贵州省财政信息化网络安全防护需求公示内容

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；

2.落实政府采购政策需满足的资格要求：/。

3.申请人的一般资格要求

符合政府采购法第二十二条规定，提供政府采购法实施条例第十七条规定资料。

（1）具有承担民事责任的能力。

具体要求：提供营业执照副本、组织机构代码证副本和税务登记证副本，或三证合一或五证合一的营业执照副本。（复印件加盖投标供应商公章）

（2）具有良好的商业信誉和健全的财务会计制度。

具体要求：供应商是法人的，应提供2023或2024年度经审计的财务报告，成立未满一年的提供基本开户银行出具的资信证明。部分其他组织和自然人，没有经审计的财务报告，提供银行出具的资信证明。（复印件加盖投标供应商公章）

（3）具有履行合同所必需的设备和专业技术能力。

具体要求：提供具备履行合同所必需的资金、设备和专业技术能力的承诺书。（按采购文件格式提供承诺）

（4）有依法缴纳税收和社会保障资金的良好记录。

具体要求：提供2024年4月至投标截止时间任意三个月依法缴纳税收和缴纳社会保障资金的有效证明材料，新成立不足三个月的企业可提供依法缴纳税收和社会保障资金的承诺函（成立时间以营业执照上的成立时间为准），依法免征、免缴、缓缴的提供相关证明材料。（复印件加盖投标供应商公章）

（5）参加本次政府采购活动前三年内，在经营活动中没有重大违法记录。

具体要求：提供参加政府采购活动前3年内在经营活动中没有重大违法记录的书面声明（按采购文件格式提供声明）。

（6）法律、行政法规规定的其他条件：

具体要求：①根据《财政部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）规定，对列入**失信被执行人、重大税收违法失信主体，政府采购严重违法失信**行为记录名单，及其他不符合《政府采购法》第二十二条规定条件的供应商，应当拒绝其参与政府采活动，响应文件作无效投标处理。**（按采购文件格式提供承诺）**

②根据《省发展改革委、省法院、省公共资源交易中心关于推进全省公共资源交易领域对法院失信被执行人实施信用联合惩戒的通知》（黔发改财金〔2020〕421号）要求，采购人或代理机构在递交响应文件截止时间后现场根据贵州信用联合惩戒平台反馈信息，查询供应商是否属于法院失信被执行人，如被列入取消其投标资格。

4.特殊资格要求

无。

技术要求：

一、采购内容概述

省级日常安全运维服务、安全巡检服务、省级安全检测和扫描服务、省级入侵渗透测试服务、省级攻防+应急演练服务、全省安全应急响应服务、全省网络安全培训服务、数据安全风险评估服务、软件供应链安全检查服务、全省实战攻防演习技术支持和地市安全风险评估等服务内容。主要体现在以下方面：

1、保障财政厅内、外网网站、信息系统和服务器平台的安全，不发生网站和系统被入侵、篡改、挂马等安全事件；

2、提高财政厅内、外网网站和系统安全防护能力，增强网络中已有的安全防护设备的防护效果，发挥设备最大功效；

3、要求开展省级安全检测和扫描服务、省级入侵渗透测试等服务，对已有信息系统进行安全评估，查找存在的安全隐患并采取措施加以防护；

4、要求开展驻场值守服务，进行实时信息系统监控，及时解决安全事件；实施应急演练服务，提高应急事故处理能力。

5、要求安排安全咨询专家为财政厅提供日常信息安全咨询服务；及时监控、收集行业内最新安全事件信息，提前进行同类事件安全通告，帮助财政厅及时了解最新安全动态并总结防护方案，对未知威胁事件进行预警预防。

6、要求开展全省网络安全培训服务，使财政厅安全技术人员能系统地掌握信息安全基础理论和技能；结合实际，安排针对性的专题讲座，增强实战经验。

7、要求开展开展数据安全风险评估服务，摸清数据资产底数，掌握的重要数据安全防护现状,识别数据生命周期面临的安全风险，规范指导数据安全管理、技术以及运行体系建设。

8、要求开展软件供应链安全检查服务，摸清软件供应链产品和企业底数，建立、健全软件供应链安全管理制度，全面排查供应链产品存在的安全隐患问题，完善供应链安全综合

技术防护体系。

9、要求开展全省实战攻防演习技术支持，主动发现和整改网络安全深层次问题隐患，切实提升整体网络安全防护能力、联防联控保障能力以及应急处置水平，有效应对各类高级网络安全威胁。

二、采购内容及技术服务要求

2.1.省级日常安全运维服务

2.1.1.风险评估服务

（1）服务内容

二线技术和5名驻场工程师针对贵州省财政厅信息化网络及业务系统每年开展一次风险评估服务，组织驻场安全技术人员、信息安全专家、顾问进行符合财政系统的风险评估方案设计。并规划风险评估实施方案，同时组织实施风险评估服务，发现风险与规避风险。

（2）服务要求

1次/年。

（3）交付成果

通过开展风险评估服务，输出用户认可的交付成果为《贵州省财政厅风险评估总结报告》。

2.1.2.驻场值守服务

（1）服务内容

提供驻场工程师5名，5×9小时提供负责开展省级日常安全运维服务：风险评估服务、驻场值守服务、安全加固服务、安全咨询服务、入网安评服务、全流量分析服务、源代码审计服务，以及省级安全服务：安全巡检服务、省级安全检测和扫描服务、省级入侵渗透测试服务、省级攻防+应急演练服务、全省安全应急响应服务、安全通告和预警服务、全省网络安全培训服务、数据安全风险评估服务、软件供应链安全检查服务、全省实战攻防演习技术支持服务。

提供设备运维工程师 1 名，针对省本级安全设备的运维和巡检、全省威胁态势感知平台，覆盖 9 个地州市和 2 个新区及 100 个区县 377 余台安全设备（详见：贵州省财政厅安全设备清单），完成相关联动安全设备日常维护与监控、网络信息安全策略优化、故障处理、软件补丁与更新、变更支持、网络巡检、工程协助等日常维护工作。按需提供运营日报、周报、月报、季报、年报等周期性运营监测报告，对整体网络安全态势进行分析与呈现，对特定目标遭受到网络攻击的态势进行分析与呈现。支持后端工程师对现有监测平台对接和定制开发。

（2）服务要求

供应商中标后须负责实现省厅态势监管平台与安全设备的协同联动，须熟练掌握省财政厅所有设备的操作、日常运维及设备调试等工作，在项目服务过程中，若拟派人员工作经验和工作能力未达到采购人服务质量要求，采购人按服务质量考评支付相应比例的合同金额或终止合同，供应商提供相应承诺函。

（3）交付成果

通过开展驻场值守服务，输出用户认可的交付成果为《贵州省财政厅驻场值守服务总结报告》和《贵州省财政厅驻场值守服务月度总结报告》。

2.1.3.安全加固服务

（1）服务内容

二线技术和 5 名驻场工程师、1 名设备运维工程师每年至少开展 4 次安全加固服务，针对安全评估、安全扫描等过程中发现的各种安全隐患，通过打补丁、安全配置增强、系统架构和安全策略调整等方式及时进行加固和安全优化，提高系统的安全性和抗攻击能力，以期将整个系统的安全状况维持在较高的水平，减少安全事件发生的可能性。

（2）服务要求

不少于 4 次/年，根据财政厅实际情况需求增加服务次数。

（3）交付成果

通过开展安全加固服务，输出用户认可的交付成果为《贵州省财政厅安全加固总结报告》和《贵州省财政厅安全加固季度总结报告》。

2.1.4.安全咨询服务

（1）服务内容

在合同期内，二线技术和 5 名驻场工程师、1 名设备运维工程师，为财政厅提供日常信息安全咨询服务，对财政厅业务系统运行环境进行安全监控、日常运行和审计检查的咨询支持。

（2）服务要求不少于 4 次/年，根据财政厅实际情况需求增加服务次数。

（3）交付成果

通过开展安全咨询服务，输出用户认可的交付成果为《贵州省财政厅安全咨询总结报告》。

2.1.5.入网安评服务

（1）服务内容

二线技术和 5 名驻场工程师、1 名设备运维工程师对新建或者发生重大调整的信息系统从整体结构安全、访问控制、主机安全、数据库系统安全、中间件系统安全、应用系统安全几个方面进行入网安全评估，确保信息系统操作系统、数据库、中间件、应用等各个层面信息安全状态可控。

（2）服务要求 1 次/年。

（3）交付成果

通过开展入网安评服务，输出用户认可的交付成果为《贵州省财政厅入网安评总结报告》。

2.1.6.全流量分析服务

（1）服务内容

全流量分析服务依据《信息安全技术网络安全等级保护基本要求》（GBT22239-2019）关于“应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络行为的攻击”安全监测分析要求，项目服务期间由二线技术和 5 名驻场工程师、1 名设备运维工程师利用财政厅网络内部已部署上线的全流量高级威胁监测设备和部署 9 个地州市高级威胁监测探针。为财政厅和 9 个地州市的业务系统和网络提供 5x8 的实时安全监控服务及每年 4 次

的集中分析服务，及时监测发现网络攻击行为和威胁，监测内容包括但不限于网络攻击、WEBSHELL 上传、弱口令、挖矿病毒等网络威胁，实时监测和发现信息网络基础设施的安全攻击及安全异常事件，发现网络攻击等异常事件时及时进行预警警示，并协助开展攻击事件处置。

（2）服务要求

及时开展。

（3）交付成果

通过开展全流量分析服务，输出用户认可的交付成果为《贵州省财政厅全流量分析总结报告》和《贵州省财政厅全流量分析季度总结报告》。

2.1.7.源代码审计服务

（1）服务内容

二线技术和 5 名驻场工程师每年开展 1 次，通过工具扫描+人工确认+人工抽取代码片段的白盒测试方式，检查源代码中的缺点和错误信息，分析并找到这些问题引发的安全漏洞，并提供代码修订措施和建议。

（2）服务要求

源代码审计服务每年至少 1 次/年。

（3）交付成果

通过开展源代码审计服务，输出用户认可的交付成果为《贵州省财政厅源代码审计总结报告》。

2.2.省级安全服务

2.2.1.安全巡检服务

（1）服务内容

二线技术和 5 名驻场工程师、1 名设备运维工程师每年对财政厅本部进行 4 次现场信息安全检查工作，动态更新拓扑图和资产信息，结合《省财政厅关于开展全省财政部门网络安全检查工作的通知》要求,包含但不限于防病毒管理、高危端口管理、基线管理、口令管理、漏洞管理、日志分析、特征库管理、违规外联、网络边界防护、准入管理等方

面，制定巡检方案。及时发现被检查单位的信息安全风险，提出信息安全改进建议，并对整个过程实行发现问题-协助加固-复查整改结果的一个良性循环的过程，实现整个过程的可追溯性，以此提高被检查单位的信息安全建设水平。

（2）服务要求

安全巡检服务每年至少 4 次/年。

（3）交付成果

通过开展安全巡检服务，输出用户认可的交付成果为《贵州省财政厅安全巡检总结报告》和《贵州省财政厅安全巡检季度总结报告》。

2.2.2.省级安全检测和扫描服务

（1）服务内容

二线技术和 5 名驻场工程师、1 名设备运维工程师每月为一个周期，在不影响财政专网系统稳定运行的前提条件下，通过远程的方式对财政厅专网服务器、网络设备、安全设备、终端使用专业的安全漏洞扫描检测软件对财政厅内进行漏洞扫描，以发现网络中和系统中存在的网络安全隐患，并出具扫描检测结果报告和修复方案，后续协助相关系统运维商对各自系统进行安全加固。

（2）服务要求 12 次/年。

（3）交付成果

通过开展省级安全检测和扫描服务，输出用户认可的交付成果为《贵州省财政厅省级安全检测和扫描服务总结报告》和《贵州省财政厅省级安全检测和扫描服务月度总结报告》。

2.2.3.省级入侵渗透测试服务

（1）服务内容

二线技术和 5 名驻场工程师针对省财政厅信息化网络和业务系统开展渗透测试，使用一系列现有安全产品和工具，结合人工智能，模拟当前流行的多种黑客入侵方法对财政厅内、外网各系统进行深度渗透测试，以发现信息系统应用的 WEB、主机、网络设备存在的漏洞，如 SQL 注入、跨站脚本、WEB 目录泄露、机密信息泄露、帐号弱口令、主机漏

洞、网络设备漏洞等；针对发现的漏洞提出整改方案，内容包括原因分析、测试方法、加固建议，并协助财政厅管理员进行安全整改。

（3）服务要求

4 次/年。

（3）交付成果

通过开展省级入侵渗透测试服务，输出用户认可的交付成果为《贵州省财政厅省级入侵渗透测试服务总结报告》和《贵州省财政厅省级入侵渗透测试服务季度总结报告》。

2.2.4.省级攻防+应急演练服务

（1）服务内容

二线技术和 5 名驻场工程师、1 名设备运维工程师针对省财政厅开展 1 次应急演练服务，组织安全技术人员、信息安全专家、顾问进行信息安全事件演练设计。并规划演练脚本，同时组织实施演练，对最新的安全事件进行预防演练，优化财政厅及各地州市财政局处置安全事件流程，提高应对安全事件能力。

（2）服务要求

每年1次。

（3）交付成果

通过开展省级攻防+应急演练服务，输出用户认可的交付成果为《贵州省财政厅应急演练实施方案》和《贵州省财政厅应急演练总结报告》。

2.2.5.省级安全应急响应服务

（1）服务内容

二线技术和 5 名驻场工程师、1 名设备运维工程师协同开展如下服务；

①**应急响应服务：**省厅出现安全应急事件或配合省厅协助地州市区县开展应急响应时，在发生安全应急事件之后，驻场工程师将提供非工作时间及非工作日内的紧急技术支持，确保在接到通知后的 30 分钟内到达现场，以迅速响应并妥善处理相关问题。及时处理、解决安全问题。在接到应急通知后，驻场安全服务工程师需能迅速完成基本分析判断，立即处理响应。遇重大安全问题时，向公司总部报告，加派安全专家做进一步的

响应处理和判断。安全事件处理完成之后，针对涉及系统的安全状况和可能再次受到的威胁，提供相应的事后安全分析和可行性安全建议，并进行事后安全加固帮助财政厅管理员解决存在的或者可能存在的安全问题。

②**配合迎检服务：**在网络信息安全检查、评估或审计过程中，为满足监管部门、上级部门要求或单位内部安全管理规定，驻场工程师提供的一系列辅助服务和应对措施，

包括但不限于：前期准备服务、安全状况自查、整改措施实施、技术支持和咨询、现场配合和总结分析与反馈；通过一系列服务服务和应对措施顺利通过安全检查，同时提升整体的网络安全防护水平，增强对网络安全事件的应对能力。

③**重大活动保障期间保障服务：**在重大节假日活动、国家重大活动或者会议期间提供7X24 小时专项安全值守服务，提供提供即时的技术支持和响应，同时对网络流量、

系统日志、安全事件等进行监控，及时发现并预警异常情况；在重大活动结束后，对保障工作进行总结，分析存在的不足和改进空间，为今后的保障工作提供经验教训。

（2）服务要求

据实，不限次数。

（3）交付成果

通过开展全省安全应急响应服务，输出用户认可的交付成果为《贵州省财政厅应急响应总结报告》,《贵州省财政厅重大节假日保障总结报告》,《贵州省财政厅配合迎检总结报告》。

2.2.6.安全通报和预警服务

（1）服务内容

二线技术和 5 名驻场工程师、1 名设备运维工程师针对网络与信息安全态势、关键漏洞通告、安全新闻或行业中发生的其他网络与信息安全事件，不定期面向贵州财政厅进行安全通报预警，确保相关单位能够在第一时间采取安全防御措施。

（2）服务要求据实，不限次数。

（3）交付成果

通过开展安全通报和预警服务，输出用户认可的交付成果为《贵州省财政厅安全通

报和预警服务总结报告》。

2.2.7.全省网络安全培训服务

（1）服务内容

二线技术和5名驻场工程师通过完善的IT核心技术培训体系更好的完善自身的运维处理能力及引导信息管理人员思考行业信息化建设的发展方向，保障重要的基础设施及信息系统的运行安全，开展针对财政系统的基础网络及信息安全培训，加强信息系统管理人才的培养，全面提升财政系统运维管理人员的技术水平；加强信息安全意识和防护能力，从技术手段和管理措施上加强财政信息系统运行维护管理，确保财政信息系统运行稳定可靠，加强数据资源安全的保护，确保财政资金运行安全。

（2）服务要求

1次/年，包含地市。

（3）交付成果

通过开展全省网络安全培训服务，输出用户认可的交付成果为《贵州省财政厅网络安全培训方案》,《贵州省财政厅网络安全培训PPT》,《贵州省财政网络安全培训服务总结报告》。

2.2.8.数据安全风险评估服务

（1）服务内容

依据依据国家法律法规以及财政行业相关要求，二线技术和5名驻场工程师、1名设备运维工程师开展数据安全风险评估，摸清数据资产底数，掌握的重要数据的种类、数量、收集、存储、加工、使用数据的现状,识别面临的数据安全风险，堵塞数据安全漏洞，进一步加强数据安全管理、技术以及运行体系建设。

（2）服务要求1次/年。

（3）交付成果

通过开展数据安全风险评估服务，输出用户认可的交付成果为《敏感数据资产台账》,《数据安全合规性评估报告》,《数据生命周期风险评估报告》。

2.2.9.软件供应链安全检查服务

（1）服务内容

二线技术和 5 名驻场工程师、1 名设备运维工程师协助财政厅梳理软件供应链产品和企业清单，掌握供应链底数，建立、健全软件供应链产品安全检查、开发安全流程管理、交付安全管理等管理制度要求，开展开源代码第三方组件安全检测等技术检查，全面排查供应链产品存在的安全隐患问题，形成供应链网络安全综合技术检测和防护体系。

（2）服务要求

软件供应链安全检查服务每年至少 1 次/年。

（3）交付成果

通过开展软件供应链安全检查服务，输出用户认可的交付成果为《供应链企业清单》,《供应链产品清单》,《系统开源组件漏洞检测报告》,《贵州省财政厅软件供应链安全检查总结报告》。

2.2.10.全省实战攻防演习技术支持服务

（1）服务内容

以习近平总书记网络强国重要思想为指引，以实战化、可视化、专业化为原则，二线技术和 5 名驻场工程师、1 名设备运维工程师开展实战化网络安全攻防演练，主动发现和整改网络安全深层次问题隐患，切实提升整体网络安全防护能力和应急处置水平，提高协同配合和联合处置能力，强化网络安全纵深防御、应急处置以及联防联控的保障体系建设，切实掌握工作主动权，有效应对网络安全威胁。

（2）服务要求 1 次/年。

（3）交付成果

通过开展全省实战攻防演习技术支持服务，输出用户认可的交付成果为《实战攻防演习总体工作方案》和《实战攻防演习总结报告》。

2.3.地市安全风险评估

1、风险评估服务

（1）服务内容

二线技术和 5 名驻场工程师针对地州市每年开展一次风险评估服务，组织驻场安全技术人员、信息安全专家、顾问进行符合财政系统的风险评估方案设计。并规划风险评估实施方案，同时组织开展风险评估服务，发现风险与规避风险。

（2）服务要求

风险评估服务每年至少 1 次/年。

（3）交付成果

通过开展风险评估服务，输出用户认可的交付成果为《地州市风险评估总结报告》。

2.4.贵州省财政厅安全设备清单

贵州省财政厅安全设备清单

供应商在用户单位授权的情况下，对用户单位 377 台网络安全设备进行使用和操作，协助用户单位管理。其中，奇安信品牌 IPS 设备 1 台，迪普品牌日志审计设备 1 台，奇安信品牌日志审计设备 1 台，亚信品牌日志审计设备 1 台，奇安信品牌堡垒机设备 1 台，迪普品牌防火墙设备 7 台，奇安信品牌防火墙设备 345 台，亚信品牌防火墙设备 6 台。

序号	设备名称	设备品牌	数量	数量汇总	备注
1	电子政务外网 IPS 入侵防御	奇安信	1	1	
2	UAG 网络行为管理	迪普	1	17	
3	运维安全管理与审计系统 V5.0	奇安信	1		
4	日志收集与分析系统 V5.0	奇安信	1		
5	安全审计系统 V5.0	奇安信	1		
6	新一代安全感知系统 V4.0	奇安信	3		
7	未知威胁发现设备	亚信	1		
8	流量探针	奇安信	9		
9	堡垒机发布服务器	奇安信	1	1	
10	服务器区安全网关	迪普	2	358	
11	应用防火墙	迪普	2		
12	外联 VPN	迪普	1		
13	边界防火墙	迪普	2		
14	电子政务外网防火墙(主)	奇安信	1		
15	电子政务外网防火墙（备）	奇安信	1		
16	防火墙系统 V4.0	奇安信	3		
17	安全接入网关系统 V5.0	奇安信	1		
18	亚信防病毒安全网关(服务器	亚信	2		

	区)				
19	亚信防病毒安全网关	亚信	4		
20	地州横向防火墙	奇安信	9		
21	地州上联防火墙	奇安信	18		
22	区县横向防火墙	奇安信	1		
23	区县上联防火墙	奇安信	208		
24	区县横向防火墙	奇安信	103		

商务要求：

一、服务期及服务地点

1.服务期：本次服务期原则上为3年，合同一年一签，采购人根据当年的情况评价确定是否续签，服务时间根据合同约定。

2.服务地点：采购人指定地点。

二、验收标准和方式

按国家及行业相关规定、采购文件、响应文件、采购合同及双方认可的其它约定执行。

三、付款方式

按合同约定执行。

四、履约保证金

合同金额的10%。

五、投标有效期

90日历天。

六、服务质量考评

年度服务结束，根据服务质量考核表进行评分，得分100-90分，付合同金额的100%；得分89-80分，扣除30%；得分79-60分，扣除50%；低于60分不付款。

服务质量考核表

考核指标	默认分值	评分标准	评分
交付物质量	10	按照《项目运维服务管理规范》和合同各项运维要求，完成各个阶段文档交付工作，且文档被甲方及最终用户认可。 1．交付物提交不及时，每次扣1分。 2．交付物质量不合格，每次扣2分。 3．每缺失一个阶段的文档交付物，每次扣5分。 4．交付物提交不及时，并且质量不合格，且发生两次及以上，每次扣10分。	
日常巡检	5	每日对系统的主要应用功能进行例行晨检，每周对系统应用程序、操作系统、数据库、中间件、硬件设备等进行巡检，根据安全要求及时更新补丁和修复漏洞，定期开展数据备份。 1．未按上述要求开展相关工作的，每出现一次扣1分。 2．因未进行日常检查，或因检查不彻底、发现隐患不及时，最终导致系统出现故障的情况，每出现一次扣5分。	
运维服务	30	运维服务要符合《项目运维服务管理规范》和合同各项运维要求，提供的运维服务需要获得甲方及最终用户的认可。	

		1．未按照《项目运维服务管理规范》和合同各项运维要求开展工作，导致不良影响的，每次扣 2 分；造成严重后果的，每次扣 10 分。造成特别严重后果的，每次扣 20 分。 2．运维服务过程中，受到甲方及最终用户的投诉电话，每次扣 20 分。 3．乙方单位在运维服务过程中受到甲方及最终用户的书面表扬的，每次加 10 分。	
应急响应和故障处置	20	要符合《项目运维服务管理规范》和合同各项运维要求，对系统和服务出现的紧急情况及时响应并妥善处理，处理情况及时反馈甲方及最终用户。 1．出现紧急情况，在 10 分钟内未响应，每次扣 1 分；在 30 分钟内未响应，每次扣 5 分；1 小时内未响应，每次扣 10 分；1 小时以上未响应，每次扣 20 分。 2．因乙方单位原因，造成系统（或关键功能）大范围中断、系统访问缓慢（响应时间在 30 秒以上），大量用户无法正常开展工作的情况，故障时间在 10 分钟以内，每次扣 5 分；30 分钟以内，每次扣 10 分；1 小时以内，每次扣 20 分，每增加 1 小时加扣 10 分。 3．日常故障处理之前，没有征得甲方及最终用户的同意，私自进行运维操作的，每次扣 20 分。 4．针对与乙方服务范围内无关的突发情况，乙方及时配合甲方及最终用户，起到决定性的作用并妥善处理，使甲方及最终用户的损失降到最小，每次加 10 分。	
重大活动及节假日保障工作	20	重大活动及节假日保障工作是指在重大活动或者特殊时期进行运维和安全保障，无任何安全事件发生。 1．因保障力度不够，没有造成安全事件发生，但是产生不良影响的，每次扣 10 分； 2．因保障力度不够，造成安全事件发生的，每次扣 20 分。	
沟通、协调	5	与本单位运维团队紧密衔接工作，并能与甲方及最终用户、其他项目运维单位保持良好沟通和协作。 1．不能有序、有效开展上述协作的，影响项目进展情况的，每次扣 1 分。 2．沟通协调过程中态度恶劣，没有责任心的，每次扣 2 分。 3．沟通协调过程中出现谩骂、不尊重人的，每次扣 5 分。	
工作态度	5	根据甲方及最终用户的要求完成项目范围内交办的有关工作。 1．能够完成交办的工作，但完成的及时性、准确性方面存在不足，每次扣 1 分。 2．针对甲方及最终用户交办工作，30 分钟内没有积极响应的，每次扣 2 分。 3．不接受、不配合交办的工作，每次扣 5 分。	

工作评价	5	对项目范围内的各项工作开展情况随机进行 2~3 次的评价，由甲方及最终用户评价。 1．评价为一般，每次扣 1 分。 2．评价为不满意，每次扣 2 分。 3．评价为极度不满意，每次扣 5 分。	
合计			

七、其他要求

1. 供应商中标后须负责实现省厅态势监管平台与安全设备的协同联动，须熟练掌握省财政厅所有设备的操作、日常运维及设备调试等工作，在项目实施过程中，若拟派人员工作经验和工作能力未达到采购人服务质量要求，采购人按服务质量考评支付相应比例的合同金额或终止合同（供应商提供相应承诺函，承诺格式自拟，并加盖工作）。

2. 供应商承技术负责人及时提供服务，在接到用户单位需求支撑需求时，确保在 60 分钟内赶到客户现场进行及时的支撑响应（承诺格式自拟，并加盖公章）。

3. 供应商承诺拟派驻场工程师未经采购人同意，不得私自更换（承诺格式自拟，并加盖公章）。

4. 供应商承诺根据用户单位的具体需求，在接到用户单位需要支撑响应时，迅速安排服务人员，确保在 30 分钟内赶到客户现场进行及时的支撑响应（承诺格式自拟，并加盖公章）

5.供应商承诺：若中标，将积极与上一年度（或下一年度）的服务商做好衔接工作。（承诺格式自拟，并加盖公章）

评标办法：

一、评标办法前附表

1.项目基本信息

项目序列号：_____

项目名称：贵州省财政信息化网络安全防护项目

采购方式：公开招标

项目资金来源：财政资金

PPP 项目：否

2.标包信息

标包编码：_____

标包名称：贵州省财政信息化网络安全防护项目

评标办法：**综合评分法**

是否考虑小微型企业价格扣除：是

是否考虑政策性加分：否

资格审查方式：资格后审

是否接受联合体：否

是否缴纳投标保证金：是

中标方法：推荐中标候选人

核心产品名称：/

报价评审：有

预算金额(元)：3357600.00

1.评标分值组成

序号	评审步骤	是否报价评审	分值（分）
1	资格性审查	否	/
2	符合性审查	否	/
3	商务评审	否	63
4	技术评审	否	27
5	政策性加分评审	否	/
6	报价评审	是	10

2.前附表

2.1 资格性审查

序号	评审因素	评审标准
1	具有承担民事责任的能力	提供营业执照副本、组织机构代码证副本和税务登记证副本，或三证合一或五证合一的营业执照副本（复印件加盖投标供应商公章）。
2	具有良好的商业信誉和健全的财务会计制度	具体要求：供应商是法人的，应提供 2023 或 2024 年度经审计的财务报告，成立未满一年的提供基本开户银行出具的资信证明。部分其他组织和自然人，没有经审计的财务报告，提供银行出具的资信证明（复印件加盖投标供应商公章）。
3	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资金、设备和专业技术能力的承诺书（按采购文件格式提供承诺）。
4	有依法缴纳税收和社会保障资金的良好记录	提供 2024 年 4 月至投标截止时间任意三个月依法缴纳税收和缴纳社会保障资金的有效证明材料，新成立不足三个月的企业可提供依法缴纳税收和社会保障资金的承诺函（成立时间以营业执照上的成立时间为准），依法免征、免缴、缓缴的提供相关证明材料（复印件加盖投标供应商公章）。
5	参加本次政府采购活动前三年内，在经营活动中没有重大违法记录	提供参加政府采购活动前 3 年内在经营活动中没有重大违法记录的书面声明（按采购文件格式提供声明）。
6	参加本次政府采购活动前三年内，在经营活动中没有数据和网络安全重大违法记录	提供参加政府采购活动前 3 年内在经营活动中没有数据和网络安全重大违法记录的书面声明（按采购文件格式提供声明）。

7	法律、行政法规规定的其他条件	（1）根据《财政部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）规定，对列入失信被执行人、重大税收违法失信主体，政府采购严重违法失信行为记录名单，及其他不符合《政府采购法》第二十二条规定条件的供应商，应当拒绝其参与政府采购活动，响应文件作无效投标处理（按采购文件格式提供承诺）。 （2）根据《省发展改革委、省法院、省公共资源交易中心关于推进全省公共资源交易领域对法院失信被执行人实施信用联合惩戒的通知》（黔发改财金〔2020〕421号）要求，采购人或代理机构在递交响应文件截止时间后现场根据贵州信用联合惩戒平台反馈信息，查询供应商是否属于法院失信被执行人，如被列入取消其投标资格**（此项由交易中心报名系统自动对失信投标供应商实施信用联合惩戒）。**
8	联合体投标	本项目**不接受**联合体投标

2.2 符合性性审查

序号	评审因素	评审标准
1	商务符合性	符合采购文件第五章第二节 商务要求
2	无效标审查	按本项目采购文件供应商须知正文 5.5 无效标条款规定，审查是否通过。

2.3 商务评审

序号	评审因素	评审标准	分值
1	企业实力	1、投标供应商具有有效的隐私信息管理体系认证、质量管理体系认证、供应链安全管理体系认证、信息安全管理体系认证、信息技术服务管理体系认证，提供证书齐全的得 10 分，每缺一项扣 2 分。本项最高得 10 分，最低得 0 分。 2、投标供应商具有有效的信息系统建设和服务能力评估证书，证书为 CS2 级或 CS3 级的得 1 分，证书为 CS4 级及以上的得 2 分。本项最高得 2 分，最低得 0 分。 3、投标供应商具有中国软件评测中心颁发的数据安全服务能力评定资格证书-数据安全建设，证书为一级的得 1.5 分，证书为二级的得 3 分。本项最高得 3 分，最低得 0 分。 **注：须提供相关证书复印件（加盖公章），未提供或提供证书资料不符的不得分。**	15
2	项目负责人	**项目负责人 1 名：** （1）具有人社部门颁发的信息系统项目管理师、中国信息安全测评中心颁发的注册信息安全专业人员（CISP-CISE）证书的得 3 分，每缺一项扣 1.5 分。本项最高得 3 分，最低得 0 分。 （2）具有国家互联网应急中心（CNCERT）的原创漏洞证明的得 2 分。 **注：须按要求提供项目负责人的身份证、相关证件资料及投标供应商为其缴纳养老保险（2025 年 1 月至投标截止时间任意三个月）证明材料的复印件（加盖公章）。未提供或提供资料不符的不得分。**	5
3	技术负责人	**技术负责人 1 名：** 具有中国信息安全测评中心颁发的注册信息安全专业人员（CISP-CISE）认证、中国网络安全审查技术与认证中心颁发的数据安全官证书、人社部门颁发的信息安全工程师的得 3 分，每缺一项扣 1 分，本项最高得 3 分，最低得 0 分。 **注：须按要求提供技术负责人的身份证、相关证书及投标供应商为其缴纳养老保险（2025 年 1 月至投标截止时间任意三个月）证明材料的复印件（加盖公章）。未提供或提供资料不符的不得分。**	3 分
4	驻场服务工程师	**驻场服务工程师（项目负责人和技术负责人除外）：** 每有 1 人具有中国信息安全测评中心颁发的注册信息安全专业人员（CISP）认证或人社部门颁发的信息安全工程师的得 1 分，最多得 6 分。 **注：①同一人不重复计分，同时具有多项证书的按得分高的计分；②须按要求提供以上人员的身份证、相关证书及投标供应商为其缴纳养老保险（2025 年 1 月至投标截止时间任意三个月）证明材料的复印件(加盖公章)。未提供或提供资料不符的不得分。**	6

5	**企业业绩**	投标供应商近 3 年（2022 年 1 月 1 日至投标截止时间），每承担过 1 个安全服务项目（服务内容包含但不限于：安全评估、安全漏洞扫描、安全应急、安全加固）业绩得 3 分，最多得 12 分。 **注：须提供中标通知书和合同（至少包括合同首页、服务内容页、双方签字盖章页），未提供或提供资料不符的不得分。**	12
6	**安全漏洞技术能力**	为体现产品制造厂商的安全漏洞技术能力，所投安全产品的生产厂商具有国家信息安全漏洞库（CNNVD）颁发（2022 年或 2023 年或 2024 年度）的“高质量通报优秀贡献奖”、“高质量漏洞优秀贡献奖”的得 2 分，每缺一项扣 1 分。本项最高得 2 分，最低得 0 分。 **注：须提供相关证书复印件（加盖公章），未提供或提供证书资料不符的不得分。**	2
7	**服务工具**	1、投标供应商提供的漏洞扫描工具，具有计算机软件著作权的得 2 分。 2、投标供应商提供的源代码审计工具，具有计算机软件著作权的得 2 分。 3、投标供应商提供的自动渗透工具，具有计算机软件著作权的得 2 分。 4、投标供应商提供的数据安全评估工具，具有计算机软件著作权的得 2 分。 **注：须提供计算机软件著作权登记证书和相关功能截图，复印件（加盖公章），未提供或提供证书资料不符的不得分。**	8
8	**技术支撑服务保障**	为确保项目服务质量，投标供应商须提供：采购人在网运行主要安全设备的制造商，针对本项目的《技术支撑承诺函》，承诺在必要时协助投标供应商操作相应安全系统，加盖制造商公章。本采购文件相关章节已描述采购人在网运行主要安全设备的类型与制造商，投标商提供所有品牌制造商《技术支撑承诺函》的得 12 分，每缺少一家制造商的《技术支撑承诺函》扣 4 分。本项最高 12 分，最低得 0 分。 **注：须提供加盖制造商公章的《技术支撑承诺函》，格式自拟。未提供承诺或承诺内容不符的不得分。**	12

2.4 技术评审

序号	评审因素	评审标准	分值
1	**技术响应**	根据响应文件对采购文件第五章第一节 采购内容及技术服务要求的响应情况进行评分，全部满足的得 12 分，有任意一项负偏离的扣 2 分，当负偏离达到 6 项及以上的，本项得 0 分。 **注：**以投标供应商技术实质性响应表作为评审依据。	0-12 分
2	**服务方案**	**整体服务方案：** 供应商针对项目实际情况提供的整体服务方案，内容包括但不限于日常问题处理、安全保障、应急处理、培训服务、质量保证措施、服务期承诺、售后服务方案： （1）方案内容完整且合理，可行性、针对性强，得 10 分； （2）方案内容较合理，可行性、针对性较强，得 7 分； （3）方案内容一般，可行性、针对性一般，得 4 分； （4）方案内容较一般，可行性、针对性弱，得 1 分； （5）未提供的不得分。	0-10 分
		重点保障服务方案： 供应商针对项目实际情况提供的重点保障服务方案，包括但不限于保障计划、人员配置、安全服务保障、应急响应措施、保密措施： （1）方案内容完整且合理，充分考虑用户需求，合理配置人员，提出的安全保障措施、应急响应措施和保密措施可行性、针对性强，且符合相关法律法律规要求，得 5 分。 （2）方案内容基本完整，基本满足用户需求，配置人员较合理，提出的安全保障措施、应急响应措施和保密措施存在某些细节或者某些方面的不足，得 3 分。 （3）方案内容不完整，存在明显不足，与用户需求严重不符，提出的安全保障措施、应急响应措施和保密措施可行性、针对性存在较大问题，实施难度大或者风险高，得 1 分。 (4)未提供的不得分。	0-5 分

2.5 政策性加分评审

序号	评审因素	评审标准	分值
/	/	/	/

注：本项目为服务类采购项目，政策性加分不适用。

2.6 报价评审

序号	评审因素	评审标准	分值
1	**报价得分**	价格分采用低价优先法计算，即满足采购文件要求的前提下，最低有效投标报价作为评标基准价，其价格为满分，其余有效供应商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** **注：**若投标人有符合政府采购优惠政策价格扣除的，评审的投标报价为扣除后的报价，但实际中标和合同价仍然为未扣除的报价。	10

注：最终以实际发布的采购公告及采购文件内容为准。