.6 甲方认为乙方在本合同履行过程中有腐败和欺诈行为的。

1.6.1“腐败行为”和“欺诈行为”定义如下：

1.6.2“腐败行为”是指提供/给予/接受或索取任何有价值的东西来影响甲方在合同签订、履行过程中的行为。

1.6.3“欺诈行为”是指为了影响合同签订、履行过程，以谎报事实的方法， 损害甲方的利益的行为。

1.7 法律、法规规定的其他情形。

2、甲方解除合同的，合同于甲方发出书面解除合同通知书送达乙方之日起解除。乙方应在合同解除后 10 日内退还甲方已支付的合同款，逾期退还合同款的，每日按未退还金额的 1 %支付违约金。

3、甲方解除合同的，应当报同级财政部门备案。

十七、破产终止合同

如果乙方破产或无清偿能力时，甲方经报同级政府采购监督管理部门审批后，可在任何时候以书面通知乙方，提出终止合同而不给乙方补偿。该合同的终止将不损害或不影响甲方已经采取或将要采取任何行动或补救措施的权利。

十八、适用

本合同应按照《中华人民共和国政府采购法》、《中华人民共和国民法典》、《浙江省政府采购合同暂行办法》等进行解释。

十九、解决争议的方法

因合同履行中发生的争议，可通过合同当事人双方友好协商解决。如自协商开始之起 15 日内得不到解决，双方应将争议提交政府采购监管部门调解。调解不成的，可申请 / 仲裁委员会进行仲裁或向 甲方所在地区 人民法院提起诉讼。

仲裁裁决为最终裁决，当事人一方在规定时间内不履行仲裁机构裁决的，另一方可以申请人民法院强制执行。

仲裁费用和诉讼费用除仲裁机构或人民法院另有裁决外，应由败诉方负担。

二十、合同的生效及其他

政府采购项目的采购合同内容的确定应以招标文件和投标文件为基础，不得违背其实质性内容。

合同将在双方签字盖章后开始生效。授权代表签署的后附法定代表人授权书。

二十一、合同附件（如有）

1、政府采购预算执行确认书

二十二、合同份数

本合同一式五份，具同等法律效力。甲方、乙方双方各执二份，采购代理机构一份。

甲方（单位章）：	乙方（单位章）：
法定代表人（签字或盖章）：	法定代表人（签字或盖章）：
或授权代表（签字）：	或授权代表（签字）：
地　　址：	地　　址：
邮政编码：	邮政编码：
电　　话：	电　　话：
开户银行：	开户银行：
账　　号：	账　　号：
纳税人识别号：	纳税人识别号：
签订时间：　　年　月　日	签订时间：　　年　月　日

签约地点：

第五章　评标办法

本评标办法遵照《中华人民共和国政府采购法》等政府采购有关规定，并结合本项目的具体情况制定。

一、总则

评标工作遵循公正、公平、科学、择优的原则，评标人员将本着认真、公正、诚实、廉洁的精神，进行评标工作，择优推荐中标候选人。在评标期间，评标委员及相关工作人员必须严格遵守保密规定，不得泄露评标的有关情况。

评标委员会成员对需要共同认定的事项存在争议的，应当按照少数服从多数的原则作出结论。持不同意见的评标委员会成员应当在评标报告上签署不同意见及理由，否则视为同意评标报告。

二、评标组织

评标工作由采购人依法组建的评标委员会负责。评标委员会负责审标、询标、评审等工作，并向采购人提出评审意见和评标报告。

三、符合性审查

评标委员会对投标文件依据招标文件规定进行符合性审查。符合性审查条件详见《第六章　投标人须知》

四、投标文件的澄清、说明或者补正

投标人根据评标委员会要求对投标文件进行澄清、说明或者补正。评标期间，投标人应随时随地答复评标委员会的询标。程序要求详见《第六章　投标人须知》

五、评标细则

1、本项目采用综合评分法（总分 100 分），评标委员会根据本评标办法进行评审，对符合性审查合格的投标文件进行商务和技术评估，综合比较与评价。每个投标人最终得分=商务技术分+价格分。

2、评审时，评标委员会各成员应当独立对每个有效响应的文件进行评价、打分，然后汇总每个投标人每项评分因素的得分。

3、对投标人的价格分等客观评分项的评分应当一致，对其他需要借助专业知识评判的主观评分项，应当严格按照评分细则公正评分。

4、评标结果按评审后得分由高到低顺序排列。得分相同的，按投标报价由低到高顺序排列。得分且投标报价相同的并列。并编写评标报告。

5、评分因素及分值范围

5.1 商务技术分

该评分分值由评标委员会根据评审情况在分值范围内独立评分（具体分值设定详见表格），小数点后最多保留一位小数。每个投标人的最终得分为评标委员会打分汇总后的算术平均值（小数点后保留二位小数，第三位四舍五入）。

序号	评分因素	评分细则 （电子投标文件中提供的证明材料（证书、合同等）应清晰可辨，如无法辨识，将不予给分。）	分值（分）
一	履约能力		
1.	投标人的管理体系认证	投标人的管理体系认证（5 分） ◇投标人通过信息技术服务管理体系认证（认证依据：GB/T24405/ISO/IEC 20000）得 2 分，否则得 0 分 ◇投标人通过信息安全管理体系认证（认证依据：GB/T 22080/ISO/IEC 27001）得 2 分，否则得 0 分	5

		◇投标人通过业务连续性管理体系认证（认证依据：GB/T 30146/ISO 22301）得 1 分，否则得 0 分； 说明：根据投标文件中提供的有效证书进行评分，未提供或不符合以上条件不得分。	
2.	投标人综合实力	投标人综合实力（4 分） （1）投标人具有 ITSS 信息技术服务运行维护三级含以上认证的，得 2 分，否则得 0 分； （2）投标人具有信息系统建设及服务能力三级含以上认证的得 2 分，否则得 0 分； 说明：根据投标文件中提供的有效证书进行评分，未提供或不符合以上条件不得分。	4
3.	投标人的类似项目业绩	投标人的类似项目业绩（5 分） ◇2018 年 1 月至今（以合同签订时间为准）提供网络安全服务的业绩，每提供一份得 1 分，满分 5 分。 说明：根据投标文件中提供的业绩合同进行评分，未提供或不符合以上条件不得分。	5
二	服务水平		
4.	需求分析	需求分析（5 分） ◇对现有网络安全系统整体情况以及维护需求情况的理解（如机房环境、网络拓扑、安全情况分析等）。	5
5.	采购需求响应满足性	采购需求响应满足性（20 分） ◇对招标文件“第三章 采购需求”中“四、相关服务要求”的响应情况，根据投标人投标文件的响应情况进行评分，标有“★”指标全部满足要求的得 10 分，每有一项不能满足项扣 2 分，**▲如有 6 项及以上标有“★”指标项未响应或不满足，投标文件作无效处理。** ◇对招标文件“第三章 采购需求”中“四、相关服务要求”的响应情况，根据投标人投标文件的响应情况进行评分，指标（标有“★”指标除外）全部满足其他要求的得 10 分，每有一项不能满足项扣 1 分。**▲如有 11 项及以上指标项未响应或不满足，投标文件作无效处理。**	20
6.	衔接及整合方案	衔接及整合方案（5 分） ◇与现有设备的衔接及整合方案，在保证现有资源充分利用的情况下进行高效的整合，并实现有效的功能扩展，确保原先系统的平稳运行。	5
7.	网络机房基础设施维护服务	网络机房基础设施维护服务（5 分） ◇根据机房环境分析，制定针对本项目的网络机房基础设施维护服务方案，根据方案的可行性、合理性等综合评审打分。	5
8.	网络系统维护服务	网络系统维护服务（5 分） ◇根据项目需求制定网络系统维护服务方案，内容包括但不限于数据接入交换平台及数据核心交换平台方案。	5

9.	安全系统维护服务	安全系统维护服务（5 分） ◇根据项目需求制定安全系统维护服务，内容包括但不限于内网出口防火墙系统、内网数据中心防火墙系统、外网出口防火墙系统、上网行为管控平台、入网规范管控系统。	5
10.	数据备份服务	数据备份服务（4 分） ◇根据数据备份服务需求中备份容灾系统的功能、备份方式、管理权限等服务方案综合评分打分。	4
11.	统一安全审计服务	统一安全审计服务（4 分） ◇根据统一安全审计服务需求中外网及内网等保一体平台、运维管控系统功能、参数等服务方案综合评审。	4
12.	应急服务方案	应急服务方案（5 分） ◇系统的应急服务响应是否合理，是否充分考虑用户实际使用需求，解决方案是否完整、经济、安全、切实可行、措施得力。	5
13.	进度控制和质量保障	进度控制和质量保障（4 分） ◇对节点进度细化合理、有利于项目开展。结合采购需求，有针对性地建立了项目质量保障工作机制。	4
14.	技术培训	技术培训（2 分） ◇投标人能根据项目建设实际需要合理安排项目培训，提供合理的培训计划、培训内容、培训老师需拥有讲师认证，满足本项目培训需求。	2
15.	项目服务团队-项目经理	项目服务团队-项目经理（2 分） ◇项目经理具有信息系统项目管理师（高级）证书的，得 2 分，否则不得分；	2
16.	项目服务团队-其他人员	项目服务团队-其他人员（10 分） ◇具有注册信息安全专业人员认证的人员得 2 分，否则不得分； ◇具有 CISAW 信息安全保障人员认证（安全集成专业级 SI/PL）的人员得 2 分，否则不得分； ◇具有备份容灾系统设备的原厂认证的人员得 2 分，否则不得分； ◇具有 HCIE/H3CTE/CCIE 等同级别能力的路由交换或安全方向认证工程师的人员得 2 分，否则不得分； ◇具有虚拟化认证工程师认证的人员，得 2 分，否则不得分； 说明：上述人员必须均为投标人在职员工，根据投标文件中提供以上人员的社保缴纳证明、有关证书进行评分，未提供或不符合以上条件不得分。社保缴纳证明以社保机构出具的社保证明为准。一人多证，仅计分一次，不重复计分。	10
17.		总分	90

5.2 价格分

价格评分将在有效投标人范围内进行，最高得 10 分，最低得 0 分（小数点后保留二位小数，第三位四舍五入）。满足招标文件要求且投标报价最低的**投标报价**为**评标基准价**，投标人的价格分统一按照下列公式计算：

投标报价得分=(**评标基准价** / **投标报价**)×10%×100

落实政府采购政策说明：本项目面向中小企业采购，不进行价格扣除。

此项由评标委员会集体核实后统一打分。

六、重新评审

评审结果形成后，除下列情形外，任何人不得重新评审：

（一）分值汇总计算错误的；

（二）分项评分超出评分标准范围的；

（三）评标委员会成员对客观评审因素评分不一致的；

（四）经评标委员会认定评分畸高、畸低的。

第六章　投标人须知

投标人须知前附表

<table>
<tr><td>投标人须知条款号</td><td>名称</td><td>内容</td></tr>
<tr><td>1.3</td><td>采购人</td><td>名称：浙江省动物疫病预防控制中心
地址：杭州钱塘新区下沙街道十五堡南浙江牧业监测大楼
项目采购联系人：陈凯
项目联系方式：0571-56269718</td></tr>
<tr><td>1.3</td><td>采购代理机构</td><td>名称：浙江省成套招标代理有限公司
地址：杭州市文晖路 42 号现代置业大厦西楼 18 楼 1804 室
项目采购联系人：卢亚君
联系电话：0571-85830198、85830257、13777489611
邮编：310004
Email：85830198@zjsct.cn</td></tr>
<tr><td>1.9</td><td>踏勘现场</td><td>不组织，投标人如有需要，经采购人同意后可自行前往，踏勘期间发生的费用或意外导致伤亡等一切责任和损失均由投标人自负。</td></tr>
<tr><td>1.10</td><td>答疑会</td><td>不召开。</td></tr>
<tr><td>3.3.2</td><td>投标文件盖章要求</td><td>投标文件按“第七章 投标文件格式”中提供的格式要求盖章。公章采用单位 CA 章或单位公章。</td></tr>
<tr><td>3.3.3</td><td>投标文件装订要求</td><td>本项目投标时采用电子文件，不需提供纸质投标文件，无装订要求。</td></tr>
<tr><td>3.5.1</td><td>投标保证金</td><td>不需交纳投标保证金</td></tr>
<tr><td>3.6.1</td><td>投标文件有效期</td><td>自投标截止时间起 120 天内</td></tr>
<tr><td>4.1.1</td><td>投标文件密封及标记要求</td><td>投标人如提交备份电子投标文件，以介质存储的数据电文形式的备份电子投标文件应密封，封皮应注明投标人名称、项目名称、备份电子投标文件。</td></tr>
<tr><td>4.2.1</td><td>投标截止时间</td><td>按“招标公告”规定</td></tr>
<tr><td>4.2.2</td><td>投标地点</td><td>按“招标公告”规定</td></tr>
<tr><td>5.1.1</td><td>开标时间和地点</td><td>按“招标公告”规定</td></tr>
<tr><td>5.18</td><td>采购代理服务费</td><td>采购代理服务费金额：以标项中标金额为计算基数，按以下标准费率计算值收取。费率标准如下：
<table>
<tr><td>金额（万元）</td><td>费率</td></tr>
<tr><td>100 以下部分</td><td>1.5%</td></tr>
<tr><td>100~500 之间部分</td><td>0.8%</td></tr>
</table>
收费计算示例：（标项中标金额 200 万元）
[100*1.5%+（200-100）*0.8%]。
采购代理服务费交纳形式：汇票/支票/电汇</td></tr>
</table>

		采购代理服务费由中标人在接到中标通知书时以人民币方式向采购代理机构支付。汇入以下账户： 户名：浙江省成套招标代理有限公司 开户：中信银行杭州西湖支行 账号：7331610182600126385
10	其他	1、本招标文件共 79 页（含封面），请各投标人收到本文件后自行核对，如有缺页、错装等情况请于当日向采购代理机构提出，如未提出，所有责任及由此造成的后果由投标人自负。 2、请投标人仔细阅读本招标文件，其中带“▲”标记的条款为实质性内容，投标人须对带“▲”标记的条款作出实质性响应。
11	特别提醒	企业信用融资：省财政厅、浙江银监局、省金融办制定了《浙江省政府采购支持中小企业信用融资试点办法》（浙财采监[2012]13号），所称的政府采购信用融资，是指银行业金融机构（以下简称银行）以政府采购诚信考核和信用审查为基础，凭借政府采购合同，按优于一般中小企业的贷款利率直接向申请贷款的供应商发放贷款的一种融资方式。供应商可登陆浙江政府采购（http://zfcg.czt.zj.gov.cn/）中小企业信用融资栏目了解相关信息。
12	特别提醒	根据《关于在政府采购活动中查询及使用信用记录有关问题的通知》财库[2016]125 号的规定： （1）采购人或采购代理机构将对本项目投标人的信用信息进行查询。 （2）查询渠道为信用中国网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）。 （3）信用信息截止时点为从本项目投标截止日往前追溯三年，期间被列入失信被执行人名单、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单等投标人信用信息均将用于本项目。 （4）信用信息查询记录和证据以网页截图等方式留存。 （5）投标截止日当日网站显示的信用信息将作为评审和确定中标人的依据。
13	特别提醒	中标人应在合同签订前完成政府采购云平台（https://www.zcygov.cn/）全部注册步骤并成为正式注册入库供应商，否则将导致合同款无法正常支付，责任由中标人承担。请投标人尽早完成注册。 https://middle.zcygov.cn/settle-front/#/registry。（供应商注册页面）
14	特别提醒	中标人应提供与电子投标文件内容一致的纸质投标文件一正二副，装订成册，采用胶订或线订，不得采用活页夹等可随时拆换的方式装订。（胶订或线订以外装订形式视为活页装订） 中标人在领取中标通知书时提供纸质投标文件。

一、总则

1.1 实施依据

本次招标工作是按照《中华人民共和国政府采购法》等有关法律、法规、规章、文件的规定组织和实施。

1.2 采购方式

公开招标，是指采购人依法以招标公告的方式邀请不特定的供应商参加投标。

1.3 定义

电子交易活动：是指以数据电文形式，依托政府采购项目电子交易平台进行的政府采购交易活动。

采购人：是指依法进行政府采购的国家机关、事业单位、团体组织，见“投标人须知前附表”；

采购代理机构：受采购人委托，在委托的范围内办理政府采购事宜的机构，见“投标人须知前附表”；

投标人：是指参加本政府采购项目投标的供应商；

投标人代表：是指参加本项目投标活动的供应商法定代表人或法定代表人授权代表；

投标联合体：是指两个以上供应商组成联合体，以一个投标人的身份参加投标；

甲方：是指合同签订的一方，一般与采购人、用户相同；

乙方：是指合同签订的另一方，与中标人相同；

中小企业：是指在中华人民共和国境内依法设立，依据国务院批准的中小企业划分标准确定的中型企业、小型企业和微型企业，但与大企业的负责人为同一人，或者与大企业存在直接控股、管理关系的除外。符合中小企业划分标准的个体工商户，在政府采购活动中视同中小企业。

中小企业划分标准：《中小企业划分标准》（工信部联企业[2011]300 号）。

在政府采购活动中，供应商提供的货物、工程或者服务符合下列情形的，享受《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）规定的中小企业扶持政策：

（1）在货物采购项目中，货物由中小企业制造，即货物由中小企业生产且使用该中小企业商号或者注册商标；

（2）在工程采购项目中，工程由中小企业承建，即工程施工单位为中小企业；

（3）在服务采购项目中，服务由中小企业承接，即提供服务的人员为中小企业依照《中华人民共和国劳动合同法》订立劳动合同的从业人员。

在货物采购项目中，供应商提供的货物既有中小企业制造货物，也有大型企业制造货物的，不享受本办法规定的中小企业扶持政策。

以联合体形式参加政府采购活动，联合体各方均为中小企业的，联合体视同中小企业。其中，联合体各方均为小微企业的，联合体视同小微企业。

监狱企业：是指由司法部认定的为罪犯、戒毒人员提供生产项目和劳动对象，且全部产权属于司法部监狱管理局、戒毒管理局、直属煤矿管理局，各省、自治区、直辖市监狱管理局、戒毒管理局，各地（设区的市）监狱、强制隔离戒毒所、戒毒康复所，以及新疆生产建设兵团监狱管理局、戒毒管理局的企业；

残疾人福利性单位：符合《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕 141 号）的规定的单位；

同级政府采购监督管理部门：浙江省财政厅政府采购监管处；

1.4 联合体

☑ 本项目不接受联合体。

☐本项目接受联合体。

以联合体形式参加本项目采购的，联合体的主办单位和成员单位均应当具备招标文件规定的条件，

并在投标文件中分别提供联合体的主办单位及成员单位的资格条件证明材料，在投标文件中提交联合体协议。

以联合体形式参加采购活动的，应当在投标文件中提交由所有联合体成员各方盖章的联合体协议。联合体协议应载明联合体各方承担的工作和义务；联合体协议应当指定主办单位，授权其代表所有联合体各成员方，具体负责参与项目采购响应和合同实施阶段的主办、协调工作；联合体协议中应当载明由联合体各成员方共同与采购人签订合同，并就采购合同约定的事项对采购人承担连带责任。

投标文件的报价表中应列明联合体各成员方的各自承担的内容及对应报价。

投标文件盖章事宜，按联合体协议约定由主办单位盖章，也可由联合体所有成员单位盖章。

联合体成交的，本项目的采购代理服务费由联合体主办单位缴纳。

联合体协议中仅约定由联合体主办单位或成员单位中某一方与采购人签订合同的，或联合体协议中仅约定由联合体主办单位或成员单位中某一方就采购合同约定的事项对采购人承担责任的，视为联合体协议不成立，该联合体的投标文件将被作无效处理。

1.5 投标费用

无论招投标过程中的做法和结果如何，投标人自行承担招投标活动中所发生的全部费用。

1.6 保密

参与招标投标活动的各方应对招标文件和投标文件中的商业和技术等秘密保密，违者应对此造成的后果承担法律责任。

1.7 语言文字

除专用术语外，与招标投标有关的语言使用中文。专用术语应附有中文注释。

1.8 计量单位

所有计量均采用中华人民共和国法定计量单位。

1.9 踏勘现场

1.9.1 投标人须知前附表规定组织踏勘现场的，采购人按投标人须知前附表规定的时间、地点组织投标人踏勘项目现场。

1.9.2 投标人踏勘现场发生的费用自理。

1.9.3 除采购人的原因外，投标人自行负责在踏勘现场中所发生的人员伤亡和财产损失。

1.9.4 采购人在踏勘现场中介绍的场地和相关的周边环境情况，供投标人在编制投标文件时参考，采购人不对投标人据此作出的判断和决策负责。

1.10 答疑会

1.10.1 投标人须知前附表规定召开答疑会的，采购人按投标人须知前附表规定的时间和地点召开答疑会，澄清投标人提出的问题。

1.10.2 投标人应在答疑会时间的前一天，以书面形式将提出的问题送达采购人，以便采购人在会议期间澄清。

1.10.3 答疑会后，采购人按本章 2.4 款规定对投标人所提问题进行澄清答复。

1.11 分包

采购需求规定允许分包的，投标人应当在投标文件载明分包承担主体，分包承担主体应具备采购需求规定的分包承担主体的资格要求。

1.12 偏离

投标文件应完全响应招标文件规定的实质性内容和条件。

1.13 其他说明

1.13.1 **根据政府采购相关法律、法规、规章、文件规定并满足招标文件规定资格条件的区域性分支机构、个体工商户、个人独资企业、合伙企业参加本项目投标并由单位负责人签署的相关投标资料**

与本招标文件规定由法定代表人签署的的文件材料具有同等效力。

1.13.2▲**投标人对所投标项内的采购内容必须全部进行投标。**

1.13.3 招标文件中所涉及的产品品牌或型号均为建议性要求或为档次选择要求或为代替部分技术指标描述，投标人可以选择其他品牌型号的产品参加投标但投标产品须具有相当于或优于招标文件要求的指标、性能、档次。否则，评标委员会将对其作出不利的评审。

1.13.4 招标文件中如有描述歧义或前后不一致的地方，评标委员会有权按公平、合理的原则进行评判，但对同一条款的评判适用于每个投标人。

1.13.5 投标文件的响应内容必须真实、明确、准确。否则，评标委员会将对其作出不利的评审。

1.13.6 项目资金为财政性投资，资金已落实。

1.13.7 投标人须对所投产品、方案、技术、服务等拥有合法的占有、使用、收益、处分的权利，并对涉及项目的所有内容可能侵权行为指控负责，保证不伤害采购人的利益。在法律范围内，如果出现文字、图片、商标和技术等侵权行为而造成的纠纷和产生的一切费用，采购人概不负责，由此给采购人造成损失的，投标人应承担相应后果，并负责赔偿。投标人为执行本项目合同而提供的技术资料等归采购人所有。

1.13.8 **投标人母公司（总机构）或者同一母公司下属的其他子公司（同一总机构下属的其他分支机构）的人员、业绩、荣誉、知识产权、项目案例等不作为投标人的资信文件。**

二、招标文件

2.1 招标文件组成

2.1.1 第一章 招标公告

2.1.2 第二章 采购需求总体要求

2.1.3 第三章 采购需求

2.1.4 第四章 采购合同

2.1.5 第五章 评标办法

2.1.6 第六章 投标人须知

2.1.7 第七章 投标文件格式

2.1.8 补充文件

2.2 招标文件的解释权

招标文件的解释权归采购代理机构所有。

2.3 招标文件的质疑

2.3.1 投标人认为招标文件规定内容使自己的合法权益受到损害的，投标人可以提出书面质疑。

2.3.2 质疑书须包括以下内容：

（一）投标人的姓名或者名称、地址、邮编、联系人及联系电话；

（二）质疑项目的名称、编号；

（三）具体、明确的质疑事项和与质疑事项相关的请求；

（四）事实依据；

（五）必要的法律依据；

（六）提出质疑的日期。

2.3.3 质疑期限为自获取招标文件之日或者招标文件公告期限届满之日（在招标文件公告期限届满后获取招标文件的，以招标文件公告期限届满之日为准）起 7 个工作日内，投标人应在质疑期内一次性向采购代理机构提出针对招标文件的质疑，逾期提出不予受理。

2.3.4 质疑书中涉及的相关材料中有外文资料的，应当将与质疑相关的外文资料完整、客观、真实地翻译为中文，并注明翻译人员姓名、工作单位、联系方式等信息。

2.3.5 投标人为自然人的，应当由本人签字；投标人为法人或者其他组织的，应当由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。否则不予受理。

2.3.6 质疑书以直接提交、传真或邮寄方式提交（一式三份）。

2.3.7 质疑书以传真形式提交后，同时须向采购代理机构提交质疑书原件，实际收到原件之日作为收到质疑日。

2.3.8 如联合体投标，质疑应由组成联合体的所有供应商共同提出。

2.4 招标文件的澄清

2.4.1 投标人对招标文件如有疑问要求澄清，或认为有必要与采购代理机构进行技术交流，投标人需将书面资料传真或送达至采购代理机构，同时将电子文件发至投标人须知前附表注明的邮箱（电子邮件与书面文件有不一致的，以书面文件为准），并与采购代理机构进行确认。

2.4.2 投标人要求澄清的资料应加盖单位公章、写明日期。

2.4.3 如有必要，采购代理机构和采购人对投标人所有要求澄清的问题都予以解答，澄清答复的文件为补充文件，作为招标文件的组成部分，补充文件将以网上公告等形式告知所有获取招标文件的投标人，补充文件对投标人均有约束力。

2.4.4 澄清的内容影响投标文件编制的，采购代理机构将顺延投标截止时间，使之满足政府采购的相关规定。

2.4.5 投标人在收到补充文件后，应在 24 小时内以书面形式向采购代理机构确认已收到该补充文件。

2.4.6 当招标文件与补充文件就同一内容的表述不一致时，以最后发出的书面文件为准。

2.5 招标文件的修改

2.5.1 在投标截止时间前，由于各种原因采购人可能以补充文件的形式修改完善招标文件。

2.5.2 补充文件作为招标文件组成部分，补充文件将以网上公告等形式告知所有获取招标文件的投标人，补充文件对投标人均有约束力。

2.5.3 修改的内容影响投标文件编制的，采购代理机构将顺延投标截止时间，使之满足政府采购的相关规定。

2.5.4 投标人在收到补充文件后，应在 24 小时内以书面形式向采购代理机构确认已收到该补充文件。

2.5.5 投标人收到补充文件后，对补充文件如有疑问要求澄清，应在 24 小时内将书面资料传真或送达至采购代理机构，同时将电子文件发至投标人须知前附表注明的邮箱（电子邮件与书面文件有不一致的，以书面文件为准），并与采购代理机构进行确认。

2.5.6 投标人要求澄清的资料应加盖单位公章、写明日期。

2.5.7 对补充文件的澄清答复按 2.4 款规定。

2.5.8 当招标文件与补充文件就同一内容的表述不一致时，以最后发出的书面文件为准。

2.5.9 任何口头答复均不属于招标文件的组成部分。

三、投标文件

3.1 投标文件

3.1.1 投标人应仔细阅读招标文件规定的所有内容，以保证能全面准确理解招标文件，并按照招标文件要求，详细编制投标文件，投标文件内容必须针对本次招标响应。

3.1.2 投标人必须按招标文件的要求提供相关资料，并对招标文件中提出的所有内容要求给予实质性响应，须保证投标文件的准确、真实、明确。投标文件响应内容对招标文件要求如有偏离均应填写偏离表，如不填写，采购人有权视作投标文件完全响应招标文件要求。

3.2 投标文件组成

3.2.1 资格文件

应包括以下内容（**均需投标人加盖公章**）：证明其符合《中华人民共和国政府采购法》规定的供应商基本条件和采购项目对投标人的特定条件（如果项目要求）的有关资格证明文件。

序号	资格条件	应提供的资格审查资料（除承诺函、说明、声明外的其他证件提供复印件）
1.	**基本资格要求：**	**/**
1.1	（1）满足《中华人民共和国政府采购法》第二十二条规定，未被“信用中国”（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单；	（1）营业执照（或事业法人登记证或其他工商等登记证明材料）复印件（供应商为自然人的，提供自然人的身份证明） （2）符合资格条件的声明函【声明函 1】
2.	**落实政府采购政策需满足的资格要求：**	**/**
2.1	本项目为服务项目，本项目服务属于【**软件和信息技术服务业**】，要求服务全部由中小企业承接，即提供服务的人员为中小企业依照《中华人民共和国劳动合同法》订立劳动合同的从业人员。中小企业是指满足《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）第二条规定的企业，监狱企业、残疾人福利性单位视为小型、微型企业；	（3）中小企业声明函/监狱企业声明函及其相关的充分的证明材料/残疾人福利性单位声明函。【声明函 2】
3.	**特定资格要求：**	**/**
3.1	（1）单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的政府采购活动。	（4）与其他供应商无利害关系的声明函。【声明函 3】
3.2	（2）根据《关于规范政府采购供应商资格设定及资格审查的通知》（浙财采监[2013]24 号）第 6 条规定接受金融、保险、通讯等特定行业的全国性企业所设立的区域性分支机构（应依法办理了工商、税务和社保登记手续，获得总公司（总机构）授权或能够提供房产权证或其他有效财产证明材料，能证明其具备实际承担责任的能力和法定的缔结合同能力）、以及个体工商户、个人独资企业、合伙企业（应依法办理了工商、税务和社保登记手续，能够提供房产权证或其他有效财产证明材料，能证明其具备实际承担责任的能力和法定的缔结合同能力）；	◇属于此种情形的供应商除基本资格要求应提供资料外。还应提供以下资料： （5）金融、保险、通讯等特定行业的全国性企业所设立的区域性分支机构提供总公司（总机构）授权； （6）个体工商户、个人独资企业、合伙企业应提供房产权证或其他有效财产证明材料。 ◇不属于此种情况的供应商提供以下资料： （7）企业类型的声明函。【声明函 4】

3.3	（3）非联合体。	（8）提供非联合体的声明函。【声明函5】

3.2.3 商务技术文件

（1）法定代表人资格证明书；

（2）法定代表人授权签署投标文件委托书；（法定代表人签署不需提供此书）

（3）法定代表人授权开标委托书；（法定代表人参与不需提供此书）；

（4）偏离表；

（5）廉政承诺书；

（6）其他资信资料；

（7）同类业绩表；

（8）提供针对本项目的完整技术解决方案；

（9）投标人认为需要提供的其他资料。

3.2.3 报价文件

（1）投标函；

（2）开标一览表；

（3）投标价格组成明细表；

（4）交纳采购代理服务费承诺书；

3.3 投标文件的编制

3.3.1 内容编制

（1）投标文件应按照本章 3.2 款中规定的顺序及采用“第七章 投标文件格式”中提供的格式进行编制，并按“政府采购云平台”的要求编辑相应内容进行关联定位、加密，形成投标文件及备份电子投标文件。投标人未按规定加密的投标文件，政府采购云平台将拒收并提示。投标文件编制详见操作指南：登录政府采购云平台（https://www.zcygov.cn/），从首页-服务中心-帮助文档-项目采购-电子招投标，查看文档和视频。

（2）关联定位规则：一个关联点只能关联一页，不能关联多页；多个关联点可以关联同一页。

（3）分别编制资格文件、报价文件、商务技术文件。

（4）投标文件应当对招标文件规定的内容进行对应明确说明，对招标文件规定的实质性内容应当作出响应。

（5）采购人如对招标文件有澄清或修改，投标人应按澄清或修改内容对电子投标文件进行补充或者修改，补充和修改时如已传输提交了投标文件的，应当先行撤回原文件，补充、修改后重新传输提交。

（6）由于字迹模糊或表达不清引起的后果由投标人负责。

（7）编制投标文件时建议选用“谷歌或火狐浏览器”。

（8）投标文件可以线下完成盖章（签署）后传输提交政府采购云平台。

（9）生成的电子投标文件的文件后缀名为【.jmbs】，备份电子投标文件的文件后缀名为【.bfbs】。

3.3.2 格式要求

（1）投标文件应编制目录。

（2）投标文件应按“投标人须知前附表”要求盖章。

（3）投标文件装订要求详见“投标人须知前附表”。

（4）投标文件格式为 PDF。

（5）单个文件上传大小上限为 300M。

3.4 投标报价

3.4.1 ▲本次投标报价为含税人民币价。

3.4.2 投标报价包括履行所有规定服务并提交服务成果所产生的全部费用。服务及服务成果须达到招标文件规定的质量标准及使用要求。

3.4.3 报价应按不同费用构成分开填写，具体详见“投标文件格式”。

3.4.4 ▲所投标项只允许有一个报价，不接受有选择报价的投标文件。

3.4.5 投标人应在“政府采购云平台”中填写报价，报价应与上传的报价文件一致，如有不一致，以上传的报价文件中报价为准。

3.5 投标保证金

3.5.1 投标人须按“投标人须知前附表”的规定提供投标保证金。

3.6 投标文件有效期

3.6.1 投标文件有效期按“投标人须知前附表”规定，投标文件应在该有效期内保持有效。合同签订后，投标文件作为合同附件，投标文件有效期同合同有效期。

3.6.2 在特殊情况下，采购人可与投标人协商延长投标文件有效期，这种要求和答复均应以书面形式进行。

3.6.3 投标人可拒绝接受延期要求。同意延长有效期的投标人不能修改投标文件。

3.6.4 投标文件有效期内，投标人撤销投标文件的，应承担采购人提出的索赔。

四、投标

4.1 投标文件的密封及标记

4.1.1 投标文件应按以下方法密封及标记

投标文件密封及标记要求见“投标人须知前附表”。

4.2 投标文件的提交

4.2.1 提交投标文件

1）电子投标文件传输提交

投标人应当在投标截止时间前完成电子投标文件的传输提交至政府采购云平台（https://www.zcygov.cn），投标截止时间前未完成传输提交的，视为未提交投标文件。投标截止时间以后传输提交的投标文件，将被拒收。

2）备份电子投标文件提交

投标人可以提交备份电子投标文件，如提交备份电子投标文件，请按以下方式提交。

应当在投标截止时间以前，供应商将以介质存储的数据电文形式的备份电子投标文件密封并以邮寄或直接送达等形式提交给采购代理机构联系人（郭剑飞 0571-85830257，杭州市文晖路 42 号现代置业大厦西楼 18 层 1804 室），使其在投标截止时间以前收到。封皮应注明投标人名称、项目名称。

备份电子投标文件仅在在线解密异常处理时使用。投标文件已按时解密的，备份电子投标文件自动失效。

4.2.2 投标人提交的投标文件均不予退还。

4.2.3 逾期传输的电子投标文件，采购人将不予受理。

4.2.4 采购人如因故推迟投标截止时间，应以书面形式通知所有投标人。在这种情况下，采购人和投标人的权利和义务将受到新的投标截止时间的约束。

4.3 投标文件的补充、修改和撤回

4.3.1 投标人在投标以后如必须补充、修改或撤回投标文件，必须在投标截止时间以前在“政府采购云平台”上补充、修改或撤回投标文件。补充、修改电子投标文件的，应当先行撤回原文件，补充、修改后重新传输提交。投标截止时间前未完成传输的，视为撤回投标文件。

4.4 备选投标方案

投标人不得提交备选投标方案，否则，投标文件将被判定为无效标。【注：备选投标方案不是指备份投标文件】

4.5 不予受理的投标文件

1）在投标截止时间以后送达的投标文件；

2）未密封的备份电子投标文件；

4.6 投标人不足三家情况处理

至投标截止时间，参加标项投标的投标人不足三家的，除采购任务取消情形外，采购人可选择以下方式之一处理：

1）可将本标项作废标处理，重新组织采购；

2）可按同级政府采购监督管理部门的审批意见采用其他采购方式组织采购；

五、开标、评标及合同签订

5.1 开标

5.1.1 采购人按“投标人须知前附表”规定的时间、地点公开开标，并邀请所有投标人代表准时在线参加。

5.1.2 投标人代表应在线参加开标活动。

开标活动组织人员告知投标人开标活动组织人员情况，已提交投标文件的投标人名单、应当回避的情形、开启报价文件的预计时间等，组织投标人签署《政府采购活动现场确认声明书》。

5.1.3 在线解密

1）开始在线解密

至投标截止时间，开标活动组织人员启动在线解密程序，投标人应登录政府采购云平台在在线解密时间内对已提交的电子投标文件进行解密。

2）解密异常处理

如在线解密失败，开标活动组织人员将启动异常处理，上传投标人在投标截止时间前提交的备份电子投标文件进行再次解密，如未提供备份电子投标文件，将不进行再次解密程序。无法在线解密视为投标人放弃投标。

3）在线解密时间

在线解密时间为 30 分钟。

5.1.4 在线开启投标文件

待所有投标人在线解密结束后，开标活动组织人员在线开启投标文件。

5.1.5 公布商务和技术评审情况

商务和技术评审结束后，开标活动组织人员在线、开标现场公布商务和技术评审有效的投标人名单及无效投标人名称及理由；采用综合评分法的，同时公布其商务和技术得分情况。

5.1.6 在线开启报价文件

开启投标人报价文件，开标活动组织人员宣读开标（报价）一览表有关内容，同时当场制作并打印开标记录表，由在开标现场的投标人代表、唱标人、记录人和现场监督员在开标记录表上签字确认。如投标人代表未签字，也未说明理由，视为无异议。

开标结束后，如发现开标结果与报价文件不一致者，由评标委员会根据报价文件内容进行纠正。

5.1.7 公布评审结果

评审结束后，开标活动组织人员公布各投标人得分、中标候选人名单，及采购人最终确定中标人名单的时间和公告方式等。

5.2 开标异议

投标人如对开标有异议，应当在开标现场提出，开标现场组织人员将当场作出答复，并制作记录。

5.3 投标人资格审查

采购人或采购代理机构将首先审查各投标人的资格条件是否满足招标文件的要求。采购人或采购代理机构对投标人所提供的资格证明材料仅负审核的责任。如发现投标人所提供的资格证明材料不合法或不真实，采购人可取消中标资格并追究投标人的法律责任。

单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的政府采购活动。违反该款规定的，相关投标均无效。

投标文件中提供的资格条件证明材料无法证明其满足招标文件规定资格条件，为无效投标。

5.4 投标文件符合性审查

5.4.1 评标委员会将首先审查每份投标文件是否实质上响应了招标文件的要求，实质性响应的投标文件是指投标文件符合招标文件规定的实质性内容、条件和规定。

5.4.2 重大偏离或保留是指将会影响到招标文件规定的服务范围、质量标准，或会给合同中规定的采购人的权利和投标人的责任造成实质性限制，而纠正这些偏离或保留将对其他提交了实质性响应的投标文件的投标人产生不公平影响的。

5.4.3 细微偏离是指投标文件对招标文件的非实质性内容存在不完全响应或不响应。

5.4.4 重大偏离和保留、细微偏离由评标委员会界定。初步评审时如发现投标文件与招标文件要求有重大偏离和保留，其投标文件将被作无效标处理。投标人不得通过修正或撤消不符合招标文件要求的重大偏离和保留从而使其投标文件实质性响应招标文件要求。但允许投标文件在实质性满足招标文件要求的前提下出现的细微偏差，在详细评审时可按评标办法对细微偏差做出不利于该投标人的评审。

5.5 投标文件的澄清、说明或者补正

5.5.1 评标委员会应当书面形式要求投标人对投标文件中含义不明确、同类问题表述不一致、有明显的文字和计算错误的内容作出必要的澄清、说明或者补正。

5.5.2 投标人的澄清、说明或者补正应当采用书面形式，并加盖公章，或者由法定代表人或其授权的代表签字。投标人的澄清、说明或者补正不得超出投标文件的范围或者改变投标文件的实质性内容。

5.5.3 投标文件的澄清、说明或者补正将在“政府采购云平台”完成。

5.6 错误修正

评标委员会将对确定为实质上响应招标文件要求的投标文件进行校核，投标文件报价出现前后不一致的，按照下列规定修正：

（1）投标文件中开标一览表（报价表）内容与投标文件中相应内容不一致的，以开标一览表（报价表）为准；

（2）大写金额和小写金额不一致的，以大写金额为准；

（3）单价金额小数点或者百分比有明显错位的，以开标一览表的总价为准，并修改单价；

（4）总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。

同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的报价以澄清方式经投标人确认后产生约束力，投标人不确认的，其投标无效。

如投标文件中报价明细表分项价格或单价有遗报，应视作已含在投标总价中；其投标总价在评标过程中不予调整。其分项价或单价由评标委员会在投标总价不变的前提下根据合理的原则对其予以确定；

5.7 合理报价澄清说明

评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在 30 分钟内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。

5.8 无效标

有下列情形之一的投标文件，由评标委员会按少数服从多数原则进行认定，经认定属实后将该投标文件作无效标处理：

1）标项投标报价超过招标文件规定的预算金额或最高限价；

2）《开标一览表》和《投标价格组成明细表》内容不完整且不接受修正意见或字迹不能辨认的或未提供；

3）投标报价明显高于其市场报价或报价明显不合理，且在规定时间内不能合理说明原因并提供证明材料的；

4）符合本须知 5.7 款规定的；

5）投标文件中提供了赠品或者与本项目采购无关的其他商品、服务；

6）获取招标文件的投标人与参加投标的投标人发生实质性变更的且未提供有效证明的；

7）投标人提交两份或两份以上内容不同的投标文件，未声明哪一份有效的；

8）投标文件内容未按招标文件规定盖章的；

9）投标文件含有采购人不能接受的附加条件的；

10）投标文件中承诺的投标有效期少于招标文件中载明的投标有效期；

11）投标人串通投标，妨碍其他投标人的竞争行为，损害采购人或者其他投标人的合法权益；

12）法律、法规、规章及省级以上规范性文件规定的其他无效情形。

13）未实质性响应招标文件中带“▲”条款要求的投标文件；

14）投标文件标明的商务、技术响应与事实不符或虚假投标的；

5.9 有下列情形之一的，其投标无效：

5.9.1 投标人直接或者间接从采购人或者采购代理机构处获得其他投标人的相关情况并修改其投标文件或者响应文件；

5.9.2 投标人按照采购人或者采购代理机构的授意撤换、修改投标文件或者响应文件；

5.9.3 投标人之间协商报价、技术方案等投标文件或者响应文件的实质性内容；

5.9.4 属于同一集团、协会、商会等组织成员的投标人按照该组织要求协同参加政府采购活动；

5.9.5 投标人之间事先约定由某一特定投标人中标、成交；

5.9.6 投标人之间商定部分投标人放弃参加政府采购活动或者放弃中标、成交；

5.9.7 投标人与采购人或者采购代理机构之间、投标人相互之间，为谋求特定投标人中标、成交或者排斥其他投标人的其他串通行为。

5.9.8 不同投标人的投标文件由同一单位或者个人编制；

5.9.9 不同投标人委托同一单位或者个人办理投标事宜；

5.9.10 不同投标人的投标文件载明的项目管理成员或者联系人员为同一人；

5.9.11 不同投标人的投标文件异常一致或者投标报价呈规律性差异；

5.9.12 不同投标人的投标文件相互混装；

5.10 评标

5.10.1 本项目原则上采用电子评审方法。

5.10.2 采购人将按相关规定组织评标委员会，对投标文件进行审查、比较和评价。

5.10.3 评标办法

评标办法详见“第五章 评标办法”。

5.11 有效投标人少于三家的情况处理

评审期间，出现符合资格条件的投标人或者对招标文件做出实质响应的投标人不足三家，采购人可选择以下方式之一处理：

1）可将本标项作废标处理，重新组织采购；

2）可按同级政府采购监督管理部门的审批意见采用其他采购方式组织采购；

5.12 废标

在招标采购中，出现下列情形之一的，应予废标：

（1）符合招标文件规定废标情形的；

（2）出现影响采购公正的违法、违规行为的；

（3）投标人的报价均超过了采购预算，采购人不能支付的；

（4）因重大变故，采购任务取消的；

5.13 确定采购结果

采购人将根据评标委员会提交的评标报告及推荐的中标候选人，确定第一中标候选人为中标人，如排序并列，按技术服务水平得分高者为中标人，如技术服务水平得分相同，抽签确定中标人。

5.14 结果公告

在采购人确认采购结果后，采购代理机构按相关政府采购规定将中标结果发布在政府采购网上进行公告。

5.15 采购过程、采购结果质疑

5.15.1 投标人认为采购过程、采购结果使自己的合法权益受到损害的，投标人可以提出书面质疑。

5.15.2 质疑书须包括以下内容：

（一）投标人的姓名或者名称、地址、邮编、联系人及联系电话；

（二）质疑项目的名称、编号；

（三）具体、明确的质疑事项和与质疑事项相关的请求；

（四）事实依据；

（五）必要的法律依据；

（六）提出质疑的日期。

5.15.3 采购过程的质疑期限自各采购程序环节结束之日起 7 个工作日内，投标人应在质疑期内一次性向采购代理机构提出针对采购过程的质疑，逾期提出不予受理。

采购结果的质疑期限自采购结果公告期限届满之日（自本公告发布之日起至第 2 个工作日止）起 7 个工作日内，投标人应在质疑期内一次性向采购代理机构提出针对采购过程的质疑，逾期提出不予受理。

5.15.4 质疑书中涉及的相关材料中有外文资料的，应当将与质疑相关的外文资料完整、客观、真实地翻译为中文，并注明翻译人员姓名、工作单位、联系方式等信息。

5.15.5 投标人为自然人的，应当由本人签字；投标人为法人或者其他组织的，应当由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。否则不予受理。

5.15.6 质疑书以直接提交、传真或邮寄方式提交（一式三份）。

5.15.7 质疑书以传真形式提交后，同时须向采购代理机构提交质疑书原件，采购代理机构以收到原件之日作为收到质疑日。

5.15.8 投标人不得捏造事实、提供虚假材料或者以非法手段取得证明材料进行质疑。

5.15.9 如联合体投标，质疑应由组成联合体的所有供应商共同提出。

5.16 发出中标通知书

5.16.1 在公告中标结果的同时，采购人及采购代理机构将以书面形式向中标人发出中标通知书。

5.16.2 中标通知书发出后，采购人不得违法改变中标结果，中标人无正当理由不得放弃中标。

5.17 签订合同

5.17.1 采购人应当自中标通知书发出之日起 30 日内，按照招标文件和中标人投标文件的规定，与中标人签订书面合同。所签订的合同不得对招标文件确定的事项和中标人投标文件作实质性修改。

5.17.2 招标文件及补充文件、中标人的投标文件及投标修改文件、评标过程中有关澄清文件和中标通知书均作为合同附件。

5.17.3 拒签合同的责任

中标人接到中标通知书后，在规定时间内借故否认已经承诺的条件而拒签合同者，以投标违约处理，赔偿采购人由此造成的直接经济损失。采购人将向同级政府采购监督管理部门进行报告。

5.18 采购代理服务费

本次采购代理服务费按“投标人须知前附表”规定收取。

中标人不按招标文件规定交纳采购代理服务费，将取消其中标资格。中标人应向采购代理机构交纳招标文件规定的采购代理服务费作为赔偿。

六、其他

6.1 采购过程中出现以下情形，导致电子交易平台无法正常运行，或者无法保证电子交易的公平、公正和安全时，采购组织机构将中止电子交易活动：

（一）电子交易平台发生故障而无法登录访问的；

（二）电子交易平台应用或数据库出现错误，不能进行正常操作的；

（三）电子交易平台发现严重安全漏洞，有潜在泄密危险的；

（四）病毒发作导致不能进行正常操作的；

（五）其他无法保证电子交易的公平、公正和安全的情况。

出现前款规定情形，不影响采购公平、公正性的，采购组织机构将待上述情形消除后继续组织电子交易活动，也可以决定某些环节以纸质形式进行；影响或可能影响采购公平、公正性的，将重新采购。

第七章　投标文件格式

（未提供格式的由投标人自拟）

第一部分 资格文件

封面

采购人：浙江省动物疫病预防控制中心

项目名称：网络安全升级服务项目

项目编号：CTZB-2021090194

标项名称：网络安全升级服务

投 标 文 件

（资格文件）

投标人全称：_____（盖单位公章）

投标文件签署人：_____（签字或盖章）

2021年　　月　　日

说明：电子投标文件可不提供此封面，中标人提供的纸质投标文件应有此封面。

一、资格审查资料

资格审查资料

（一）资格审查须知

1、投标人必须认真填写招标文件规定的所有表格，并对其真实性负责，采购人有权对其进行调查核实和要求澄清。

2、资格审查按通过和不通过两种方式进行评定，投标人的资格等方面的要求作为资格审查通过的强制性资格条件，经核实有一项不符合要求，则投标人的资格审查为不通过，对不通过的投标人的投标文件不进行后续评审。

（二）资格审查资料格式

表1 强制性资格条件

表附件

表 1：强制性资格条件

强制性资格条件表

采购人：浙江省动物疫病预防控制中心

项目名称：网络安全升级服务项目

项目编号：CTZB-2021090194

标项名称：网络安全升级服务

序号	资格条件	应提供的资格审查资料（除承诺函、说明、声明外的其他证件提供复印件）
1.	**基本资格要求：**	**/**
1.1	（1）满足《中华人民共和国政府采购法》第二十二条规定，未被“信用中国”（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单；	（1）营业执照（或事业法人登记证或其他工商等登记证明材料）复印件（供应商为自然人的，提供自然人的身份证明） （2）符合资格条件的声明函【声明函 1】
2.	**落实政府采购政策需满足的资格要求：**	**/**
2.1	本项目为服务项目，本项目服务属于**【软件和信息技术服务业】**，要求服务全部由中小企业承接，即提供服务的人员为中小企业依照《中华人民共和国劳动合同法》订立劳动合同的从业人员。中小企业是指满足《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）第二条规定的企业，监狱企业、残疾人福利性单位视为小型、微型企业；	（3）中小企业声明函/监狱企业声明函及其相关的充分的证明材料/残疾人福利性单位声明函。【声明函 2】
3.	**特定资格要求：**	**/**
3.1	（1）单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的政府采购活动。	（4）与其他供应商无利害关系的声明函。【声明函 3】
3.2	（2）根据《关于规范政府采购供应商资格设定及资格审查的通知》（浙财采监[2013]24 号）第 6 条规定接受金融、保险、通讯等特定行业的全国性企业所设立的区域性分支机构（应依法办理了工商、税务和社保登记手续，获得总公司（总机构）授权或能够提供房产权证或其他有效财产证明材料，能证明其具备实际承担责任的能力和法定的缔结合同能力）、以及个体工商户、个人独资企业、合伙企业（应依法办理了工商、税务和社保登记手续，能够提供房产权	◇属于此种情形的供应商除基本资格要求应提供资料外。还应提供以下资料： （5）金融、保险、通讯等特定行业的全国性企业所设立的区域性分支机构提供总公司（总机构）授权； （6）个体工商户、个人独资企业、合伙企业应提供房产权证或其他有效财产证明材料。 ◇不属于此种情况的供应商提供以下资料： （7）企业类型的声明函。【声明函 4】

	证或其他有效财产证明材料，能证明其具备实际承担责任的能力和法定的缔结合同能力）；	
3.3	（3）非联合体。	（8）提供非联合体的声明函。【声明函5】

【证明材料需加盖投标人单位公章。】

【各声明函格式附后】

表附件：证明资料

相关附件格式附后

【声明函1】符合资格条件的声明函

符合资格条件的声明函

浙江省动物疫病预防控制中心：

浙江省成套招标代理有限公司：

截至浙江省动物疫病预防控制中心（采购人）网络安全升级服务项目（项目名称）CTZB-2021090194（项目编号）的投标截止时间，具有良好的商业信誉，依法缴纳税收和社会保障资金，具有履行合同所必需的设备和专业技术能力，未被列入失信被执行人名单、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单，在参加政府采购活动前三年内没有重大违法记录（重大违法记录是指因违法经营受到刑事处罚、没有被责令停产停业、被吊销许可证或者执照、被处以较大数额罚款等行政处罚），没有因违法经营被禁止参加政府采购活动的期限未满情形。

我方对上述声明的真实性负责。如有虚假，愿意承担相应责任，对此无任何异议。

特此声明！

投标人全称：_____（盖单位公章）

日期：2021 年　月　日

【声明函2】中小企业声明函/监狱企业声明函及其相关的充分的证明材料/残疾人福利性单位声明函

中小企业声明函

本公司郑重声明，根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）的规定，本公司参加浙江省动物疫病预防控制中心（采购人）网络安全升级服务项目（项目名称）CTZB-2021090194（项目编号）采购活动，服务全部由符合政策要求的中小企业承接。相关企业的具体情况如下：

序号	标的名称	行业	承接企业名称	从业人员人数	营业收入（万元）	资产总额（万元）	企业类型
1.	网络安全升级服务	软件和信息技术服务业					□中型 □小型 □微型

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

投标人全称：_____（盖单位公章）

日期：2021 年　月　日

说明：

（1）从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报。

（2）可采用工业和信息化部网站（https://www.miit.gov.cn/）中小企业规模类型自测小程序进行自测后填写。

（3）空格部分由供应商填写，企业类型根据实际情况勾选。

（4）标的名称见采购需求。

监狱企业声明函

本企业郑重声明，根据《关于政府采购支持监狱企业发展有关问题的通知》（财库[2014]68号）的规定，本企业为监狱企业。

根据上述标准，我企业属于监狱企业的理由为：【　　】。

本企业为参加浙江省动物疫病预防控制中心（采购人）网络安全升级服务项目（项目名称）CTZB-2021090194（项目编号）采购活动提供本企业的产品。

本企业对上述声明的真实性负责。如有虚假，将依法承担相应责任。

投标人全称：_____（盖单位公章）

日期：2021 年　月　日

说明：

（1）监狱企业参加政府采购活动时，应当提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件。

监狱企业：是指由司法部认定的为罪犯、戒毒人员提供生产项目和劳动对象，且全部产权属于司法部监狱管理局、戒毒管理局、直属煤矿管理局，各省、自治区、直辖市监狱管理局、戒毒管理局，各地（设区的市）监狱、强制隔离戒毒所、戒毒康复所，以及新疆生产建设兵团监狱管理局、戒毒管理局的企业。

（2）**不属于监狱企业，不用提供此函**

残疾人福利性单位声明函

本单位郑重声明，根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141 号）的规定，本单位为符合条件的残疾人福利性单位，且本单位参加浙江省动物疫病预防控制中心（采购人）网络安全升级服务项目（项目名称）CTZB-2021090194（项目编号）采购活动由本单位提供服务。

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

投标人全称：_____（盖单位公章）

日期：2021 年　月　日

说明：

（1）不属于残疾人福利性单位，不用提供此函。

【声明函3】与其他供应商无利害关系的声明函

与其他供应商无利害关系的声明函

浙江省动物疫病预防控制中心：

浙江省成套招标代理有限公司：

我方参加浙江省动物疫病预防控制中心（采购人）网络安全升级服务项目（项目名称）CTZB-2021090194（项目编号）政府采购活动，与同一标项的其他供应商不存在单位负责人为同一人或存在直接控股、管理关系。

我方对上述声明的真实性负责。如有虚假，愿意承担相应责任，对此无任何异议。

特此声明！

投标人全称：_____（盖单位公章）

日期：2021 年　月　日

【声明函4】企业类型的声明函

企业类型的声明函

浙江省动物疫病预防控制中心：

浙江省成套招标代理有限公司：

我方不属于金融、保险、通讯等特定行业的全国性企业所设立的区域性分支机构、个体工商户、个人独资企业、合伙企业。

本公司对上述声明的真实性负责。如有虚假，将依法承担相应责任。

特此声明！

投标人全称：_____（盖单位公章）

日期：2021 年　月　日

【声明函5】非联合体的声明函

非联合体的声明函

浙江省动物疫病预防控制中心：

浙江省成套招标代理有限公司：

我方独立参加浙江省动物疫病预防控制中心（采购人）网络安全升级服务项目（项目名称）CTZB-2021090194（项目编号）政府采购活动，未与其他单位组成联合体。

我方对上述声明的真实性负责。如有虚假，将依法承担相应责任。

特此声明！

投标人全称：_____（盖单位公章）

日期：2021 年　月　日

第二部分 商务技术文件

封面

采购人：浙江省动物疫病预防控制中心

项目名称：网络安全升级服务项目

项目编号：CTZB-2021090194

标项名称：网络安全升级服务

投 标 文 件

（商务技术文件）

投标人全称：_____（盖单位公章）

投标文件签署人：_____（签字或盖章）

2021年 月 日

说明：电子投标文件可不提供此封面，中标人提供的纸质投标文件应有此封面。

一、法定代表人资格证明书

法定代表人资格证明书

投标人名称：【　　】

法定地址：【　　】

姓名：【　　】性别：【　　】年龄：【　　】职务：【　　】

身份证号码：【　　】

该同志系单位法定代表人。

特此证明！

投标人全称：　　（盖单位公章）

日期：2021 年　月　日

附：

法定代表人信息：

法定代表人联系方式（手机）：【　　】

法定代表人身份证复印件：

法定代表人身份证复印件

二、法定代表人授权签署投标文件委托书

法定代表人授权签署投标文件委托书

（由授权代表签署时提供）

浙江省动物疫病预防控制中心：

浙江省成套招标代理有限公司：

我【（法定代表人姓名）】以【（投标人全称）】法定代表人的身份授权我单位在职员工【（授权代表姓名）】、【（身份证号）】，为我单位的授权代表，签署浙江省动物疫病预防控制中心（采购人）网络安全升级服务项目（项目名称）CTZB-2021090194（项目编号）网络安全升级服务（标项名称）的投标文件。

投标人全称：_____（盖单位公章）

日期：2021 年　月　日

附：

授权代表信息：

授权代表联系方式（手机）：【_____】

授权代表身份证复印件：

授权代表身份证复印件

投标人为其缴纳社保的证明材料（附后）。

说明：投标人法定代表人按招标文件要求签署投标文件时，不需提供此委托书。

三、法定代表人授权开标委托书格式

法定代表人授权开标委托书

浙江省动物疫病预防控制中心：

浙江省成套招标代理有限公司：

我【（法定代表人姓名）】以【（投标人全称）】法定代表人的身份授权我单位在职员工【（授权代表姓名）】、【（身份证号）】，为我单位的授权代表，参加你机构组织的浙江省动物疫病预防控制中心（采购人）网络安全升级服务项目（项目名称）CTZB-2021090194（项目编号）网络安全升级服务（标项名称）的开标活动，签署开标活动中需由投标人签署相关文件、澄清答复、说明等与本项目投标有关的资料。我单位承认授权代表做出的与本项目开标活动有关的全部行为。

投标人全称：_____（盖单位公章）

日期：2021 年　月　日

附：

授权代表信息：

授权代表联系方式（手机）：【_____】

授权代表身份证复印件：

授权代表身份证复印件

投标人为其缴纳社保的证明材料（附后）。

说明：投标人法定代表人作为投标人代表参与本项目采购活动时，不需提供此委托书。

四、偏离表

偏离表

采购人：浙江省动物疫病预防控制中心

项目名称：网络安全升级服务项目

项目编号：CTZB-2021090194

标项名称：网络安全升级服务

序号	招标文件内容	投标响应	说明（正偏离/负偏离）

投标人全称：_____（盖单位公章）

日 期：2021 年　月　日

填表说明：

（1）对招标文件有任何偏离（包括正偏离及负偏离）均应汇总并填写在此表中。

（2）完全满足招标文件要求的投标人只需填写【**完全满足招标文件的全部要求**】。

（3）若中标人以未在偏离表中列出的负偏离为由，不按招标要求签约，采购人有权取消该中标人的中标资格，并按有关规定重新确定中标人或另行采购。

（4）投标文件响应内容对招标文件要求如有偏离均应填写偏离表，如不填写，采购人有权视作投标文件完全响应招标文件要求。

（5）投标人可调整、修改上述表格。

五、廉政承诺书

廉政承诺书

浙江省动物疫病预防控制中心：

我单位响应浙江省动物疫病预防控制中心（采购人）网络安全升级服务项目（项目名称）CTZB-2021090194（项目编号）项目招标要求参加投标。在这次投标过程中和中标后，我们将严格遵守国家法律法规要求，并郑重承诺：

一、不向项目有关人员及部门赠送礼金礼物、有价证券、回扣以及中介费、介绍费、咨询费等好处费；

二、不为项目有关人员及部门报销应由你方单位或个人支付的费用；

三、不向项目有关人员及部门提供有可能影响公正的宴请和健身娱乐等活动；

四、不为项目有关人员及部门出国（境）、旅游等提供方便；

五、不为项目有关人员个人装修住房、婚丧嫁娶、配偶子女工作安排等提供好处；

如违反上述承诺，你单位有权立即取消我单位投标、中标资格，由此引起的相应损失均由我单位承担。

投标人全称：_____（盖单位公章）

日期：2021 年　月　日

六、其他资信资料

其他资信资料

<table>
<tr><td>单位名称</td><td></td><td>电话</td><td></td><td>主管部门</td><td></td><td>单位法人</td><td></td><td>职务</td><td></td></tr>
<tr><td>地 址</td><td></td><td>传真</td><td></td><td>单位性质</td><td></td><td>技术负责人</td><td></td><td>职务</td><td></td></tr>
<tr><td rowspan="10">单位概况</td><td>营业执照经营范围</td><td colspan="3"></td><td rowspan="10">上一年主要经济指标</td><td>年营业收入</td><td colspan="3"></td></tr>
<tr><td>统一社会信用代码</td><td colspan="3"></td><td>资产总额</td><td colspan="3"></td></tr>
<tr><td>资质情况</td><td colspan="3"></td><td></td><td colspan="3"></td></tr>
<tr><td>信用情况</td><td colspan="3"></td><td></td><td colspan="3"></td></tr>
<tr><td>荣誉情况</td><td colspan="3"></td><td></td><td colspan="3"></td></tr>
<tr><td>体系认证</td><td colspan="3"></td><td></td><td colspan="3"></td></tr>
<tr><td>开户银行</td><td colspan="3"></td><td></td><td colspan="3"></td></tr>
<tr><td>账号</td><td colspan="3"></td><td></td><td colspan="3"></td></tr>
<tr><td>在职员工总数</td><td colspan="3">共 人
其中：</td><td></td><td colspan="3"></td></tr>
<tr><td>其他说明</td><td colspan="9"></td></tr>
</table>

【说明】：相关证明材料附后。

投标人全称：_____（盖单位公章）

日期：2021 年 月 日

说明：

（1）投标人的技术力量、资质、信用、荣誉、管理体系认证等资料（如有）。（资格审查资料中已提供的不需重复提供）附后。

（2）投标人应如实填写以上内容，不得有虚假。没有内容可不填。

（3）评标办法所要求资料请务必提供。

七、同类业绩表格式

同类业绩表

采购人：浙江省动物疫病预防控制中心

项目名称：网络安全升级服务项目

项目编号：CTZB-2021090194

标项名称：网络安全升级服务

序号	合同编号	用户名称	合同内容描述	合同金额	签约及完成日期	联系人	联系电话	备注

投标人全称：_____（盖单位公章）

日期：2021 年　月　日

填表说明：

（1）此表不提供，可视为无业绩。

（2）此表仅提供了格式，表格不够可自行增加。

（3）表后附合同等相关证明材料。

（4）评标办法所要求资料请务必提供。

八、提供针对本项目的完整技术解决方案

提供针对本项目的完整技术解决方案

（一）项目需求分析

投标人通过对项目情况的了解，并对项目需求进行分析，阐述项目现状、重点、难点。

（二）采购内容响应说明

招标文件要求			投标文件对应响应内容	是否满足（是/否）
序号	内容名称	具体要求		
“第三章 采购需求”内容（要求点对点逐项列明）				
1				
2				
….	….	….		
“第四章 采购合同”内容（直接注明不能符合内容即可，未注明视为全部满足）				
1				
2				
….	….	….		

投标人全称：_____（盖单位公章）

日期：2021 年 月 日

说明：

（1）投标人应说明具体响应内容。

（2）投标人不得提供与本项目采购无关的其他商品、服务。

（3）不限于表格形式，可采用其他形式表述。

（三）针对本项目的组织实施方案

1．衔接及整合方案

2．网络机房基础设施维护服务

3．网络系统维护服务

4．安全系统维护服务

5．数据备份服务

6．统一安全审计服务

7．应急服务方案

8．进度控制和质量保障

9．技术培训

10．验收方案

投标人自身经验拟定的验收方案齐备性、可操作性、科学性，应从有利于项目实施角度制订方案。

（四）投标人为完成本项目组建的项目组人员名单

每个专职人员的情况应该明确表示，主要内容包括项目组职务、姓名、性别、学历、专业、社保

缴纳等情况。在提交的标书中安排的人员，须为单位的固定职员。

不限于表格形式，可采用其他形式表述。

（1）项目组人员情况表

项目组职务	姓名	性别	学历	专业	社保缴纳	备　注 （人员能力及实施经验说明）

附：相关人员的社保机构出具的社保缴纳证明材料。

（2）项目负责人简历表

姓　名		年 龄		身份证号	
学　历		职 务		拟在本合同任职	项目负责人
毕业学校	年毕业于　　学校　　专业				
主要工作经历					
时　间	参加过的类似项目			担任职务	业主及联系电话

应附身份证、学历证等复印件，管理过的项目业绩附相关证明材料。

第三部分 报价文件

封面

采购人：浙江省动物疫病预防控制中心

项目名称：网络安全升级服务项目

项目编号：CTZB-2021090194

标项名称：网络安全升级服务

投 标 文 件

（报价文件）

投标人全称：_____（盖单位公章）

投标文件签署人：_____（签字或盖章）

2021年 月 日

说明：电子投标文件可不提供此封面，中标人提供的纸质投标文件应有此封面。

一、投标函格式

投标函

浙江省动物疫病预防控制中心：

浙江省成套招标代理有限公司：

（投标人全称）参加你方组织的浙江省动物疫病预防控制中心（采购人）网络安全升级服务项目（项目名称）CTZB-2021090194（项目编号）招标的有关活动，并对网络安全升级服务（标项名称）进行投标。为此我方：

1、承诺在投标人须知规定的投标截止日起遵守本投标文件中的承诺，且在投标有效期满之前均具有约束力。本投标文件的有效期为自投标截止时间起 120 天。

2、承诺已经具备招标文件规定的投标人应具备的资格条件。

3、已详细审核全部招标文件，包括招标文件补充（如果有）、参考资料及有关附件，确认无误。

4、提供投标人须知规定的全部投标文件。

5、投标报价详见《开标一览表》。

6、保证遵守招标文件中的其他有关规定。

7、完全理解不一定接受最低价中标。

8、我公司自愿参加本项目的投标，并保证投标文件中所列举的投标报价文件及相关资料和公司基本情况资料是真实的、合法的。愿意向你方提供任何与该项目投标有关的数据、情况和技术资料。若你方需要，愿意提供我方做出的一切承诺的证明材料。

9、保证忠实地执行双方所签订的合同，并承担合同规定的责任和义务。

10、承诺，招标过程中不存在以下行为：

（一）提供虚假材料谋取中标、成交的；

（二）采取不正当手段诋毁、排挤其他投标人的；

（三）与采购人、其他投标人或者采购代理机构恶意串通的；

（四）向采购人、采购代理机构行贿或者提供其他不正当利益的；

（五）在招标采购过程中与采购人进行协商谈判的；

（六）拒绝有关部门监督检查或者提供虚假情况的。

11、承诺，投标文件有效期内我单位如果撤销投标文件的，我单位接受采购人提出的索赔。

投标人全称：_____（盖单位公章）

日期：2021 年　月　日

单位地址：_____邮编：_____电话：_____传真：_____

二、开标一览表格式

开标一览表

采购人：浙江省动物疫病预防控制中心

项目名称：网络安全升级服务项目

项目编号：CTZB-2021090194　　（价格单位：元人民币）

序号	标项名称	数量	单位	服务周期
1	网络安全升级服务	1	项	**响应招标文件要求**
2	投标价	小写：￥_____元 大写：人民币_____		

投标人全称：_____（盖单位公章）

日期：2021 年　月　日

说明：

（1）具体价格明细详见《投标价格组成明细表》。

（2）大写金额与小写金额不一致时，以大写金额为准。

三、投标价格组成明细表格式

投标价格组成明细表

采购人：浙江省动物疫病预防控制中心

项目名称：网络安全升级服务项目

项目编号：CTZB-2021090194

标项名称：网络安全升级服务

（价格单位：元人民币）

序号	构成服务费名称	内容描述	数量	单位	单价	合价	备注
合计（以上费用之和）							

投标人全称：_____（盖单位公章）

日期：2021 年　月　日

报价说明：

（1）除甲方提供招标文件约定的内容外，其他均由乙方完成。

（2）合计费用结转至开标一览表。

（3）表中不得有给予采购人的赠品、回扣或者与本项目采购无关的其他商品、服务。

（4）各分项报价应合理，且不得低于成本。

（5）投标价格组成明细表是报价的唯一载体。

四、交纳采购代理服务费承诺书

交纳采购代理服务费承诺书

浙江省成套招标代理有限公司：

我单位在你公司组织的浙江省动物疫病预防控制中心（采购人）网络安全升级服务项目（项目名称）CTZB-2021090194（项目编号）网络安全升级服务（标项名称）的招标中若获中标，我单位保证按招标文件**投标须知前附表**的规定，向你公司即浙江省成套招标代理有限公司支付采购代理服务费。如我单位未按上述承诺支付采购代理服务费，你公司有权取消我单位中标资格，由此产生的一切法律后果和责任由我单位承担。我单位声明放弃对此提出任何异议和追索的权利。

特此承诺。

投标人全称：_____（盖单位公章）

日期：2021 年　月　日

政府采购活动现场确认声明书

政府采购活动现场确认声明书

浙江省成套招标代理有限公司：

本人经由单位法定代表人合法授权参加浙江省动物疫病预防控制中心（采购人）网络安全升级服务项目（项目名称）CTZB-2021090194（项目编号）网络安全升级服务（标项名称）政府采购活动，经与本单位法人代表人联系确认，现就有关公平竞争事项郑重声明如下：

一、本单位与采购人之间 □不存在利害关系 □存在下列利害关系_____：

A.投资关系　　B.行政隶属关系　　C.业务指导关系

D.其他可能影响采购公正的利害关系（如有，请如实说明）_____。

二、现已清楚知道参加本项目采购活动的其他所有供应商名称，本单位 □与其他所有供应商之间均不存在利害关系 □与_____（供应商名称）之间存在下列利害关系_____：

A.法定代表人或负责人或实际控制人是同一人

B.法定代表人或负责人或实际控制人是夫妻关系

C.法定代表人或负责人或实际控制人是直系血亲关系

D.法定代表人或负责人或实际控制人存在三代以内旁系血亲关系

E.法定代表人或负责人或实际控制人存在近姻亲关系

F.法定代表人或负责人或实际控制人存在股份控制或实际控制关系

G.存在共同直接或间接投资设立子公司、联营企业和合营企业情况

H.存在分级代理或代销关系、同一生产制造商关系、管理关系、重要业务（占主营业务收入 50%以上）或重要财务往来关系（如融资）等其他实质性控制关系

I.其他利害关系情况_____。

三、现已清楚知道并严格遵守政府采购法律法规和现场纪律。

四、我发现_____供应商之间存在或可能存在上述第二条第_____项利害关系。

投标人全称：_____（盖单位公章）

日期：2020 年　月　日

说明：

（1）投标人解密投标文件及获知其他投标人信息进行如实声明并盖章，以扫描件形式提交给采购代理机构，邮箱：85830198@zjsct.cn。

（2）此声明函不用编入投标文件。