附件

政府采购项目采购文件公平竞争自查表

项目名称		开化县电子政务外网综合保障服务项目		
项目编号		KHZFCG-2025-04		
采购人	名称	开化县人民政府办公室（开化县数据局）		
	联系人	郑先生	联系电话	0570-6019919
采购代理机构	名称	开化县公共资源交易中心		
	联系人	徐先生	联系电话	0570-6016598
专家咨询意见	（可附专家意见书）			

序号	采购文件公平竞争影响性条款	主要内容	审查结果（划√）
1	是否存在排斥或者限制外地经营者参加本地采购活动。	**包括但不限于：**未依法及时、有效、完整地公开采购意向、发布采购公告；直接规定外地经营者不能参与本地特定的采购活动；对外地经营者设定歧视性的资质资格要求或者评标评审标准；将经营者在本地区的业绩、所获得的奖项荣誉作为投标条件、加分条件、中标条件或者用于评价企业信用等级，限制或者变相限制外地经营者参加本地的采购活动；没有法律、行政法规或者国务院规定依据，要求经营者在本地注册分支机构，在本地拥有一定办公面积，在本地缴纳社会保险等，限制或者变相限制外地经营者参加本地采购活动。	□是 ☑否

加盖骑缝章（采购人及采购代理机构）

序号	采购文件公平竞争影响性条款	主要内容	审查结果（划√）
2	是否存在以不合理的条件对供应商实行差别待遇或者歧视待遇。	**包括但不限于：**设定的资格、技术、商务条件与采购项目的具体特点和实际需要不相适应或者与合同履行无关；采购需求中的技术、服务等要求指向特定供应商、特定产品；以特定行政区域或者特定行业的业绩、奖项作为加分条件或者中标、成交条件；对供应商采取不同的资格审查或者评审标准；限定或者指定特定的专利、商标、品牌或者供应商。	□是 ☑否
3	是否限定供应商的所有制形式、组织形式或者股权结构。	**包括但不限于：**没有法律、行政法规或者国务院规定依据，对不同所有制、地区、组织形式的经营者实施不合理的差别化待遇，设置不平等的政府采购准入和退出条件；对民营企业设置不平等条款，对内资企业和外资企业在中国境内生产的产品、提供的服务区别对待。	□是 ☑否
4	是否存在设置或变相设置供应商规模、成立年限等门槛。	**包括但不限于：**将供应商的注册资本、资产总额、营业收入、从业人员、利润、纳税额等规模条件作为评审因素，将有规模要求的认证作为资格要求；要求达到与采购金额不匹配的国家行政主管部门规定的从业等级标准。	□是 ☑否
5	是否合法合理设置资格条件和实质性条款。	**包括但不限于：**将国内非普遍性的认证或对企业规模作出限制的认证作为资格条件；将除进口货物外的生产厂家授权、承诺、证明、背书等作为资格条件；将已明令取消的资质、资格证书作为资格条件；将行业协会、商会颁发的无法律法规依据的资质、资格证书作为资格条件；非单一产品采购项目，未根据采购项目技术构成、产品价格比重等合理确定核心产品，并在采购文件中载明。	☑是 □否
6	是否合法合理设置评审因素。	**包括但不限于：**评审因素未细化和量化，未与相应的商务条件和采购需求对应；商务条件和采购需求指标有区间规定的，评审因素未量化到相应区间，并设置各区间对应的不同分值；将资格条件作为评审因素；将经营年限、特定金额、特定区域、特定行业的合同业绩作为评审因素；将信用等级、信用名单作为评审因素；将投标（响应）文件的规范性、完整性作为评审因素。	☑是 □否

加盖骑缝章（采购人及采购代理机构）

序号	采购文件公平竞争影响性条款	主要内容	审查结果 （划√）
7	是否在法律法规规定之外要求经营者提供或扣留经营者各类保证金。	**包括但不限于：**没有法律、行政法规依据或者经国务院批准，要求经营者交纳各类保证金；限定只能以现金形式交纳投标保证金或履约保证金；在经营者履行相关程序或完成相关事项后，不依法退还经营者交纳的保证金及银行同期存款利息。	□是 ☑否
8	其他不合理限制和壁垒。	（具体情况可附说明）	□是 ☑否
其他需要说明的情况			
审查结论	（参考意见：经审查，本项目采购（招标）文件不存在影响市场主体公平竞争条款，符合现行法律、法规等公平竞争审查相关规定。）		
代理机构主要负责人意见	签字：　　日期：2025.7.18　　单位盖章：开化县公共资源交易中心		
采购人主要负责人意见	签字：郑晓翔　日期：2025.7.18　　单位盖章：开化县人民政府办公室		

加盖骑缝章（采购人及采购代理机构）

评分标准表

序号	评审内容		分值	评分标准	打分方法
1	技术商务部分90分	技术要求	33	根据服务明细中的性能指标及服务描述满足程度进行评分： ①完全满足或高于招标文件要求的，得33分； ②重要指标（★）每有一项负偏离或未响应的扣2分，其他指标每有一项负偏离或未响应的扣1分，扣完为止。 **注：服务描述中要求提供证明材料而未提供的，视为负偏离。**	客观分
		认证证书	4	投标人具有信息及通信系统集成类售后服务五星及以上的得2分，四星及以下的得1分；具有信息安全服务二级资质以上的得2分，三级及以下的得1分；本项最高得4分。 **注：须提供证书扫描件以及国家认证认可监督管理委员会官网（http：//www.cnca.gov.cn/）查询截图，不提供不得分。**	
		投入人员	5	1.投标人拟派的项目负责人具备信息安全管理工程师（高级）、信创集成项目管理师（高级）、注册信息安全管理人员CISP-CISO的，每提供一项证书得1分，最高得3分，以上证书须由同一人持有，提供多人证书的只按一人计分。 2.投标人拟派的项目技术负责人具备信息系统项目管理师（高级）、网络工程师，每提供一项证书得1分，最高得2分，以上证书须由同一人持有，提供多人证书的只按一人计分。 **须提供有效的相关证书扫描件和截至开标前6个月内投标人为该项目投入人员缴纳社会保障资金证明（缴纳凭证扫描件或人社部门出具的证明扫描件，至少提供一个月）并加盖投标人公章，否则不得分。**	客观分
		功能演示	8	根据一体化智能平台功能演示进行评分： 1.平台具有根据密评要求内容做密评自测的能力，得2分； 2.平台具有根据单位资产网络拓扑图可视化，并能自定义绘制的能力，得2分； 3.平台具有包括生成告警规则模型、自动告警监测、异常告警、处理结果数据、处理数据汇总存储功能，得2分； 4.平台具有对接省级政务网设备统一纳管的能力，得2分。 **注：建议演示视频时长不超过15分钟。**	主观分
		技术方案	6	根据投标人对本项目网络建设、网络改造、网络安全的理解，对需求的了解程度等方面综合评分： 方案完整、合理思路清晰的得6分；措施方案内容不清晰不全面有缺陷的每处扣1分；内容不符合或不提供的	主观分

				不得分。	
			9	根据投标人对本项目的现状，包括政务外网现网架构、网络拓扑、技术路线情况、现网设备、链路、机房等情况的详细描述说明分析进行综合评分： 方案完整、合理思路清晰的得9分；措施方案内容不清晰不全面有缺陷的每处扣1.5分；内容不符合或不提供的不得分。	主观分
			6	根据投标人的电子政务外网网络及安全建设方案，从方案的完整性、可实施性和技术前瞻性等角度进行综合评分： 方案详实、内容完整、可实施性强、技术前瞻性强的，得6分；方案一般、内容常规、可实施性一般、技术前瞻性一般的，得3分；方案粗糙、内容缺漏、可实施性差、技术前瞻性不足的，得1分；方案有重大缺陷或无方案的，得0分。	主观分
		服务方案	6	根据投标人的运维服务方案，包括传输链路运维、网络管理维护、安全管理维护、运维巡检服务、本地化服务能力、驻场和重保等方面进行综合评分： 方案详实、内容完整、操作性强的得6分；措施方案内容不清晰不全面有缺陷的每处扣1分；内容不符合或不提供的不得分。	主观分
			3	根据投标人的应急响应方案，从方案的完整性、可实施性和应急保障能力等方面进行综合评分： 方案详实、内容完整、操作性强的得3分；措施方案内容不清晰不全面有缺陷的每处扣1分；内容不符合或不提供的不得分。	主观分
			2	投标人承诺严格按照在接到故障申报10分钟内响应、1小时内到达现场和2小时内故障处理完毕、难以解决的故障经县大数据中心同意后，由双方协商限定时间解决，提供相应承诺函的，得2分，否则不得分。	主观分
			1	针对培训服务的培训人员技术、培训方式、培训内容等方面详细描述方案。根据投标人提出的培训方案合理性进行综合评分： 方案详实、内容完整、操作性强的得1分；措施方案内容不清晰不全面有缺陷的每处扣0.5分；内容不符合或不提供的不得分。	主观分
		实施方案	6	根据投标人的政务网升级演进制定迁移具体实施方案，从方案可行性及实施便捷性等方面进行综合评分： 方案详实、内容完整、可行性及实施便捷性强的，得6分；方案一般、内容常规、可行性及实施便捷性一般的，得3分；方案粗糙、内容缺漏、可行性及实施便捷性不足的，得1分；方案有重大缺陷或无方案的，得0分。	主观分
		项目业绩	1	根据投标人自2021年1月1日（以合同签订时间为准）以来的类似业绩进行打分，每个业绩得0.5分，最高得1分。 **须提供项目合同扫描件。**	客观分

2	报价	10	满足招标文件要求且投标报价折扣最低的为评标基准价，其价格分为满分，其他投标人的价格分统一按下列公式计算（按四舍五入取至小数点后两位）： 投标报价得分=（评标基准价/投标报价）×10。	
3	总得分	100	总得分=技术商务部分得分+报价得分	

采购需求

一、项目概况

开化县电子政务外网是各级政务部门重要公共网络通道、服务设施和数据枢纽，为数字化条件下提升行政效能、改进政务服务、优化营商环境提供平台支撑。为开化县各机关事业单位（含机关事业单位、社区，简称“机关事业单位”）提供政务办公网络服务、互联网服务和网络安全服务。2024年，浙江省数据局发布最新《浙江省电子政务外网建设指南（试行）》浙数局发〔2024〕8号（下文简称《建设指南》），本项目基于《建设指南》要求，进行整体项目规划设计。

二、建设要求

项目服务需基于省数据局《建设指南》的前提下提供网络和安全服务。

网络服务内容含电子政务外网互联网出口服务、电子政务网出口服务、机关事业单位电子政务外网接入服务、公共接入区服务、日常维护服务及网络调整等内容。

安全服务内容含满足二级等保及以上要求的电子政务外网安全设施，保证所承载各级政务部门信息系统的网络畅通，抵御病毒和人为的攻击，在所管辖的网络边界范围内，管理好统一的互联网出入口、并实现非政务类行业用户接入边界的访问控制，及网络管理、安全管理中心等业务信息的安全保障。根据浙江省电子政务外网建设规范要求，本项目对开化县电子政务外网的网络安全进行综合规划与部署，提高电子政务外网网络安全服务能力，提供电子政务外网边界安全等运维服务。

三、项目遵循依据和参考规范

1. 《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）

2. 《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）
3. 《信息安全技术信息系统密码应用基本要求》（GB/T39786-2021）
4. 《信息安全技术 政务网络安全监测平台技术规范》（GB/T 42583-2023）
5. 《浙江省电子政务外网建设指南（试行）》浙数局发〔2024〕8 号
6. 《接入政务外网的局域网安全技术规范》（GW0206-2014）
7. 《国家电子政务外网IPv4地址规划》（GW0206-2015）
8. 《国家电子政务外网 IPv4 地址地方分配部署指南》（GW0207-2015）
9. 《政务外网终端一机两用安全管控技术指南》（GW0015-2022）
10. 《浙江省电子政务外网IPV6地址规划指南（试行稿）》
11. 《浙江省政务外网安全运行监测指标（试行）》
12. 《浙江省电子政务外网网络安全评估指标体系（试行）》

四、服务内容

为了保证与原有项目的一致性和服务配套要求，此次项目服务基于现有使用情况进行服务采购，具体服务架构及内容如下:

- 满足互联网出口带宽4Gbps、不少于120家机关事业单位接入带宽1Gbps的服务能力。
- 公共接入区服务体系：在满足《建设指南》安全要求的基础上进行非政务类行业用户的分级权限接入。同时支持无线局域网、物联网等应用的接入。
- 核心PE网络层面支持IPv4/IPv6双栈与SRv6能力;
- 满足《建设指南》对网络安全的要求，并在部门单位间实现安全隔离;

- 构建统一运维管理系统，提供数据分析和可视化、网络设备识别，以及安全性和隐私保护等功能；
- 满足公安视频专网接入安全要求。
- 行政中心1-4#楼、政务服务中心网络扁平化。

五、服务清单

序号	费用类别
1	网络服务
2	政务安全服务
3	公共接入区
4	一体化智慧管理服务

六、服务要求

序号	名称	服务内容	服务描述	数量及单位
1	网络服务	业务连续性核心网络加固服务	通过2套核心PE传输服务实现政务网网络流量的集中和分发，负责连接区域内多个子网、专网等区域，通过高速的传输线路和先进的路由技术，实现网络中各个节点的通讯。提供高性能、高冗余、可扩展的设备进行组网，满足骨干网络互联互通的业务连接需求。 1.交换容量≥390Tbps，包转发率≥57600Mpps；（提供服务设备能力官网截图） ★2.采用正交CLOS架构，主控槽位≥2个，独立交换网板槽位≥4个，电源槽位≥4，整机业务板线卡槽位数≥4；主控、交换网板、业务板线卡均支持热插拔； ★3.支持 IPv4、IPv6 协议：静态路由、OSPF、OSPFv3、BGP、BGP4+、 IS-IS、IS-ISv6；EVPN、MPLS等协议； ★4.支持SRv6、支持QoS，支持FlexE（灵活以太网）或信道化子接口等网络切片技术、Telemetry； ★5.支持将两台物理设备虚拟化为一台逻辑设备，虚拟组内可以实现一致的转发表项，统一的管理，跨物理设备的链路聚合；（提供官网截图证明材料） 6.支持 SNMP、Syslog、Netconf、Netstream 等基础网络管理协议，支持 NTP 时钟同步； 7.实配：独立主控板卡≥2个，独立交换网板≥2个，千兆光端口≥8个，复用千兆电口端口≥8个，万兆光口≥5个；独立虚拟化万兆光口≥4个；每台实配冗余内置电源模块；SRv6授权；	3年

		互联网出口服务	为政务外网提供互联网出口服务，出口带宽4G。	3年
		网络接入服务	1.提升各机关事业单位网络连接能力，达到千兆接入要求。满足不少于120个接入点电子政务外网访问需求。 2.提供机房租赁服务1项，（租用机柜机房存放设备，包含运行电费、管理等，保障全部设备正常运行。）	3年
		网络集成服务	按现有规范要求对网络整体规划、设计、实施等网络集成服务。	1次
2	政务安全服务	边界安全防护服务1	根据国家信息安全等级保护相关要求，对开化县电子政务外网与省市电子政务外网连接的边界区域设置安全防护边界，并采取必要的安全隔离措施。 ★1.安全操作系统采用冗余设计，出于安全性考虑，多系统需在设备启动过程中进行选择不得在WEB维护界面中设置系统切换选项，可在发生系统故障时，实现系统自动修复。**（提供第三方检测报告证明材料）** 2.为保障系统运行的可靠性与稳定性，要求信息安全设备、系统软件的开发、生产符合TL9000-HSV R6.0/5.5标准; 3.支持根据入接口、源/目的IP地址/地址对象、源/目的端口、协议、用户、应用、选路算法、探测、度量值、权重等多种条件设置策略路由; 4.内置P2P应用、网页应用、加密应用明、数据库应用、工控物联网协议等应用特征库; 5.内置内容过滤功能，可对FTP上传文件、下载文件、删除文件、重命名文件、创建目录、删除目录、列出目录等信令以及邮件发件人、收件人、主题、内容、附件等进行过滤; 6.内置邮件安全防护功能，可进行匿名发件人、收发件人同名、非标客户端、收/发件人频率、收/发件IP频率、邮件长度、附件名称、附件数量检测，支持黑、白名单检测; 7.支持NTP流量检测清洗，能对NTP REQUEST FLOOD、NTP REPLY FLOOD等攻击进行检测并提供基于NTP请求限速、NTP响应限速、源认证、会话认证的防御策略；8.支持配置文件本地备份和回滚，支持＞3个配置文件备份，支持对访问控制策略、NAT策略等关键配置进行单独及加密备份和恢复；支持对配置命令及配置文件的操作行为进行审计; 9.支持日志外发至多个SYSLOG服务器，可设置日志传输协议、外发时间类型、日志语言、合并传输、加密传输等参数;	3年
		边界安全防护服务2	根据国家信息安全等级保护相关要求，对开化县电子政务外网与互联网的边界区域设置安全防护边界，并采取必要的安全隔离措施。 1.互联网防火墙原厂软硬件三年维保; 2.原厂技术支持服务：提供原厂7x24远程技术支持服务，提供产品技术咨询、故障申报受理等服务内容; 3.现场技术支持服务：当网络故障不能使用有效的远程支持方式进行解决时，将派遣工程师到达现场，协助进行现场故障诊断及现场故障排除; 4.备件支持服务：提供快速备件先行服务，故障申报受理后次日内发出; 5.软件支持服务：提供设备软件支持服务,如软件版本更新，软件补丁等; 6.合同签订前提供原厂服务承诺函;	3年
		边界安全防护服务3	边界节点策略防护服务：对各单位间提供边界策略防护服务，“最小化”开放安全原则，包括访问控制、入侵防护等能力。 1.支持路由、网桥、旁路、混合、虚拟网线工作模式，工作模式切换无需重启设备	3年

			2.支持4G接入，并可实现4G连接与有线链路之间互为备份 3.支持静态路由、动态路由、ISP路由 4.支持基于入接口、源地址、目标地址、用户、服务、应用、时间、域名的策略路由 5.支持基于7元组、域名的链路负载均衡策略，负载算法支持优先级和权重 6.支持一体化安全策略：可基于设备接口/安全域、地址、服务、应用、用户、时间等属性，配置入侵防御、病毒防护、URL过滤、应用过滤、会话老化时间、终端过滤等高级访问控制功能 7.内置IPS规则库不少于8000条主流攻击规则，包含安全漏洞、CGI攻击、缓存溢出、木马后门、网络数据库攻击、蠕虫病毒、间谍软件、欺骗劫持等安全类型，并支持在线升级和手动升级 8.拥有自有数据来源，每日可获得不低于6亿次的互联网访问样本，提供在设备端上的全网威胁情报的搜索查询，包括IP、域名、文件（MD5/SHA1等）情报的查询，提供最新的威胁情报信息，能够对新爆发的0day、高危漏洞等进行预警，并提供配置向导协助管理员生成安全防护策略。 9.支持SSL VPN用户防暴力破解功能，可根据用户和IP设置防护阈值 10.可制定策略分别设置私接终端类型个数为阀值进行封堵，同时支持基于IP配置白名单，支持自定义阻断时间，支持限速时长内添加到惩罚通道 11.支持私接用户的PPPoE账号展现，支持状态监控、解锁操作，支持基于用户、MAC、终端数量的监控和搜索 12.可支持基于接口、协议、IP地址、端口、应用进行网络抓包，并可下载导出分析 13.支持三权管理方式，包括账号管理员、权限管理员、审核员，各管理员权限制约；权限管理员支持分配权限，可细致分配界面中每一个模块的读写权限	
		边界安全防护服务4	边界节点策略防护服务：对公共接入区需访问电子政务网的非政务单位客户进行边界区域提供边界策略防护服务，包括访问控制、入侵防护等能力。 1.整机吞吐≥10Gbps,最大并发数≥500万,最大新建数≥20万/秒，2U机架式，国产CPU（8核）+操作系统，内存≥16GB，硬盘≥2TB HDD，电源规格≥1+1冗余电源，风扇数≥3个。网络接口：千兆电口≥16个(含2组电口Bypass），管理电口≥1个，HA电口≥1个，千兆光口≥16个，万兆光口≥8个，接口扩展槽≥4个。 2.支持双机热备；支持主备模式和主主模式；支持同步配置、运行状态等；支持配置抢占模式 3.支持IPv4/IPv6双栈协议的源地址转换、目的地址转换、双向NAT、NAT64等地址转换 ★4.系统定义超过20万条资产指纹库，可识别的主机资产类型包括但不限于通用主机、移动电话、防火墙、网络摄像机、温湿度变送器、呼叫中心、云安全等；可识别的主机资产操作系统包括但不限于Windows，Linux，MAC OS，Android，IOS等；可识别的软件资产类型包括但不限于WEB组件、WEB中间件等WEB应用，Oracle、Hive等数据库，电脑游戏、图像设计等桌面软件以及各类网络协议等；可识别的软件包括但不限于CrushFTP httpd，Android VNC Server等。（提供界面截图证明材料） 5.系统预定义至少11000条主流攻击规则，包含对应IPS规则的级别、防护对象、操作系统、CVE编号等详细信息。 6.支持独立的Web防护模块，系统定义超过4500条WAF规则防护功能，支持常规HTTP漏洞、SQL注入、组件、CMS、WebShell和XSS等类型的Web防护；支持HTTP协议的URL、Method、Referer、	3年

			User-Agent、Cookie、URL-args等字段的等于、不等于、包含、不包含、正则等多种匹配方式的访问控制。 7.威胁情报检索：支持通过关键IP、域名、文件HASH在线检索威胁情报并查看威胁详情。提供界面截图并加盖公司公章 8.安全模式支持智能模式和普通模式。在普通模式下，安全引擎处理网络报文遇到资源不足时会将报文直接丢弃，会影响网络转发；在智能模式下，安全引擎将尽可能的处理网络报文，但不影响网络转发。 9.支持SSL加密流量解密功能，支持HTTPS、SMTPS、POPS、IMAPS协议加密的流量解密，支持HTTPS流量按域名分类做流量解密。并支持上层内容安全功能查杀和访问控制，如入侵防御，内容过滤等。 10.提供对控制策略、上网认证策略、带宽策略、策略路由、源NAT等策略的策略分析，可分析并展示问题策略数量以及所占百分比、问题策略详情、策略宽松度分布情况，简化运维工作。**（提供第三方检测报告）**	
		边界安全防护服务5	边界节点策略防护服务：对开化县电子政务外网与公安视频专网的边界区域提供边界策略防护服务，包括访问控制、入侵防护等能力。 1.整机吞吐≥10Gbps,最大并发数≥500万,最大新建数≥20万/秒，2U机架式，国产CPU（8核）+操作系统，内存≥16GB，硬盘≥2TB HDD，电源规格≥1+1冗余电源，风扇数≥3个。网络接口：千兆电口≥16个(含2组电口Bypass)，管理电口≥1个，HA电口≥1个，千兆光口≥16个，万兆光口≥8个，接口扩展槽≥4个。 2.支持双机热备；支持主备模式和主主模式；支持同步配置、运行状态等；支持配置抢占模式 3.支持IPv4/IPv6双栈协议的源地址转换、目的地址转换、双向NAT、NAT64等地址转换。 4.系统定义超过20万条资产指纹库，可识别的主机资产类型包括但不限于通用主机、移动电话、防火墙、网络摄像机、温湿度变送器、呼叫中心、云安全等；可识别的主机资产操作系统包括但不限于Windows，Linux，MAC OS，Android，IOS等；可识别的软件资产类型包括但不限于WEB组件、WEB中间件等WEB应用，Oracle、Hive等数据库，电脑游戏、图像设计等桌面软件以及各类网络协议等；可识别的软件包括但不限于CrushFTP httpd，Android VNC Server等。 ★5.系统预定义至少11000条主流攻击规则，包含对应IPS规则的级别、防护对象、操作系统、CVE编号等详细信息。**（提供第三方检测报告）** 6.支持独立的Web防护模块，系统定义超过4500条WAF规则防护功能，支持常规HTTP漏洞、SQL注入、组件、CMS、WebShell和XSS等类型的Web防护；支持HTTP协议的URL、Method、Referer、User-Agent、Cookie、URL-args等字段的等于、不等于、包含、不包含、正则等多种匹配方式的访问控制。 7.威胁情报检索：支持通过关键IP、域名、文件HASH在线检索威胁情报并查看威胁详情。 8.安全模式支持智能模式和普通模式。在普通模式下，安全引擎处理网络报文遇到资源不足时会将报文直接丢弃，会影响网络转发；在智能模式下，安全引擎将尽可能的处理网络报文，但不影响网络转发。 9.支持SSL加密流量解密功能，支持HTTPS、SMTPS、POPS、IMAPS协议加密的流量解密，支持HTTPS流量按域名分类做流量解密。并支持上层内容安全功能查杀和访问控制，如入侵防御，内容过滤等。	3年

			10.提供对控制策略、上网认证策略、带宽策略、策略路由、源NAT等策略的策略分析，可分析并展示问题策略数量以及所占百分比、问题策略详情、策略宽松度分布情况，简化运维工作。	
		政务外网安全监管服务	建立安全风险报告和情报共享机制，满足安全监测考核项。同时完成市级网络安全监管平台的对接，省平台实时对接市平台，一旦省平台发生监管变动，市平台会进行二次开发保持一致性，同理区县对接与省市对接一致，做到省市县一体实时同步防护，提供全网安全态势可视化的安全监测感知服务、日志采集服务、流量采集服务、威胁情报服务，强化信息系统基础平台的安全管理，构建可信的信息系统环境，为电子政务外网上所承载的各类信息系统的安全、可靠、稳定、高效地运行提供良好的基础和强有力的保障。 一、威胁态势感知服务，要求如下： 1.工作台首页支持自定义个性化配置，支持以拖拽方式进行画布页面设置，页面可选组件包括原始告警、资产管理、组件管理、风险资产、安全事件、安全日志、平台概览、快速搜索、安全设备、SOAR、系统消息、通报预警、工单、告警监控等，可选组件不少于36个，每个组件均支持点击“收藏”按钮进行自定义收藏； 2.支持安全态势的可视化呈现，以大屏的方式从攻击事件、资产安全、追踪溯源、运行监测、重保方案等多个维度进行可视化展示，提供不少于10块大屏展示界面，并可根据“组织架构”筛选大屏展示数据范围，支持自定义大屏轮播时间和大屏轮播顺序； ★3.安全运营：平台具有统一的安全运营门户，作为重点关注功能的统一入口，如集成态势感知、Sherlock网络星空、通报预警、联动策略、运行监测等多个功能模块，实现平台功能的快速跳转；支持用户配置个人专属的统一门户，可配置项包括门户名称、菜单名称、应用图标等，且菜单内容支持自定义编辑，可链接平台以外的域名地址；**（提供功能截图证明材料）** 4.安全设备资产管理支持一键访问设备的管理界面、大屏投屏演示及设备原始日志，支持查看设备在线状态。 二、日志采集服务，要求如下： 1.日志采集方式应支持但不仅限于Syslog、kafka、ftp、部署代理等4种方式 2.支持采集异构设备的日志数据，实现包括但不限于安全类、网络类、应用服务器类、操作系统类等至少4大类、50种设备的日志接入采集； 3.支持接入应用服务器的性能类数据，包括但不限于CPU、内存和磁盘的性能告警数据； 4.内置解析规则支持厂商>100家，支持解析日志设备型号>2000种，支持对接日志源≥200个。 5.原始日志或原始告警支持多种语法查询，语法至少包括但不限于AND、OR、NOT、==、!=、>、<、>=、<=、exist、notexist、in，语法可任意组合并支持利用中括号和小括号的嵌套查询。 6.日志分析：可对日志进行细粒度解析，解析后的日志根据具体日志包含但不限于：日期、发生时间、接收时间、设备类型、日志类型、日志来源、源地址、目的地址、事件类型、时间范围、操作主体、操作对象、行为方式、技术动作、技术效果、攻击类型、特征类型、协议、地理信息，≥30个字段； 7.具备同时保存事件原始日志数据和标准化后日志数据的能力。 三、流量采集服务，要求如下： 1.资产发现：支持人工录入、流量自动发现、主动扫描、web自动发现、资产同步等不少于5种的资产数据接入方式；流量自动发现方式能自动识别资产类型，如Web服务器、DNS服务器、邮件服务	3年

			器、FTP文件服务器等多种类型资产，支持web业务系统自动发现；支持批量确认流量发现的资产 2.支持自定义流量采集策略，包括过滤策略和采集策略，支持根据IP和协议进行过滤，包括DNS、FTP、HTTP、HTTPS、IMAP、KRB5、LDAP、POP3、RDP、SMB、SMTP、SSH、TELNET、TLS等。 四、威胁情报服务，要求如下： 1.碰撞情报IOC支持通过情报源、IOC类型、情报类型、置信度等多维度进行碰撞分析； 2.支持对接威胁情报中心，支持情报离线更新及在线更新，支持查看情报源中有效情报数、最近更新条数、最近更新时间、今日更新情报数、昨日命中情报数等；支持对接第三方威胁情报平台，支持配置外部情报碰撞接口及查询接口，可对接口请求进行限制 3.本地情报库支持离线导入和手动添加；情报库支持以情报源、IoC、IoC类型、置信度、情报类型、危害等级、是否过期等多条件组合查询；查询结果支持批量导出、删除。 五、数据分析处理服务，要求如下： 1.应内置包括规则模型、关联模型、统计模型、情报模型等多类安全分析模型； 2.安全分析模型支持自定义创建，可通过字段映射、静态值、模板、表达式等多种方式自由定义分析模型的告警名称、威胁等级、告警类型、攻击链、可选字段、告警描述、处置建议等内容 3.支持智能检索语句分析，支持检索语句的中文、英文、拼音智能联想，支持逻辑运算符与字段值的自动提示补全；检索语句支持快速保存，保留检索语句历史记录；检索语句可直接发布成统计指标、规则模型、关联模型、情报模型，对实时数据进行分析与告警。 六、实时监测服务，要求如下： 1.支持对资产进行精细化评级评分计算，资产风险等级包括已失陷、高风险、中风险、低风险，资产评分为百分制，具备资产评级标签；支持查看资产最近15天评级评分趋势、资产威胁词云、资产评分比较等信息； 2.支持告警展示偏好设置，可配置登录默认筛选告警条件，配置包括攻击结果、告警类型、威胁等级、攻击阶段、攻击方向、处置状态、时间范围等信息；支持告警自动刷新； 3.通过在目标主机上安装Agent程序，支持监测目标主机的CPU利用率、内存使用率、磁盘使用率、磁盘使用情况、流量等信息。 七、资产管理服务，要求如下： 1.支持根据探针的内部IP配置或从态势感知平台同步的内部IP配置从流量中进行资产信息的识别，资产信息包括IP、MAC地址、首次发现时间、最近活跃时间、资产类型、发现来源、服务与端口、标签。 2.支持自定义添加组网配置，并可根据配置对资产信息进行组网划分。 八、攻击追踪溯源服务，要求如下： 1.支持安全态势的可视化呈现，以大屏的方式从攻击事件、资产安全、追踪溯源、运行监测、重保方案等多个维度进行可视化展示。 ★2.支持调查场景的四维自定义攻击流向图取证，攻击趋势取证、攻击链分布取证、和实体信息取证，展示攻击者和受害者的威胁情报与资产信息，可联动会话详情，点击查看不同溯源维度的会话详情，通过请求头、响应头等详情字段定位攻击；**（提供功能截图证明材料）** 3.实现实体间网络互访关系的多级钻取，支持通过端口、协议、	

			异常访问类型、攻击链等过滤关联关系，支持实体间网络互访关系的多级钻取，通过“一键溯源”按钮进行威胁关系的自动拓展。 九、威胁溯源服务，要求如下： 1.支持在平台中在线查询情报（如IP/域名/哈希），查询结果包括：威胁类型、情报来源、WHOIS、开放端口、关联情报、SSL证书、样本分析等多个维度的溯源结果； 十、安全模型服务，要求如下： 1.应内置包括规则模型、关联模型、统计模型、情报模型、AI模型等不少于5类安全分析模型，数据配置可选择不同作用域，如全局通用、单选机构，单选机构可选择单独的组织架构；**（提供功能截图证明材料）** 2.支持智能检索语句分析，支持检索语句的中文、英文、拼音智能联想，支持逻辑运算符与字段值的自动提示补全；检索语句支持快速保存，保留检索语句历史记录；检索语句可直接发布成统计指标、规则模型、关联模型、情报模型，对实时数据进行分析与告警 3.支持在告警详情中展示数据血缘关系，包括数据来源、原始日志、规则模型及原始告警，支持下钻至原始日志和规则模型 4.支持安全模型的启用状态恢复出厂设置；支持通过权限认证实现数据恢复出厂设置； 十一、事件通报服务，要求如下： 1.支持选择生成报告时间范围、显示TOP、导出文件类型、报告名称；支持自定义报告统计条件，包括统计业务范围、告警威胁等级、处置状态、告警结果等； 2.报告统计内容支持自定义选择，包括重点安全风险等级、专家建议和指导、平台运行优化建议、详细检查结果和修复建议；支持在线编辑报告 3.支持将预警信息直接转为内部通报，支持将通报内容作为工单定向指派； 4.支持按照组织架构进行绩效考核，总部管理员可查看全局或单个组织的工单处理情况，包括滞留工单情况、风险资产情况及风险资产概率等	
		威胁探针服务	对开化县政务外网关键节点进行威胁流量探针布点，对流量数据进行多维度全方位的威胁监测分析，提供威胁监测与态势分析的能力输出。 1.具备违规操作、违规访问、违规应用、数据外发等370种以上行为审计检测规则，可针对任意单条规则进行启用和禁用。 2.具备隧道通信、可疑内容、恶意IP、恶意域名、恶意证书、远程控制等1800种以上可疑通信检测规则，可针对任意单条规则进行启用和禁用。 3.具备端口扫描、主机存活扫描、服务扫描、Web扫描、扫描器指纹检测等600种以上的探测扫描检测规则，可针对任意单条规则进行启用和禁用。 4.具备SMB漏洞、RDP漏洞、软件漏洞、设备漏洞、系统漏洞、拒绝服务漏洞、Shellcode等6700种以上漏洞利用检测规则，可针对任意单条规则进行启用和禁用。 5.具备挖矿活动、流氓软件、可疑文件、勒索软件、僵木蠕、Webshell、恶意邮件等17000种以上恶意程序检测规则，可针对任意单条规则进行启用和禁用。 6.具备弱口令风险、明文传输风险、HTTP配置风险、中间件配置风向、数据库配置风险、服务配置风险等300种以上配置风险检测规则。 7.支持端口异常、主机对外扫描、主机对外攻击等主机异常检测	3年

			，对任意单条检测规则支持启用和禁用。 8.支持登录异常、暴力破解、行为异常等账号异常检测，对任意单条检测规则支持启用和禁用。 9.支持自定义流量采集策略，包括过滤策略和采集策略，支持根据IP和协议进行过滤，包括DNS、FTP、HTTP、HTTPS、IMAP、KRB5、LDAP、POP3、RDP、SMB、SMTP、SSH、TELNET、TLS等。 10.页面支持多种类型弱口令策略可选，支持的口令字典库50000种以上；支持自定义弱口令字典，可选不同格式弱口令，支持导入自定义弱口令列表；WEB登录参数灵活可配，支持字符串和正则表达式配置；支持Base64编码弱口令和md5散列弱口令检测。 11.支持HTTP、FTP、Telnet、SMB、邮件（SMTP、POP3、IMAP）、RDP、MySQL、Oracle、SQL Server、PostgreSQL、Redis、Mongodb、SSH等暴力破解检测，SSH暴力破解支持爆破登录结果判定；支持暴力破解检测策略自定义，支持添加暴力破解白名单功能。 12.支持对DNS隐蔽隧道通信和DGA域名进行检测，用户可自定义域名检测域名长度和告警阈值，也可以选择是否检测DGA域名家族。 13.支持添加阻断策略，匹配条件包括威胁类型、规则ID、威胁等级，并可自定义阻断策略的生效时间。 14.支持添加访问封禁策略，用户可配置单IP、指定源目的IP、多个端口进行封禁，并可自定义访问封禁策略的生效时长。 15.支持跨三层MAC地址获取，用户可新增指定SNMP服务器，配置包括服务器IP、ARP OID、获取时间间隔、每次获取最大个数、SNMP版本（V1、V2C、V3）；支持自动识别或手动添加交换机的MAC地址并进行识别排除，可自定义配置自动识别的个数阈值。 16.可监控系统CPU、内存、磁盘、TOP CPU进程、TOP内存进程使用情况、网口状态、网口流量、网口丢包情况及数据外送量大小情况，界面可支持 CPU、内存信息获取，实时查看各进程CPU和内存使用情况。 17.支持显示原始日志以及外发到平台的日志曲线图，支持光标悬停至曲线图上，展示该时间点的日志量详情。 18.支持通过Kafka、syslog接口向态势感知平台报送流量审计数据与风险告警信息，Kafka推送支持传输加密，支持SSL、SASL认证+SSL、Kerberos认证+SSL加密 19.自定义配置：可在前端页面自定义配置与态势感知平台之间的数据传输类型、各类型数据均支持任意字段的发送配置。 20.支持系统内用户的业务操作和运维操作。支持审计操作账号、客户端IP、操作时间、操作模块、操作结果，支持审计登录登出、规则运行状态调整、时间同步等10多种操作类型。 21.支持屏幕水印，支持登录失败锁定用户、设置登录密码复杂度、密码过期、用户登录IP绑定等安全策略。	
		入侵检测服务	对针对常见的用户提权、任意代码执行、木马、后门等相关入侵防御进行实时监测。 1.采用非X86多核架构，具备独立的攻击检测引擎与病毒检测引擎。虚拟IPS数量≥16，支持500GB/1TB SATA硬盘和480G SSD 硬盘。 2.支持一体化安全策略，能够基于时间、用户/用户组、应用层协议、五元组、内容安全统一界面进行安全策略配置。 ★3.支持应用风险调优，通过应用层检测引擎智能地分析安全策略允许通过的流量中存在的潜在风险。（提供服务功能截图证明材料） 4.集成入侵防御与检测、病毒防护、带宽管理和URL 过滤等功能；所有特性全面支持IPv6。 5.采用全面深入的分析检测技术，结合模式特征匹配、协议异常检测、流量异常检测、事件关联等多种技术，实现对黑客攻击、	3年

			蠕虫/病毒、漏洞、木马、恶意代码、间谍软件/广告软件等攻击的防御，实现缓冲区溢出、SQL注入、IDS/IPS逃逸等攻击的防御。 ★6. IPS检测到攻击报文或攻击流量后，支持Web重定向、黑名单等响应方式，以实现第一时间隔离有安全威胁的主机。**（提供服务功能截图证明材料）** 7. 支持HTTPS加密流量的安全检测。支持TCP代理和SSL代理，且代理策略中可同时配置多类过滤条件，具体包括：源安全域、目的安全域、源地址、目的地址、用户和服务。一类过滤条件可以配置多个匹配项。 8. 能够防范DOS/DDOS攻击： Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing、SYN Flood、ICMP Flood、UDP Flood、SIP Flood、DNS reply Flood、HTTP Flood（cc）攻击、HTTP慢速攻击检测、ARP欺骗、TCP报文标志位不合法、超大ICMP报文、地址扫描的防范、端口扫描的防范、DNS Flood、ACK Flood、FIN Flood、分片Flood、Tiny-Fragment。 9. 设备提供海量预分类的URL地址库，支持根据URL类别实现URL过滤，URL过滤可以基于时间、主机，能够精细到单一IP地址，设备提供海量预分类的URL地址库，支持管理者自定义新的URL地址和URL分类。 10. 支持关键文件的识别与阻断，能识别的关键文件类型应包含至少以下几类：文档类如Excel、PDF、PowerPoint、Word等，压缩文件类如ZIP、RAR、TGZ等，图像类如BMP、PNG、JPEG等，音频视频类如ASF等，脚本类如JS、Perl、PYTHON、PHP等，网页类如XML、HTML等。	
		上网行为监管服务	通过上网行为管理服务精准识别政务人员网络访问、数据传输、应用使用等行为，实时阻断非法网站访问、恶意软件传播、敏感数据泄露等风险操作，实现网络行为全程可管、可控、可追溯。有效规范政务人员上网行为，提升网络使用效率，降低安全隐患，为政务网安全稳定运行与数据合规流转筑牢防护屏障。 1. 网络层吞吐量≥15Gb；规格不低于：内存：16G，硬盘容量：128G SSD+960G SSD，接口：6千兆电口+2万兆光口SFP+。每秒新建连接数≥30000，最大并发连接数≥1400000，带宽性能≥3Gb，支持用户数≥20000， 2. 要求设备支持网关模式，支持NAT、路由转发、DHCP等功能；支持网桥模式，以透明方式串接在网络中；支持旁路模式，无需更改网络配置，实现上网行为审计；支持两台及两台以上设备同时做主机的部署模式； 3. 支持部署在IPv6环境中，相应的所有功能（上网认证、应用控制、内容审计、报表等等）均都支持IPv6。 ★4. 支持在设置流量策略后，根据整体线路或者某流量通道内的空闲情况，自动启用和停止使用流量控制策略，以提升带宽的高使用率；线路空闲值可自定义；**（提供产品第三方检测报告）** 5. 支持终端用户账号绑定手机号码和微信号，绑定后可以通过手机验证码和微信扫码实现上网快捷登录认证；（提供产品界面截图） 6. 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； 7. 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以及审核人账号。	3年

			8.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； 9.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； ★10.支持账号密码+动态令牌（Authenticator APP）验证码身份认证，支持通过短信和密码绑定动态令牌；**（提供产品第三方检测报告）** 11.内置URL数量在3000万以上，包含分类数量150个以上；管理员可自定义新的URL地址和URL分类； 12.设备内置应用识别规则库，支持超过9000条应用规则数，支持超过6000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；★13.支持外发截屏，当用户外发附件时，会自动截取外发时刻的屏幕，并记录到文件审计日志；**（提供产品第三方检测报告）** ★14.支持通过抑制P2P的下行丢包，来减缓P2P的下行流量，从而解决网络出口在做流控后仍然压力较大的问题；**（提供产品第三方检测报告）** 15.支持超过900种主流Saas应用，对Saas应用有默认分类标签，帮助客户统一配置策略；（提供产品界面截图） 16.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）	
		漏洞扫描服务	全面、快速、准确地发现被扫描网络中的存活主机，准确识别其属性，包括主机名称、设备类型、端口开放情况、操作系统以及开放的服务和软件版本等信息。 一、提供专业的漏洞扫描工具，要求如下： 1.产品具备《计算机软件著作权登记证》。提供有效证书的复印件； 2.漏洞知识库支持自定义编辑，可编辑漏洞描述、修复建议、漏洞等级等内容，在扫描结果和导出报告中应展示编辑后的内容。 3.支持更细粒度扫描任务创建，在一个界面内展示所有任务类型，方便管理员操作。 4.支持主机扫描、网站扫描、数据库扫描、基线配置、事件内容、协同扫描、弱口令扫描、存活主机探测、大数据漏洞扫描、物联网漏洞扫描、信创漏洞扫描、无感扫描14种任务类型。 5.具备“两高一弱”专项扫描任务，一个任务完成对主机和网站资产的“两高一弱”风险排查。任务结果直观展示系统开放端口是否为高危端口。**（提供相关截图证明）** 6.具备弱口令扫描功能，支持弱口令扫描协议数量≥28种，包括FTP、SMB、RDP、SSH、TELNET、SMTP、IMAP、POP3、Oracle、MySQL、MSSQL、DB2、REDIS、MongoDB、Sybase、Rlogin、RTSP、SIP、Onvif、Weblogic、Tomcat、SNMP、Digest、Kingbase、Gbase8s等协议进行弱口令扫描，允许用户自定义用户、密码字典。 ★7.厂商漏洞特征库大于360000条；提供详细的漏洞描述和对应的解决方案描述；漏洞知识库与CVE、CNNVD、Bugtraq、CNCVE、CNVD等国际、国内漏洞库标准兼容。**（提供相关截图证明）** 8.支持自定义扫描策略模板，可以将自定义策略模板导出备份，也可以导入备份的策略模板，能够对策略模板进行编辑、另存为新的模板。 9.漏洞知识库支持检索，可通过CVE ID、CNCVE ID、CNVD ID、CNNVD ID、Bugtraq、CVSS分值、漏洞名称、风险等级、发现日期等进行检索查看。 10.支持导出的报告类型≥5种，包括HTML、WORD、EXCEL、XML、	3年

			PDF报告格式。 11.支持在线查看报告和离线导出报告，报告导出可将弱口令隐藏不以明文的形式展现至报告。 12.提供审计功能，能够对登录日志、操作日常进行记录和查询，并可以将日志导入导出操作。	
		网络保障与驻场人员服务	一、网络运维服务：为开化县电子政务网络系统所处机房的软硬件正常运行提供运行维护保障服务，提供应急抢修加定期巡检服务，软硬件故障分析与处理。日常维护重点在于保障开化县电子政务外网的正常运行。包括接入设备的日常维护、设备配置的维护与管理、相关网络环境的运维。 1.要求技术服务人员接到故障申报后，应在最短的时间内使维护服务设备尽快恢复正常，维护人员故障处理完毕需将故障处理情况反馈给贵中心相关负责人，并提交维护运维报告，分析故障原因，详细记录故障处理过程，提出预防同类故障解决方案。 2.要求相关设备发生重大故障，应在24小时内修复，若因各种原因需要联系厂家或因备件不到位等原因不能及时修复的，将提供故障分析报告，报告主要内容是针对安全重大或重复发生的故障，分析根本原因，提出问题解决方案。如设备损坏或无法修复，中标人应在24小时内予以替换，替换设备性能不低于原设备。 3.要求按标准操作规范执行巡检服务。每月对维护设备进行巡检，巡检的频率在确保不影响业主单位业务正常开展的前提下全面巡查一次。巡检结束后将租用和维保设备运行状态和故障情况进行汇总，以书面形式递交给贵中心。 二、驻场人员服务：派驻一名具有丰富网络安全处理工程师至开化县大数据中心进行驻点服务。完成网络运维服务和政务外网日常等工作。具备相关网络知识技能及相关机房故障应急处理和维护措施，定期巡检、监控等措施，运维过程通过运维系统闭环管控，及时发现上报各种隐患和风险，供决策使用。 1、全面分析客户信息系统和网络中存在的各种安全问题，确保整体网络环境安全性，及时对系统进行软件或硬件的升级，设备策略调优等工作。 2、对政务外网资产进行全生命周期安全管理，围绕着确认归属、确认构成、变更管理三个维度减少业务系统在政务外网上的受攻击面。 3、对监测的业务系统，提供脆弱性管理服务，对发现的隐患进行通报，跟进并协助做好漏洞修复工作。 4、分析安全监管平台所产生的安全事件，包括发现安全事件进行通报预警预防、发现高危访问源攻击、持续性攻击源进行预警阻断、攻陷事件发现通报处置。 5、对各类网络安全设备和信息系统进行安全配置、安全加固、日常巡检。 6、严守工作秘密，驻场工程师通过背景调查并签署保密责任书，供应商与采购人签署保密协议，对所知悉的事项及信息须严格保密，所有资料、技术文档妥善保管，不得遗失、转借、复印，不得以任何形式向第三方透露。 7、承担维保工作质量责任，严格遵循操作规程（规范）。若因违反操作规程、调试检测或操作维护使用不当，造成系统设备损坏的，按照采购人要求限期无条件恢复，并承担由此而带来的全部责任和损失。 8、对各类安全检查任务进行安全检查指标对比，形成统计分析、安全评价和工作质量考核。驻场人员协助开化大数据中心开展日常考评工作，有效促进网络安全检查工作落实，逐步提升相关单位网络安全工作水平。有效开展网络安全防护工作，了解网络安全现状，分析存在问题，通过该服务对被监管单位开展网络及数	3年

			据安全工作评价，根据各类指标项评估情况等直观展示内容为监管单位提供数据决策支持。 9、驻场人员具备相关的网络故障处理经验或中级网工证书，在驻场服务期间，无法胜任此工作，甲方有权提出更换驻场人员，并在2个月内完成更换。	
		二级等保测评	对本次改造的电子政务外网从技术与管理两大方面进行测评，并提供咨询服务，协助业主等保测评分数达到良好及以上。	1次
		二级密评	对本次改造的电子政务外网对重要信息系统、关键信息基础设施等使用的密码技术、产品和管理体系进行合规性、有效性的专业检测与评估服务，并提供咨询服务，协助业主等保测评分数达到良好及以上。	1次
3	公共接入区服务体系	公共接入区核心网络服务	提供满足公共接入区核心服务能力的PE设备一台，实现对接入电子政务网的非机关事业单位、物联感知终端、无线局域网、5G终端等进行访问权限控制。 1.交换容量≥120Tbps，包转发率≥14000Mpps；**（提供服务设备能力官网截图）** 2.主控槽位≥2个，电源槽位≥2，整机最大业务槽位数≥4，主控、电源、线卡板均支持热插拔； 3.支持 IPv4、IPv6 协议：静态路由、OSPF、OSPFv3、BGP、BGP4+、 IS-IS、IS-ISv6；EVPN、MPLS等协议； ★4.支持将两台物理设备虚拟化为一台逻辑设备，虚拟组内可以实现一致的转发表项，统一的管理，跨物理设备的链路聚合；**（提供官网截图证明材料）** 5.支持NQA或iFIT等网络质量检测技术； 6.支持 SNMP、Syslog、Netconf、Netstream 等基础网络管理协议，支持 NTP 时钟同步； 7.双主控，双电源，万兆光口≥4个，千兆电口≥12个，千兆光口≥8个，SRv6授权；	3年
4	一体化智慧管理服务	数据采集服务	通过一体化智慧管理服务可实现政务数据的高效汇聚与精准分发，确保数据传输零中断、服务响应毫秒级；同时，借助动态路由优化与负载均衡机制，平台能灵活适配政务专网、业务子网及公共服务网络，实现多类型数据的安全隔离与无缝交互，全面满足政务决策分析、民生服务办理、跨域协同办公等多样化场景需求，为政务数字化转型提供坚实的智慧化服务底座。 一体化智慧管理服务的工具需要满足如下要求： ★1.轻量级数据智能分析：基于与平台端关联的定制分析策略，采用轻量的智能数据分析模型，对数据智能分类和智能分析。**（提供相关截图证明）** 2.操作系统：国产化的边缘计算终端，包括操作系统和硬件的国产化。 3.资产生命周期：通过资产管理模型，对资产的在用、故障、清退等阶段进行数字化管理，提供有效的管理模型，实现资产的全生命周期管理。 ★4.自定义画布：对网络拓扑图实现拖拉拽形式的自定义绘制，根据网络部署的需求及变化，通过平台随时更新网络拓扑图，实现可视化操作管理。**（提供相关截图证明）** ★5.可视化分析模型管理：管理服务端的多维度可视化分析模型，支撑全局可视化总览服务模块。**（提供相关截图证明）** 6.智能分析策略管理：管理探针终端的定制分析策略，为探针终端的轻量级数据分析进行参数配置。 7.提供20套探针 8.能够接收指令、停止指令，能够进行数据存储、数据上报，能够进行数据统计策略和数据过滤策略配置。 9.从多个数据源收集数据，并将其汇总到一起，对采集数据进行	3年

			统一策略管理。 10.基于与平台端关联的定制分析策略，采用轻量的智能数据分析模型，对数据智能分类和智能分析。	

▲七、安全保密要求

提供的产品和服务符合国家相关安全规定及《浙江省信息技术服务外包安全网络管理办法》要求。

▲八、质量保证措施

1.整体项目服务期间，提供7×24小时故障响应服务，包括中心机房、全县电子政务外网的故障处理及安全服务事件处理等；5×8小时的工作日驻点服务；重大活动、重要节假日、应急情况期间，进行24小时现场值守。

2.现场即时服务工程师应充分了解开化县政务外网和各系统现状。

3.驻场服务。驻点人员必须服从采购人的工作安排，具备工作责任心，驻点人员工作时间原则上同采购人上班时间，驻点人员办公场所由采购人免费提供，其办公设备（符合信创要求并固定）及其他事项由中标人自理。中标人要做好对驻点人员日常管理工作，定期安排驻点人员进行业务培训。

4.服务期间，对系统进行扫描、渗透测试之前必须要先提供相应的技术方案与采购人技术人员充分沟通，以确保系统的安全运行。任何渗透测试，需要在采购人许可的时间、环境下由经验丰富的专业技术人员进行。

5.中标人应及时处置服务过程中所发现的所有问题，取得较好的处置成效，并在事后提交安全处置情况报告。

6.对于现场驻点人员无法解决的问题，项目负责人应第一时间抽调公司具备问题解决能力的人员奔赴现场协同处置。

7.中标人须对采购人的数据严格保密，未经采购人授权，不得泄露给其他单位和个人。