2024省工业和信息化厅网络安全维护 需求公示

一、资格审查要求

供应商资格及相关证明材料要求		供应商名称
资格审查	具有独立承担民事责任的能力：提供法人或者其他组织的营业执照（或事业单位法人证书）；自然人参与响应的提供身份证明；（复印件加盖供应商单位公章）	√/×
	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2022年度或2023年度财务审计报告，或基本开户银行出具的资信证明；（复印件加盖供应商单位公章）	√/×
	具有履行合同所必需的设备和专业技术能力：提供具备履行合同所必需的设备和专业技术能力的承诺函；（加盖供应商单位公章）	√/×
	具有依法缴纳税收和社会保障资金的良好记录：提供2024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)；（复印件加盖供应商单位公章）	√/×
	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：提供参加本次采购活动前3年内在经营活动中没有重大违法记录的书面声明函；（加盖供应商单位公章）	√/×
	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； 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；如未提供，则以采购代理机构在响应文件递交截止当日查询结果为准，并把查询结果放入归档资料；如未能在“信用中国”中查询到相关信息，需自行提供承诺书，格式自拟。（“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”。）	
联合体投标	是否满足本项目不接受联合体磋商的要求。	√/×
结论（√代表通过，×代表不通过，结论填通过或不通过）		**通过或不通过**

二、符合性审查要求

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）	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	评审因素及说明	分值
	一、价格部分（10分）	
1.1	磋商报价得分＝（磋商基准价/最后磋商报价）×10 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【例如：成本价格分析及近一年内所投同类项目签订的合同（原件）】；供应商不能证明其报价合理性的，磋商小组有权将其作为无效响应处理。	10分
	二、商务部分(45分)	
2.1	**同类项目业绩（满分20分）** 供应商2021年1月1日至今承担过的同类项目(同类项目是指：网络安全维护服务或网络运维服务）业绩，每提供一个同类业绩得5分，最高得20分。 注1：提供合同关键页复印件。 注2：关键页指：签订合同方的单位名称、合同名称、采购内容及含有签订合同方的落款盖章、签订日期页。未显示上述内容的合同不予计分。	20分
2.2	**供应商认证情况（满分8分）** **1.基础认证证书（满分4分）：** 1.1 具有有效期内的质量管理体系认证证书，得2分； 1.2 具有有效期内的信息安全管理体系认证证书，得2分。 **2.信息系统安全类认证证书（满分4分）：** 2.1 具有信息安全服务资质认证证书-信息系统安全运维服务二级及以上，得2分。	8分

	2.2 具有信息安全服务资质认证证书-信息系统安全集成服务二级及以上，得2分。 注：提供上述评分所述证书。	
2.3	**供应商为本项目投入的项目实施团队综合能力（满分17分）** **1.项目经理（1人，满分6分）：** 1.1 具有计算机技术与软件专业技术资格-信息系统项目管理师证书，得3分； 1.2 具有计算机技术与软件专业技术资格-网络工程师证书，得1分； 1.3 具有通信专业工程师（中级）及以上职称，得2分。 **2.技术负责人（1人，满分7分）：** 2.1 具有计算机技术与软件专业技术资格-信息系统项目管理师证书，得3分； 2.2 具有中国信息安全测评中心-注册信息安全专业人员(CISP)证书，得2分； 2.3 具有通信专业工程师（中级）及以上职称，得2分。 **3、项目团队人员（满分4分）：** 3.1 具有中国信息安全测评中心-注册信息安全专业人员(CISP)证书，每有1人得2分，最多得4分； **注：上述人员均需提供身份证、评分中要求的证书以及2024年任意2个月供应商为其缴纳社保的证明，未提供证明材料的对应评分项不得分。**	17分
三、技术部分（45分）		
3.1	**服务方案（满分35分）** 供应商需根据项目采购需求提供服务方案，方案至少包含以下内容： ①运维响应时间； ②运维手段； ③应急处置方案； ④日常售后服务计划； ⑤风险控制。	35分

	评审规则： 1、供应商按要求提供有针对本项目的以上方案，每提供一个得4分，满分20分； 2、磋商小组针对供应商提供的服务方案进行综合评审。若供应商的方案在表现出内容的完整性、详尽性，并且无任何缺陷，得满分15分。方案中每有一处缺陷（如：包括但不限于有不足之处、遗漏或偏差、逻辑不连贯、技术漏洞等）扣1分，扣完为止。（主观分） **注：**有缺陷是指：套用其他项目方案、与实际情况明显不符、或存在与项目明显无关的文字内容、内容欠缺或前后矛盾、合理性或可行性不足、内容原理错误、涉及的规范及标准错误、有错别字（引起歧义情况）的任意一种情形。	
3.2	**故障处理时间承诺** 1.供应商承诺：重大网络故障30分钟内到达现场并进行排除，得5分。 2.供应商承诺：一般性故障，接到用户网络安全故障申告电话后，10分钟内响应并按要求排除，得5分。	10分
四、政策性加分（5分）		
4.1	**节能环保加分（满分2分）** 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	**少数民族加分（满分3分）** 对原产地在少数民族自治区和享受少数民族自治区待遇的省份	3分

	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%进行认定。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。	
合计		105 分
备注：上述评分标准中，未要求提供原件的，响应文件中提供复印件（扫描件）加盖供应商单位公章即可，未加盖供应商单位公章的视为未提供。提供的证明材料未按评分标准提供，且不能直接证明其有效性，需要通过供应商响应文件以外的其它途径佐证的，视为其证明材料无效。		

★四、商务要求

（一）服务期限及实施地点

1.服务期限：三年，合同一年一签，每年度服务期结束后，依据采购人对供应商的服务质量评估结果决定是否续签下一年度合同。第一年服务期至2025年3月31日；第二年服务期为2025年4月1日至2026年3月31日；第三年服务期为2026年4月1日至2027年3月31日。

2.服务地点：采购人指定地点。

（二）付款方式

合同签订后15至30个工作日内采购人向成交供应商支付50%的合同款，12月底前采购人向成交供应商支付剩余50%的合同款。

（三）履约保证金

不收取履约保证金。

（四）检查验收

按照国家及行业相关标准、采购文件要求、供应商响应文件承诺及合同约定进行验收。

（五）知识产权

成交供应商应保证向采购人提供的服务不会侵犯任何第三方的合法权益(如知识产权)，因成交供应商侵权行为产生的责任由成交供应商自行承担。采购人因此承担责任的，成交供应商应当赔偿。

（六）保密协议

成交供应商对在合作过程中接触到的采购人的任何资料、文件、数据（无论是否纸质文档）等一切载体所载明的信息，负有严格的保密义务。未经采购人书面同意，成交供应商不得以任何方式向任何第三方提供或透露，违反保密义务给采购人造成损失的，成交供应商应负责赔偿。

★五、技术要求

（一）运维内容

需驻场服务人员 1 名，按工作日以及重大活动日等特殊时间如两会期间、数博会期间等提供驻场服务，具体运维需完成提供 16 个系统的安全基线核查和加固服务、渗透测试服务、风险评估服务、网络分析与优化服务、符合性检查服务、安全策略管理服务、应急响应服务、应急演练服务、驻场运维服务、备品备件及非国产电脑终端漏洞扫描及加固等相关安全工作。

序号	安全服务名称	服务内容	数量	安全服务范围
1	漏洞扫描服务	每月对省工业和信息化厅局域网资产进行全面的漏洞扫描。对扫描的结果进行人工分析，排除扫描系统误报，出具漏洞分析报告；每月按需对高危风险持续复查、指定漏洞定向检测、持续对 0Day 漏洞进行检测/监控。资产范围：10 个服务器 IP、30 个网络设备、250 终端。（说明：态势感知是流量监测，分析流量日志，漏洞扫描是主动给业务系统扫描漏洞。(被动与主动)）。 服务周期：12 次/年，16 个系统。	1 项	涉及本地终端安全
2	安全基线核查和加固服务	每半年针对已建立安全基线的 IT 基础设施（包括操作系统等）开展安全基线配置核查，若存在极限配置发生变动，结合实际情况立即展开修复整改，完成后出具 IT 基础设施安全基线配置核查报告。资产范围：10 个服务器 IP、30 个网络设备、250 终端。 服务周期：12 次/年，16 个系统。	1 项	涉及本地终端安全
3	渗透测试服务	高级服务工程师在获得授权的情况下，以主流渗透工具结合深信服自研的工具模拟黑客攻击为主要手段，发现常见的高中危漏洞为主要目标，将发现的安全漏洞进行整理，给出详细说明，并针对每一安全漏洞提供相应的解决方法。并结合客户修复情况，协助客户	1 项	涉及本地终端安全

		针对修复后的漏洞进行复测验证。资产范围：16 个业务系统。 服务周期：16 个系统，1 次/年。		
4	风险评估服务	具体工作内容包括评估用户信息系统安全现状，对信息资产面临的威胁、存在的脆弱性、现有防护措施及综合作用而带来风险的发生可能性和对资产造成的影响进行评估，最终提供全面性的风险评估报告。风险评估以技术手段（漏扫、基线等）为基础，结合资产信息进行威胁关联分析，同时访谈业务人员了解安全现状，最终汇总数据分析并整合成风险评估报告。 服务周期：1 次/12 个月，16 个系统	1 项	涉及本地终端安全
5	网络分析与优化服务	每半年按照国家相关安全标准和架构安全性对现有网络架构和安全域其进行分析对比，若存在安全隐患则结合现有业务情况整改，完成后出具网络结构和安全域分析报告或架构整改报告。	2 次	涉及本地终端安全
6	安全策略管理服务	根据业务属性、业务风险与行业安全策略最佳实践相结合制定出最符合业务情况的安全策略，同时具备策略有效性检测机制。新增资产、业务变更时策略随业务变化而同步更新，并提供策略有效性调优服务。对所有网络安全和网络设备合规性检查，并进行整改。 服务周期：1 次/月，12 个月	12 次	涉及本地终端安全
7	应急演练服务	每年组织省工业和信息化厅各部门针对省工业和信息化厅局域网开展一次应急演练，模拟安全事件发生后的应急处置流程和工作方式，为真实应急做准备。完成后出具标准的应急演练报告。	1 次	涉及本地终端安全
8	驻场运维服务	采用安全专业的安全人员，通过加强对现场的安全的运维，为贵州省省工业和信息化厅提供日常驻场服务运维、重大节假日保障服务，确保省工业和信息化厅的网络安全。 驻场人员一：安全运维员 1.参与安全运维体系建立和实施，设计并推进安全运	12 人月	涉及本地终端安全

		维自动化； 2.保障部门安全运维安全，处理安全运维事故,优化各项维护工作流程，不断降低系统风险； 3.参与基础设施项目交付包括新的或改进的核心基础设施服务、网络、主机、安全等参与新 IT 基础设施的可行性研究。协助厅级软件的选择和 IT 咨询服务。		
9	备品备件	为现有局域网等保服务体系提供保障，UPS 系统作为省工业和信息化厅局域网等保二级建设需求评审项之一，因此需对 UPS 系统进行提升服务。提供备品备件服务，包含 UPS 备用电池服务及局域网接入交换机备用服务，当 UPS 电源间设备发生故障时，提供规格 12V、100AH 电池进行更换及光模块、千兆交换机 2 台故障时提供服务等。	1 项	涉及本地终端安全

（二）运维指标

提供 5×8 小时运维服务及 7×24 小时电话服务，响应时间不得超过半小时，如需现场处理 4 小时内到达现场；重大事项及活动期间需提供 24 小时保障服务。

（三）服务方式

采用远程+驻场服务方式。