中共贵州省委组织部云资源总集（二次）

需求公示

一、资格审查

1.满足《中华人民共和国政府采购法》第二十二条规定；

2.落实政府采购政策需满足的资格要求：

标项 1：供应商应为中小企业/小微企业，供应商应为监狱企业，供应商应为残疾人福利企业。

3.申请人一般资格要求：

（1）供应商符合《中华人民共和国政府采购法》第二十二条规定，并提供下列材料：

① 具有独立承担民事责任的能力：根据竞争性磋商文件“第三章　评审方法和评审标准”中的“1.3 资格审查要求”表中的1-1提供营业执照等证明文件；

② 具有良好的商业信誉和健全的财务会计制度：提供经合法审计机构出具的2023年度或2024年度财务审计报告，或2025年基本账户银行出具的有效的资信证明；

③ 具有履行合同所必需的设备和专业技术能力：填写本采购文件《响应文件格式》中提供的《供应商资格声明书》作为证明材料；

④ 具有依法缴纳税收和社会保障资金的良好记录：提供2025年任意1个月依法缴纳税收和社会保障资金的相关材料（如不需缴纳的，须出具有效的证明材料）；

⑤ 参加政府采购活动前三年内，在经营活动中没有重大违法记录：填写本采购文件《响应文件格式》中提供的《供应商资格声明书》作为证明材料；

（2）信用信息查询：

① 供应商在“信用中国”网站（www.creditchina.gov.cn）未被列入“失信被执行人”和“重大税收违法失信主体”名单；（“信用中国”网站查询路径：信用服务→重点领域严重失信主体名单查询→“失信被执行人”和“重大税收违法失信主体”）。

② 供应商在“中国政府采购网”（www.ccgp.gov.cn）未被列入“政府采购严重违法失信行为记录名单”。

需提供自采购公告发出之日到响应文件递交截止时间之前的任何时候在“信用中国”网站及“中国政府采购网”（www.ccgp.gov.cn）的信用信息查询记录截图；或提供信用信息记录符合要求的承诺书（格式自拟）。

4.本项目的特定资格要求：

标项1：无

二、符合性审查

序号	检查因素	检查内容	是否允许澄清、说明或者更正
1	响应文件的签署、盖章	响应文件按照磋商文件要求签署、盖章的，或签字人有法定代表人有效委托书的。	不允许
2	报价金额	响应报价未超过磋商文件中规定的预算金额或者最高限价	不允许
3	是否低价	响应报价是否明显低于成本或市场价，可能影响采购质量的。	允许澄清、说明；不允许更正
4	附加条件	响应文件不含有采购人不能接受的附加条件	不允许
5	响应有效期	响应有效期满足磋商文件要求	不允许
6	违法行为	无串通响应、弄虚作假、行贿等违法行为。	不允许
7	实质性响应	响应文件对磋商文件的实质性要求和条件作出响应（标注★号项）；（评审依据为：采购需求偏离表）	不允许
8	其他情形	无法律法规和磋商文件中规定的其他无效情形。	不允许

三、评审标准

序号	评分因素及说明	分值
	一、价格部分（20 分）	
1.1	磋商报价得分＝（磋商基准价/最后磋商报价）×20 注： ①磋商基准价指满足磋商文件要求且磋商价格最低的磋商报价，最后磋商报价指满足磋商文件要求的各供应商的最后报价。 ②磋商小组认为供应商的报价明显低于其他通过符合性审查的供应商的报价，有可能影响服务质量或者不能诚信履约的，应当要求其在磋商小组规定的合理时间内提供书面说明或承诺函，必要时提交相关证明材料；供应商不能证明其报价合理性的，磋商小组应将其作为无效响应处理。	20 分
	商务部分（35 分）	
2.1	**履约经验（满分15分）：** 供应商提供 2021 年 1 月 1 日至响应文件递交截止日期（以合同签订时间为准）承接过的类似项目业绩，每提供 1 份业绩得 3 分，满分 15 分。 **证明材料：**需提供含合同关键页（包括双方盖章、合同金额、签约时间、采购内容）复印件或扫描件并加盖供应商公章，未按要求提供或未提供的不得分。 **类似业绩定义：**指云安全类项目业绩；是否属于有效的类似项目业绩由磋商小组根据供应商提供的业绩在采购内容、技术特点等方面与本项目的类似程度进行认定，不能判定具体类别的业绩无效。	15 分
2.2	**服务评价（满分10分）：** 供应商提供“2.1 履约经验”评分中，所提供业绩对应的采购方（甲方）出具的感谢信或表扬信或评价为优（好）的正面评价文件，每提供一份得 2 分，满分 10 分。 **证明材料：**提供感谢信或表扬信或评价文件复印件加盖供应商公章。	10 分
2.3	**项目快速响应能力（满分 10 分）：** 供应商书面承诺，如成交，服务期内在贵阳市内设立专门的项目组，	10 分

	并确保该项目组在服务期内持续存在，以确保项目的顺利进行和高效完成。提供承诺得 10 分，不提供不得分。 **证明材料：提供书面承诺函作为证明材料，未提供不得分。**	
三、技术部分（45 分）		
3.1	**拟派项目负责人（1 人）（满分 10 分）：** 1.具有计算机软考高级证书-信息系统项目管理师，得 3 分； 2.具有注册信息安全管理人员（CISP）证书，得 3 分； 3.具有 5 年及以上工作经验，得 3 分，不满足不得分； 4.具有计算机相关专业本科及以上学历，得 1 分，不满足不得分。 **证明材料：**提供人员的身份证及社保证明，并按对应评分要求提供以下材料： 针对评分 1：提供信息系统项目管理师证书； 针对评分 2：提供 CISP 证书； 针对评分 3：提供工作经验证明（提供承诺函，须注明从业年限）； 针对评分 4：提供毕业证或学位证。 上述材料提供复印件加盖供应商公章，未提供或提供不全的不得分。 **社保证明：**供应商单位 2025 年任意 1 个月为其缴纳社保的证明材料。	10 分
3.2	**拟派项目技术负责人（1 人）（满分 5 分）：** 1.具有计算机软考高级证书-信息系统项目管理师，得 2 分； 2.具有 5 年及以上工作经验，得 2 分； 3.具有计算机相关专业本科及以上学历，得 1 分。 **证明材料：**提供人员的身份证及社保证明，并按对应评分要求提供以下材料： 针对评分 1：提供信息系统项目管理师证书； 针对评分 2：提供工作经验证明（提供承诺函，须注明从业年限）； 针对评分 3：提供毕业证或学位证。 上述材料提供复印件加盖供应商公章，未提供或提供不全的不得分。 **社保证明：**供应商单位 2025 年任意 1 个月为其缴纳社保的证明材料。	5 分
3.3	**拟派团队成员（不含项目负责人、技术负责人）（满分 15 分）：** 1.每有一名成员具有计算机相关专业本科及以上学历，得 1 分，满分 5 分； 2.每有一名成员具有注册信息安全工程师（CISP）证书或计算机软考	15 分

	中级及以上证书，得 2 分，满分 10 分。 **证明材料：**提供人员的身份证及社保证明，并按对应评分要求提供以下材料： 针对评分 1：提供毕业证或学位证； 针对评分 3：提供 CISP 证书或计算机软考证书。 上述材料提供复印件加盖供应商公章，未提供或提供不全的不得分。 **社保证明：**供应商单位 2025 年任意 1 个月为其缴纳社保的证明材料。	
3.4	**项目理解与实施计划（满分 5 分）：** 供应商需针对本项目提供详细的项目理解与实施计划，包括项目理解与概述、项目进度安排、任务分解和实施步骤、人员配置及角色分工。磋商小组将根据方案内容进行综合评审： **一档（5 分）：**项目理解深刻，目标明确，实施计划详尽合理，进度安排科学，任务分解和角色分工明确，资源保障充分。 **二档（4 分）：**项目理解较好，目标较明确，实施计划较为详尽合理，进度安排基本科学，任务分解和角色分工较明确。 **三档（3 分）：**项目理解一般，实施计划基本合理，进度安排较为科学，任务分解和角色分工一般。 **四档（2 分）：**项目理解较差，实施计划不合理，进度安排不科学，任务分解和角色分工不明确。 **五档（1 分）：**项目理解严重不足，实施计划严重不合理，进度安排混乱，任务分解和角色分工缺失。 **注：未提供方案不得分。**	5 分
3.5	**运维服务方案（满分 5 分）：** 供应商需针对本项目提供详细的运维服务方案，包括运维服务方式、运维服务交付物等。评标委员会将根据方案内容进行综合评审： **一档（5 分）：**运维服务方案全面完善，运维服务方式科学高效，交付物详尽全面，可操作性强，能够充分满足项目需求。 **二档（4 分）：**运维服务方案较为完善，运维服务方式较为科学，交付物较为全面，具备较强的可操作性，能够较好满足项目需求。 **三档（3 分）：**运维服务方案基本完整，运维服务方式基本可行，交付物基本覆盖，具备一定的可操作性，能够满足项目基本需求。 **四档（2 分）：**运维服务方案不够完整，运维服务方式不够科学，交付	5 分

	物覆盖不全，可操作性较弱，满足项目需求能力有限。 **五档（1 分）：**运维服务方案严重缺失，运维服务方式不明确，交付物严重不足，缺乏可操作性，无法满足项目需求。 **注：未提供方案不得分。**	
3.6	**应急保障方案（满分 5 分）：** 供应商需针对本项目提供详细的应急保障方案，包括应急响应方式、应急服务内容等。评标委员会将根据方案内容进行综合评审： **一档（5 分）：**应急保障方案全面完善，应急响应方式科学高效，应急服务内容详尽全面，可操作性强，能够有效应对各类突发情况。 **二档（4 分）：**应急保障方案较为完善，应急响应方式较为科学，应急服务内容较为全面，具备较强的可操作性，能够较好应对突发情况。 **三档（3 分）：**应急保障方案基本完整，应急响应方式基本可行，应急服务内容基本覆盖，具备一定的可操作性，能够满足基本应急需求。 **四档（2 分）：**应急保障方案不够完整，应急响应方式不够科学，应急服务内容覆盖不全，可操作性较弱，应对突发情况能力有限。 **五档（1 分）：**应急保障方案严重缺失，应急响应方式不明确，应急服务内容严重不足，缺乏可操作性，无法有效应对突发情况。 **注：未提供方案不得分。**	5 分
四、政策性加分（5 分）		
4.1	**节能、环境标志产品：** 投标产品属于节能产品、环境标志产品的（强制采购产品除外），在评审过程中，给予适当加分，即在总得分基础上，每一项加 0.3 分；如投标产品同时属于节能产品和环境标志产品的，每一项加 0.5 分，最高不得超过 2 分。须提供投标产品在财政部、发展改革委、生态环境部等部门出具的品目清单所在页和国家市场监管总局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（复印件加盖投标单位公章）。	2 分
4.2	**原产地少数民族投标主产品：** 对原产地在少数民族自治区和享受少数民族自治待遇的省份的投标主产品(不含附带产品)，享受政策性加分和价格扣除，在总得分基础上加 3 分。投标主产品按照不得低于本采购项目预算金额 50%进行确	3 分

	定。 ①少数民族自治区：内蒙古自治区、新疆维吾尔自治区、宁夏回族自治区、广西壮族自治区、西藏自治区； ②享受少数民族自治待遇的省份：青海省、云南省、贵州省。	

★四、商务要求

（一）服务期限及地点

1.服务期限：合同生效之日起12个月。

2.服务地点：采购人指定地点。

（二）付款方式

合同签订后采购人向成交供应商支付50%的合同款，项目整体服务内容完成，且提供的成果通过验收、项目结算审计后，根据审计的金额采购人向成交供应商支付剩余合同款，如履约保证金扣除后仍然不能与审计后的金额保持一致的，供应商退还相应费用。

（三）履约保证金

签订合同前，成交供应商须以银行汇票、电汇凭据、银行进账账单等非现金形式向采购人缴纳合同金额10%的履约保证金。在履约期内，若成交供应商不按双方签订合同规定履约，则履约保证金不予退还。履约保证金不足以赔偿损失的，按实际损失金额赔偿。履约保证金在履约期结束后无任何服务及质量问题，且项目结算审计后无须供应商退还费用或扣除金额的，采购人将一次性无息全额退还履约保证金给成交供应商。

（四）验收标准与程序

项目完成后，采购人将按照合同约定的验收标准和程序进行验收。

若项目未通过验收，供应商应按照采购人要求进行整改，直至项目通过验收为止。

（五）保密要求

供应商应严格遵守国家保密法律法规，对项目实施过程中获取的采购人敏感信息予以严格保密。未经采购人书面同意，供应商不得将项目信息泄露给第三方或用于其他用途。

（六）项目建设配合

1.本项目的设计费用已包含在采购预算内，供应商的报价应包含本项目的设计

费。成交供应商需按成交价的1%向设计方支付设计费。

2.服务期的补充说明

为规范本次信息系统运维政府采购项目，妥善处理新旧运维服务过渡及运维周期统一问题，特制定本规则：

2.1 已到期运维合同过渡处理

（1）对于在本次采购完成前已到期的运维合同，在新运维供应商确定前，原运维供应商需继续提供运维服务，保障系统正常运行。

（2）新运维供应商确定后，需按照其成交价，结合原运维供应商继续提供服务的实际时长，核算相应运维费用，并支付给原运维商。

费用结算范围：对于本次采购完成前，原运维供应商已为各系统持续提供的运维服务，其服务费用由本次中标供应商承担。

核算方式：以本次成交总金额为基数，除以“原运维供应商延续服务时长+新运维供应商 12 个月服务时长”的总和，得出月度单价后，再乘以原运维供应商的实际服务月数，即为应支付给原运维供应商的费用。

例：若系统原运维供应商已延续服务 5 个月，本次成交供应商需提供 12 个月服务，则总服务周期合计 17 个月。应支付原运维供应商的费用=（A 系统中标金额÷17 个月）×5 个月。

（3）新运维供应商签订的运维合同起始时间自合同签订生效之日起计算，且需确保承担至少连续 12 个月的运维服务周期。

2.2 运维服务时间统一规则：本次采购涉及的所有运维项目，自新运维供应商合同生效后，统一将运维服务周期起始时间调整为合同生效日，实现运维周期与非涉密运维总集服务周期同步。

3.如采购人聘请第三方审计机构对本项目进行结算审计，结算审计产生的费用，由成交供应商据实支付。

4.若本项目在下一年度采购工作完成前服务期限已超，成交供应商需持续提供服务直至采购流程全部结束并完成交接工作。对于此期间额外提供的服务，将根据实际服务时长据实结算。

（七）应急响应要求

1.中标人接到中共贵州省委组织部故障报修通知或监测到中共贵州省委组织部运维对象监控预警后，及时与中共贵州省委组织部责任人联系，及时通过远程或现

场处理方式采取必要措施解决各类技术故障。

2.对于重大软硬件系统故障，应立即通知领导部门，协调技术人员保障系统尽快恢复运行，最大限度保护系统资源和数据资源。

3.对运维过程及结果进行书面记录，重大事件维护完成后将故障处理结果逐级上报。

4.严格按照国家相关规范执行各类运维服务内容。

5.建立健全各类维护文档和资料记录文件，并妥善保管。

6.中标人应当根据有关标准规范，根据中共贵州省委组织部各系统的重要性和运维事件的紧急程度，划分运维服务级别，制定相应的服务响应指标，具体情况如下：

控制指标	一级	二级	三级	四级
业务重要性	非常重要	重要	较重要	一般
系统年可用率	≥99.95%	≥99.5%	≥98%	≥95%
年无故障运行时间	8756h	8716h	8585h	8322h
服务支持时间	7×24h	7×24h	7×24h	法定工作时间
服务响应时间	≤10min	≤0.5h	≤1h	≤4h
	驻场，即时响应	驻场，即时响应	驻场，即时响应	驻场，工作时间响应
故障恢复时间	一般故障≤1h；重大故障≤2h	一般故障≤2h；重大故障≤8h	一般故障≤12h；重大故障≤36h	一般故障≤24h；重大故障≤72h

一般故障：出现系统报错或警告，但业务系统能继续运行且性能不受影响。或系统技术功能、安装或配置咨询等，不影响业务的预约服务。

重大故障：系统崩溃导致业务停止、数据丢失。或出现部分部件失效、系统性能下降但能正常运行，不显著影响正常业务运作。

若不能按照上述服务响应标准及时处理故障，中标人应当组织技术专家对故障进行诊断，并出具解决方案，处理过程及时向中共贵州省委组织部报告。

（八）其他要求

1.重要时刻及重大节假日开展相关安全服务：在重大事件及突发事件时刻，成

交供应商应按要求开展相关安全服务，开展防护，安排专业技术人员进行值守，并出具相关报告。

2.按时提供安全周报、月报、半年报、年报，并根据相关检测报告，开展漏洞修复工作。

★五、技术要求

（一）采购清单

序号	名称	最高限价（万元）	备注
1	等保测评、云安全设备、安全服务及自建机房设备硬件质保及特征库升级服务（非等保测评部分）	113.01	2025年01月01日至2025年12月31日
2	国密资源续费及密码应用安全性评估（非密码测评部分）	47.05	2025年01月01日至2025年12月31日
3	合计	160.06	对以上备注有疑问的请及时联系采购代理机构，避免产生理解上的偏差。

（二）采购内容

序号	项目名称	运维内容和指标	工程量	单位	备注
（一）	**等保测评、云安全设备、安全服务及自建机房设备硬件质保及特征库升级服务（非等保测评部分）**	1.服务需求：包括安全产品、安全服务。 2.服务要求：相关人员有义务对用户单位提交的任何文档资料以及数据与结果保密,严格依照《中华人民共和国保密法》相关事宜执行，以确保任何相关技术及业务文档不得泄露。 3.服务方式：远程服务。			
1	云安全保障	互联网区域--上云系统：12380 举报网站、贵州省委组织部人才项目网络申报评审系统、贵州党建云、贵州省“优才卡”网上综合服务平台、贵州省党员干部网络培训学院信息系统。			

序号	项目名称	运维内容和指标	工程量	单位	备注
1.1	下一代防火墙	1.具备传统防火墙、web 应用安全防护、网络入侵检测与防御功能。 2.支持基于应用的策略路由，可实现为不同的应用类型智能选择相应的链路。 3.支持基于 WEB 地址 URL 的策略路由，可实现将不同类型的网站流量智能分配到不同的链路。 4.支持一体化安全策略配置，可以通过一条策略实现用户认证、IPS、AV、URL 过滤、协议控制、流量控制、并发、新建限制、垃圾邮件过滤、审计等功能,简化用户管理。 5.支持将源 MAC 作为独立的访问控制条件，防止非法设备接入。 6.支持针对策略中的源、目的地址进行新建限制,可以针对单 IP(或地址范围)进行新建控制。 7.支持根据 IP 地址进行策略查询、支持根据服务端口进行策略查询。	5	套	防护流量 100M
1.2	堡垒机	1.详细记录多种运维协议，为违规、误操作等提供追查依据。 2.支持用户客户端 IP 和 MAC 限制，支持黑白名单两种工作模式。 3.支持限定配置中可指定用户通过指定的应用发布服务器对资源进行访问。 4.支持 WEB 界面上传改密脚本，通过	1	套	授权资产 100 个

序号	项目名称	运维内容和指标	工程量	单位	备注
		自定义脚本模式实现新增改密类型，满足多种改密需求。 5. 支持僵尸、幽灵、孤儿账号稽核功能，并可以导出异常账号稽核情况报告，方便管理员统计异常账号情况。 6. 支持管理员通过 WEB 界面自定义上传用户手册，保证使用手册及时更新。 7. 支持页面空闲超时退出，支持启用验证码，支持多次登录锁定账号。			
1.3	GMVPN	1. 提供通用安全套件，确保传输数据的机密性及完整性。实现安全、快速接入。 2. 支持 IPSec、SSL、PPTP、L2TPVPN 的统一用户管理和认证体系，实现用户名口令一次配置，即可适用于全部 VPN 类型接入，无需分别购买不同类型 VPN 接入授权。 3. 支持多数据库，根据用户规模的大小，可以灵活切换 SQLite 和 Mysql 数据库，支持数据库备份和还原操作。 4. 支持对在线用户的实时监测，包括 VPN 用户信息、程序名称、会话 ID、客户端名称和用户类型。 5. 支持用户访问策略，支持访问痕迹的留存、支持对访问用户的详细信	1	套	最大并发连接 20 个

序号	项目名称	运维内容和指标	工程量	单位	备注
		息查询（客户端名称、客户端特征码、客户机 MAC、登录时间、登录用户名等）、支持账号和客户端 MAC 的关联绑定，仅允许绑定的 MAC 地址客户机访问。			
1.4	漏洞扫描	1.通过对系统进行安全脆弱性深度检测，发现可被利用漏洞，达到主动防御效果。 2.支持对主流 SCADA/HMI 软件的识别与扫描，包括 Wincc、IGSS、Movicon、Promotic、iFix、WebAccess、ForceControl、KingView 等。 3.支持 IPv4 和 IPv6 环境的部署和扫描,可扫描的 IP 地址总数量无限制。 4.支持对主流大数据组件的识别与扫描，包括：Ambari、Cassandra、Elasticsearch、Flume、Hadoop、Hbase、Hive、Impala、Kafka、Mongodb、Oozie、Redis、Spark、Storm、Splunk、Yarn、Zookeeper，能够扫描的大数据组件漏洞扫描方法不小于 300 种。	1	套	授权资产 50 个
1.5	数据库审计	1.以全面审计和精确审计为基础，实时记录网络上的数据库活动，对数据库操作进行细粒度审计的合规性管理，对数据库遭受到的风险行为进行实时告警。 2.支持对 Oracle 数据库状态的自动监	1	套	授权数据库 10 个

序号	项目名称	运维内容和指标	工程量	单位	备注
		控，可监控会话数、连接进程、CPU和内存占用率等信息。 3.支持国产数据库人大金仓、达梦、南大通用、神通、高斯、瀚高、巨杉、OceanBase、AnalyticDBMySql、AnalyticDBMySql、AnalyticDBPostgreSQL、RDSMySql、RDSPostgreSQL等数据库的审计。 4.支持MongoDB、redis数据库的审计。 5.支持对针对数据库的SQL注入、CVE高危漏洞利用、口令攻击、缓冲区溢出等攻击行为进行审计。 6.系统支持数据库中存储过程自动学习，可学习存储过程中涉及的操作并与审计事件中的存储过程名进行关联，方便确认存储过程是否存在风险。			
1.6	日志审计	1.对每天所记录的信息进行审计和检查，采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月。 2.支持全智能范式化解析模式，通过配置原始日志标识库，系统自动识别原始日志，并匹配映射系统通用标准字段，支持解析字段的编辑和调整，确保日志解析的高精准。 3.支持自定义事件搜索条件，并作为	1	套	授权资产共需要100个

序号	项目名称	运维内容和指标	工程量	单位	备注
		检索策略保存，以树形结构进行组织，形成一个搜索分析策略树。 4. 支持系统在数据存储时进行阈值设置，包括存储时间不能少于 180 天、使用容量告警、剩余容量告警、删除方式等设置。 5. 支持对选中的事件日志提供在线/离线地图定位、支持源 IP 与目的 IP 分布走向的视网膜图展示、支持事件拓扑分析用于描述整个事件的访问关系及过程。			
1.7	EDR	1. 支持可疑文件检测，支持过滤邮件病毒、文件病毒、恶意网页代码、木马后门、蠕虫等多种类型病毒查杀。 2. 支持勒索病毒专项检测防护能力；支持挖矿病毒专项检测防护能力。 3. 支持首页声音告警，有新事件及时提醒管理人员关注。 4. 支持 windows 与 linux 策略进行差异化配置与维护。 5. 支持终端基础资产清点，包括：IP、连接 IP、MAC、资产名称、操作系统版本、内核版本、处理器、内存、硬盘大小和型号、网卡型号、首次在线时间、最后在线时间等。 6. 支持详细记录终端进程每一次变动信息，包括：进程 ID、进程名、动	1	套	授权资产共需要 70 个

序号	项目名称	运维内容和指标	工程量	单位	备注
		作（启动、退出）、进程路径、父进程 ID、父进程名、进程命令行参数、启动或退出时间。			
2	**云安全保障**	电子政务外网区域--上云系统：贵州党建云平台、贵州省党员干部网络培训学院(二期)			
2.1	下一代防火墙	1.具备传统防火墙、web 应用安全防护、网络入侵检测与防御功能。 2.支持基于应用的策略路由，可实现为不同的应用类型智能选择相应的链路。 3.支持基于 WEB 地址 URL 的策略路由，可实现将不同类型的网站流量智能分配到不同的链路。 4.支持一体化安全策略配置，可以通过一条策略实现用户认证、IPS、AV、URL 过滤、协议控制、流量控制、并发、新建限制、垃圾邮件过滤、审计等功能,简化用户管理。 5.支持将源 MAC 作为独立的访问控制条件，防止非法设备接入。 6.支持针对策略中的源、目的地址进行新建限制,可以针对单 IP(或地址范围)进行新建控制。 7.支持根据 IP 地址进行策略查询、支持根据服务端口进行策略查询。	1	套	防护流量 50M
2.2	下一代防火墙	1.具备传统防火墙、web 应用安全防护、网络入侵检测与防御功能。	1	套	防护流量 2

序号	项目名称	运维内容和指标	工程量	单位	备注
		2.支持基于应用的策略路由，可实现为不同的应用类型智能选择相应的链路。 3.支持基于 WEB 地址 URL 的策略路由，可实现将不同类型的网站流量智能分配到不同的链路。 4.支持一体化安全策略配置，可以通过一条策略实现用户认证、IPS、AV、URL 过滤、协议控制、流量控制、并发、新建限制、垃圾邮件过滤、审计等功能,简化用户管理。 5.支持将源 MAC 作为独立的访问控制条件，防止非法设备接入。 6.支持针对策略中的源、目的地址进行新建限制,可以针对单 IP(或地址范围)进行新建控制。 7.支持根据 IP 地址进行策略查询、支持根据服务端口进行策略查询。			OOM
2.3	堡垒机	1.详细记录多种运维协议，为违规、误操作等提供追查依据。 2.支持用户客户端 IP 和 MAC 限制，支持黑白名单两种工作模式。 3.支持限定配置中可指定用户通过指定的应用发布服务器对资源进行访问。 4.支持 WEB 界面上传改密脚本，通过自定义脚本模式实现新增改密类型，满足多种改密需求。	1	套	授权资产 20 个

序号	项目名称	运维内容和指标	工程量	单位	备注
		5.支持僵尸、幽灵、孤儿账号稽核功能，并可以导出异常账号稽核情况报告，方便管理员统计异常账号情况。 6.支持管理员通过 WEB 界面自定义上传用户手册，保证使用手册及时更新。 7.支持页面空闲超时退出，支持启用验证码，支持多次登录锁定账号。			
2.4	SSL/VPN	1.提供通用安全套件，确保传输数据的机密性及完整性。实现安全、快速接入。 2.持 IPSec、SSL、PPTP、L2TPVPN 的统一用户管理和认证体系，实现用户名口令一次配置，即可适用于全部 VPN 类型接入，无需分别购买不同类型 VPN 接入授权。 3.支持多数据库，根据用户规模的大小，可以灵活切换 SQLite 和 Mysql 数据库，支持数据库备份和还原操作。 4.支持对在线用户的实时监测，包括 VPN 用户信息、程序名称、会话 ID、客户端名称和用户类型。 5.支持用户访问策略，支持访问痕迹的留存、支持对访问用户的详细信息查询（客户端名称、客户端特征码、客户机 MAC、登录时间、登录用	1	套	最大并发连接 5 个

序号	项目名称	运维内容和指标	工程量	单位	备注
		户名等）、支持账号和客户端 MAC 的关联绑定，仅允许绑定的 MAC 地址客户机访问。			
2.5	漏洞扫描	1. 通过对系统进行安全脆弱性深度检测，发现可被利用漏洞，达到主动防御效果。 2. 支持对主流 SCADA/HMI 软件的识别与扫描，包括 Wincc、IGSS、Movicon、Promotic、iFix、WebAccess、ForceControl、KingView 等。 3. 支持 IPv4 和 IPv6 环境的部署和扫描，可扫描的 IP 地址总数量无限制。 4. 支持对主流大数据组件的识别与扫描，包括：Ambari、Cassandra、Elasticsearch、Flume、Hadoop、Hbase、Hive、Impala、Kafka、Mongodb、Oozie、Redis、Spark、Storm、Splunk、Yarn、Zookeeper，能够扫描的大数据组件漏洞扫描方法不小于 300 种。	1	套	授权资产 10 个
2.6	日志审计	1. 对每天所记录的信息进行审计和检查，采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月。 2. 支持全智能范式化解析模式，通过配置原始日志标识库，系统自动识别原始日志，并匹配映射系统通用	1	套	授权资产共需要 20 个

序号	项目名称	运维内容和指标	工程量	单位	备注
		标准字段，支持解析字段的编辑和调整，确保日志解析的高精准。 3. 支持自定义事件搜索条件，并作为检索策略保存，以树形结构进行组织，形成一个搜索分析策略树。 4. 支持系统在数据存储时进行阈值设置，包括存储时间不能少于 180 天、使用容量告警、剩余容量告警、删除方式等设置。 5. 支持对选中的事件日志提供在线/离线地图定位、支持源 IP 与目的 IP 分布走向的视网膜图展示、支持事件拓扑分析用于描述整个事件的访问关系及过程。			
2.7	EDR	1. 支持可疑文件检测，支持过滤邮件病毒、文件病毒、恶意网页代码、木马后门、蠕虫等多种类型病毒查杀。 2. 支持勒索病毒专项检测防护能力；支持挖矿病毒专项检测防护能力。 3. 支持首页声音告警，有新事件及时提醒管理人员关注。 4. 支持 windows 与 linux 策略进行差异化配置与维护。 5. 支持终端基础资产清点，包括：IP、连接 IP、MAC、资产名称、操作系统版本、内核版本、处理器、内存、硬盘大小和型号、网卡型号、首次	1	套	授权资产共需要 10 个

序号	项目名称	运维内容和指标	工程量	单位	备注
		在线时间、最后在线时间等。 6. 支持详细记录终端进程每一次变动信息，包括：进程 ID、进程名、动作（启动、退出）、进程路径、父进程 ID、父进程名、进程命令行参数、启动或退出时间。			
2.8	数据库审计	1. 以全面审计和精确审计为基础，实时记录网络上的数据库活动，对数据库操作进行细粒度审计的合规性管理，对数据库遭受到的风险行为进行实时告警。 2. 支持对 Oracle 数据库状态的自动监控，可监控会话数、连接进程、CPU 和内存占用率等信息。 3. 支持国产数据库人大金仓、达梦、南大通用、神通、高斯、瀚高、巨杉、OceanBase、AnalyticDBMySql、AnalyticDBMySql、AnalyticDBPostgreSQL、RDSMySql、RDSPostgreSQL 等数据库的审计。 4. 支持 MongoDB、redis 数据库的审计。 5. 支持对针对数据库的 SQL 注入、CVE 高危漏洞利用、口令攻击、缓冲区溢出等攻击行为进行审计。 6. 系统支持数据库中存储过程自动学习，可学习存储过程中涉及的操作并与审计事件中的存储过程名进行关联，方便确认存储过程是否存在	1	套	授权数据库 10 个

序号	项目名称	运维内容和指标	工程量	单位	备注
		风险。			
3	**安全服务**	云上业务系统（含电子政务外网）安全服务，延续服务项目			
3.1	安全检测服务	对系统开展网络安全检测服务，即安全渗透测试服务，及时发现对系统的漏洞及其脆弱性，并提供修复建议。	40	人天	
3.2	服务器安全基线核查和加固服务	按照工信部安全基线标准，开展安全基线核查和加固服务。包括的云服务器资源开展安全基线核查服务，同时对不合规的基线项开展安全加固。安全加固是保证设备和系统安全运行的关键防护措施。	1	项	
3.3	网络安全监测服务	开展系统的网络安全监测服务，及时发现网络攻击行为，开展网络安全预警，网络安全事件分析，网络安全事件处置等服务。	1	项	
4	本地机房安全服务	自建机房业务系统（贵州省综合党务管理系统）安全服务（含人工驻场服务一年，持证‘CISP 证书’上岗，一名。）			
4.1	本地机房安全产品巡检服务	定期对信息化系统开展安全巡检工作，可以充分掌控企业信息系统的安全现状，提前发现信息化系统运行过程中存在的安全隐患，根据巡检过程中发现的问题进行针对性治理，使得业务持续稳健运行。	12	次/年	
4.2	安全检测服务	是通过模拟恶意黑客可能使用的攻击技术和漏洞发现技术，对受测企业的	40	人天	

序号	项目名称	运维内容和指标	工程量	单位	备注
		网络及应用系统进行深入探测，发现信息系统最薄弱的环节，充分了解企业网络当前存在的安全隐患。 渗透测试的过程如同网络真实入侵事件的演练。通过专业的渗透测试服务，可以使得信息系统的管理人员了解入侵者可能利用的途径，直观的了解系统真实的安全强度。能够真正未雨绸缪，主动发现安全问题并在第一时间完成有效防护，让攻击者无机可乘，进而避免企业由于网络黑客攻击造成重大损失。			
4.3	服务器安全基线核查和加固服务	基线核查加固服务是根据国际、国内、行业相关标准，建立各主流操作系统、数据库、中间件、虚拟设备等相关资产的安全基线要求，核查加固安全运维服务人员所维护的安全设备系统安全基线情况。 有效修复、减少系统中存在的高、中危漏洞，降低安全漏洞和隐患带来的安全风险，提升系统自身的安全防护能力，最大程度保障系统的持续、安全、稳定运行。	1	项	
4.4	网络安全监测服务	网站监测服务是通过网站安全监测平台全方位的对网站可用性进行监控，敏感词监测、网页防篡改监测、木马暗链等监测，最终以报告的形式呈现给客户，提醒用户对网站存在的漏洞	1	项	

序号	项目名称	运维内容和指标	工程量	单位	备注
		进行修复和整改。 使客户节省精力，更多的投入到自身业务中，提高工作效率；按需购买，无需专职人员维护和管理，降低投入成本，获得更高收益；专业团队提供服务，及时发现风险隐患，通知客户采取措施，降低损失。			
4.5	应急演练	应急演练服务是一项针对单位整体安全状态保障的服务，该项服务形式多样，可根据用户实际情况进行调整。行业、单位或部门通过采取安全演练的方式，反思、整改，吸取教训弥补不足，总结经验推动工作，进一步完善网络信息安全工作方案及应急预案，提高工作能力。 通过应急演练活动，行业、单位或部门建立健全应用系统和网络运行应急工作机制，验证相关组织、人员对应用系统及网络运行突发事件的组织指挥能力和应急处置能力，同时验证单位现有应急预案的可行性，并对应急预案进行及时更新完善，进一步提高应对突发紧急安全事件的能力。	1	项	
4.6	驻场服务	安排一名具有 CISP 认证的网络安全服务工程师，提供 5*8 驻场服务，主要服务内容包括日常的安全运维工作，及时处理出现的异常情况；同时对安全设备流量进行分析、监测，以保证	1	年	

序号	项目名称	运维内容和指标	工程量	单位	备注
		网络的正常、有序，提升网络安全等级。优化安全设备的安全策略，使得应用系统安全平稳的运行。			
5	**本地机房安全设备**	等保三级要求，硬件质保服务项			
5.1	安全网管系统	采购时间为 2017 年 12 月，设备采购第 7-8 年，即 2025 年	1	台	
5.2	上网行为管理系统	采购时间为 2017 年 12 月，设备采购第 7-8 年，即：2025 年	1	台	
5.3	防火墙系统	采购时间为 2016 年 11 月，设备采购第 8-9 年：2025 年	1	台	
5.4	入侵检测系统	采购时间为 2016 年 11 月，设备采购第 8-9 年：2025 年	1	台	
5.5	网络安全审计	采购时间为 2016 年 11 月，设备采购第 8-9 年：2025 年	1	台	
5.6	堡垒主机	采购时间为 2016 年 11 月，设备采购第 8-9 年：2025 年	1	台	
6	**特征库、软件版本升级服务**				
6.1	入侵检测系统	特征库升级，2025 年	1	年	
6.2	入侵防护系统	特征库升级，2025 年	1	年	
（二）	**国密资源续费及密码应用安全性评估**	1.服务内容：国密应用。 2.服务指标：在检查整个过程中,因现场工作人员不当操作造成用户单位设备、系统故障或损坏,应当承担相应的赔偿责任。相关人员有义务对用户单			

序号	项目名称	运维内容和指标	工程量	单位	备注
		位提交的任何文档资料保密，严格依照《中华人民共和国保守国家秘密法》相关事宜执行，以确保任何相关技术及业务文档不得泄露。 3.服务方式：远程服务。			
1	云密码服务（VSM）	国密算法服务即 SM2、SM3、SM4 等国产算法； 相关标准服务即符合 GMT 0018-2012 等国家、行业标准； 云密码服务即签名、验签及摘要密码服务； 云加密服务数据加解密服务。	12台	年	
2	密钥管理控制台（TMC）	提供对称密钥管理、非对称密钥管理、证书管理、密钥同步与导出、密钥监控、日志审计分析	3台	年	
3	安全代理服务（SPS）	即 SSL 代理服务，支持传输加密、数字证书认证	8台	年	
4	云安全接入服务（GMVPN）	用于运维管理的 vpn 代理服务	3台	年	
5	弹性 IP（EIP）	弹性 IP	8个	年	
6	身份认证服务	使用省信息中心提供的互联网、电子政务网数字证书，身份认证服务	/	/	

（三）其他

工作内容以2025年贵州省政务信息化运维项目实施方案及其评审报告内容为准。

注：未尽事宜由采购人及成交供应商在签订合同时进行完善。