第3章招标项目技术、服务、商务及其他要求

（注：带“★”的参数需求为实质性要求，供应商必须响应并满足的参数需求，采购人、采购代理机构应当根据项目实际需求合理设定，并明确具体要求。带“▲”号条款为允许负偏离的参数需求，若未响应或者不满足，将在综合评审中予以扣分处理。）

3.1采购项目概况

金财工程是关系国计民生的重要关键信息基础设施，财政核心业务信息系统具有“准金融”的特性，财政信息资产的高价值、高关注度和数据高度集中化也吸引了大量网络黑产和敌对势力的目光，资金窃取、票据篡改、信息泄露等网络安全事件在财政系统时有发生，对财政系统资金安全、数据安全和业务安全提出了严峻挑战。习近平指出：网络安全和信息化是一体之两翼、驱动之双轮，必须统一谋划、统一部署、统一推进、统一实施。党和国家高度重视网络安全工作，《中华人民共和国网络安全法》、《党委（党组）网络安全责任制实施办法》等重要网络安全法律法规相继出台，财政部印发相关文件，全面规定了关键信息基础设施运营主体的法律义务和责任，对新形势下强化财政网络安全工作提出了具体要求。 目前财政厅共有 40 余个业务应用系统，分别部署在四川省财政厅机房和四川省政务云平台，共有70余台物理服务器和 780 余台虚拟服务器，财政业务应用较多，网络安全保障压力较大，经过2021-2022年度四川省财政厅整体网络安全建设优化，四川省财政厅已初步构建适应全省财政系统数字化发展的网络安全整体保障体系，四川省财政信息中心将持续深化网络安全技术与服务运营体系的建设，强化网络安全运维力量，做实做细网络安全防护工作，提高突发事件应对能力。通过常态化开展网络安全日常运维、专项保障等网络安全服务、网络安全培训及安全宣传周服务工作，提高网络安全整体安全保障水平。

3.2服务内容及服务要求

3.2.1服务内容

采购包1：

采购包预算金额（元）：1,896,000.00

采购包最高限价（元）：1,896,000.00

序号	标的名称	数量	标的预算（元）	计量单位	所属行业	是否核心产品	是否允许进口产品	是否属于节能产品	是否属于环境标志产品
1	运行维护服务	1.00	1,896,000.00	项	软件和信息技术服务业	否	否	否	否

3.2.2服务要求

采购包1：

标的名称：运行维护服务

参数性质	序号	技术参数与性能指标
★	1	# 项目要求 ## 背景介绍 金财工程是关系国计民生的重要关键信息基础设施，财政核心业务信息系统具有“准金融”的特性，财政信息资产的高价值、高关注度和数据高度集中化也吸引了大量网络黑产和敌对势力的目光，资金窃取、票据篡改、信息泄露等网络安全事件在财政系统时有发生，对财政系统资金安全、数据安全和业务安全提出了严峻挑战。习近平指出：网络安全和信息化是一体之两翼、驱动之双轮，必须统一谋划、统一部署、统一推进、统一实施。党和国家高度重视网络安全工作，《中华人民共和国网络安全法》、《党委（党组）网络安全责任制实施办法》等重要网络安全法律法规相继出台，财政部印发相关文件，全面规定了关键信息基础设施运营主体的法律义务和责任，对新形势下强化财政网络安全工作提出了具体要求。 目前财政厅共有 40 余个业务应用系统，分别部署在四川省财政厅机房和四川省政务云平台，共有70余台物理服务器和 780 余台虚拟服务器，财政业务应用较多，网络安全保障压力较大，经过2021-2022年度四川省财政厅整体网络安全建设优化，四川省财政厅已初步构建适应全省财政系统数字化发展的网络安全整体保障体系，四川省财政信息中心将持续深化网络安全技术与服务运营体系的建设，强化网络安全运维力量，做实做细网络安全防护工作，提高突发事件应对能力。通过常态化开展网络安全日常运维、专项保障等网络安全服务、网络安全培训及安全宣传周服务工作，提高网络安全整体安全保障水平。 **服务目标** 落实网络安全法、密码法、等级保护 2.0 相关要求，加强网络安全监测防护能力，强化网络安全服务力量，做细做实网络安全防

护工作，通过开展常态化安全运维服务，同时加强运维服务支撑能力，提高财政厅网络安全整体保障水平。达到全面等保合规、无重大安全事件、无重大安全隐患的目标要求，形成全面覆盖、持续不断、动态更新的安全服务保障体系。

服务内容

本次服务内容包括：安全咨询服务（安全建设咨询、安全管理咨询、商用密码咨询、安全加固咨询）、安全保障服务（安全检测保障服务、应急响应保障服务、专项保障服务、日常安全运维保障服务）、网络安全培训及安全宣传周服务。

安全咨询服务

安全建设咨询

目前四川省财政厅已具备基础网络架构安全，满足稳定运行、安全可控的防护要求，后期按照业务实际需求可能会涉及局部架构微调，需按照后期实际需求，结合数据安全、零信任等新技术进行安全规划指导，使得整体网络安全建设符合安全防护水平的趋势发展，做到信息化建设和网络安全建设“三同步”。

安全管理咨询

根据最新国家相关要求及行业相关管理规定，结合财政厅信息安全管理实际情况，针对财政厅安全管理制度提供调整建议，促进各项安全管理制度的优化完善，推动安全管理制度的有效执行。

配合及时更新信息安全管理及操作规范的编制，使之符合财政厅信息安全管理运维实际情况，以指导规范信息安全工作中的主要业务活动，包括但不限于安全基线规范、各项安全管理活动规程、信息安全技术操作规范等,指导市县财政部门优化完善安全管理制度。

商用密码咨询

财政厅关键信息系统涉及到财政收入、财政支付等敏感数据，需要使用商用密码提供电子认证、密钥管理、密码运算等服务，按照

《密码法》《信息安全等级保护商用密码管理办法》等法律法规要求，须对采用商用密码技术、产品和服务集成建设的网络和信息系统密码应用的合规性、正确性、有效性进行评估。针对财政厅商密应用，需要提供系统密码应用建设/改造规划咨询服务，包括信息系统建设初期密码应用设计咨询，密码技术/密码产品/密码服务相关咨询。

安全加固咨询

为保障财政业务的安全运行，防止系统“带病上线、带伤运行”，加快落实安全整改措施，需根据安全基线核查、系统漏洞扫描以及渗透测试等检测评估结果，针对所发现的安全漏洞、安全风险，提出可操作性强、效果佳的整改计划，及时指导各信息系统运维公司开展风险治理、安全加固工作，并逐一核查整改完成情况。包括但不限于硬件服务器、云主机、应用系统、数据库、中间件、网络设备、安全设备等的漏洞修复建议、配置整改建议等。同时，应针对各类通报的或发现的安全风险及漏洞进行评估，及时提出应对措施建议并协助落实，以及落实情况的逐一核查。

安全保障服务

安全检测保障服务

安全基线核查

不安全配置是黑客攻击中容易被利用的弱点盲区，需要按照财政厅基线检测机制，对财政厅相关系统和设备等进行全面的安全配置核查和分析，发现配置的不合规项，并结合财政实际需求提出系统整改建议，输出《信息系统基线整改记录单》，基线检测的频率不低于每月 1 次。每次基线核查资产数量约为500台主机（操作系统以实际为准，包括但不限于Linux、Windows、中标麒麟等），核查范围为财政厅管理的信息系统。

通过对现有信息系统基线配置进行扫描监测，及时发现网络安全设备、服务器、中间件、数据库等资产的不安全配置，降低由于配置

不当导致安全事件的几率，根据已修订基线版本对各对象目标进行持续监测。

系统漏洞扫描

漏洞攻击是网络安全攻防实战中最直接有效的手段，开展常态化漏洞扫描服务，定期发现财政厅设备和系统中存在的安全漏洞，并通过及时修补完善，避免对信息系统造成严重影响。建立全年的风险及漏洞检测机制，漏洞扫描频率不低于每月 1 次，针对评估结果中的高危漏洞整改时间不能大于 1 周，中危漏洞整改时间不能大于 3 天，每次系统漏洞扫描资产包括财政厅管理的系统。

通过对业务应用系统开展主机、中间件、数据库等脆弱性扫描，及时发现安全漏洞，制定安全加固建议，作为安全加固工作输入；通过对新应用系统进行上线前漏洞扫描工作，提前发现系统安全漏洞，输出《信息系统漏洞整改记录单》，提交至信息中心，信息中心通知系统相关人员进行实施整改，安全服务团队提供技术指导。

渗透测试

为充分了解财政业务当前存在的安全隐患，验证漏洞修复情况、安全策略有效性以及安全配置合理性，需要开展常态化渗透测试服务，重点检测核心及重要业务应用的风险情况。通过安全服务人员模拟真正的黑客入侵攻击方法，对财政厅业务系统进行渗透测试，最大程度挖掘财政厅业务系统潜在的安全威胁（包括系统存在的漏洞、脆弱点、网站的不安全因素等），并将最终结果以专业安全测评报告的形式呈现，渗透完成后对发现的问题和风险进行修复，每年护网行动之前，需加强人员配置，针对财政重要业务完成护网前的集中覆盖测试，找出风险点，提出整改建议并指导完成。按需开展渗透测试服务，每年度开展不低于10次渗透测试服务（含复测），每次渗透测试对象不低于1个系统，财政厅提供渗透测试纸质版授权后，开展渗透测试服务，渗透测试完成后输出渗透测试报告、复测报告。

APP安全测试

为保证财政厅移动业务应用建设的安全开展，需要对财政厅业务应用 APP 进行安全分析测试，保证整个安全测试过程都在可以控制和调整的范围之内，全面发现财政厅 Android、IOS、微信应用等程序可能存在的安全缺陷，并提供安全测试报告和改进建议，最大程度保障财政移动应用的程序安全，每年测试业务APP不少于1个。

代码审计

为了消除代码中的漏洞、减少不必要的补丁升级，从根源上解决源代码导致的安全问题，需要对财政业务核心系统及新上线重要系统的源代码和程序进行白盒+黑盒测试。

通过实施代码安全审计服务，快速发现项目中的代码安全漏洞、快速评估系统代码安全风险、增强系统安全性，抵御黑客恶意攻击，最大程度保护财政厅信息系统资产。

应急预案演练

为应对财政厅信息系统遇到突发的安全问题如：发生网络入侵事件、大规模病毒爆发、遭受拒绝服务攻击等，无法及时对该事件进行处理或解决的情况，需要提前针对安全事件进行分级分类，在此基础上，梳理应急场景，完善调整攻击应急响应流程，形成财政厅完善、可落地的网络安全应急预案和应急处置操作手册，建立应急响应组织机构及沟通渠道，并指导市（州）财政部门建立完善应急预案，当不同安全事件发生时以便进行针对性的快速应对处置。并保证每年开展不少于一次的厅本级安全应急演练工作，检验应急预案的时效性，并根据应急演练结果实时调整优化应急预案。

全省网络安全风险评估及问题整改服务

从制度执行、运维安全、数据安全、终端安全、通信安全、日志审计和机房安全8个方面，共计85项内容，服务频次每年不超过80人天，具体情况按照财政厅现场实际需求再进行调整。

每季度对财政厅开展1次网络安全风险评估及问题整改，每次不少于2个系统，每季度工作时间不少于5个工作日，投入人员不少于2

人，提供《风险评估报告》，具体情况按照财政厅现场实际需求再进行调整。

根据工作实际情况，按财政厅安排，对至少6个市县财政部门开展不少于1次的网络安全风险评估及问题整改，提供《风险评估报告》，具体情况按照财政厅现场实际需求再进行调整。

风险评估服务实施方法至少包括：现场访谈、漏洞扫描、人工审计、基线配置核查等。

应急响应保障服务

驻场人员按照财政厅实际需求，按需提供应急保障支持，对驻场人员无法迅速解决的网络入侵、拒绝服务攻击、大规模病毒爆发、主机或网络异常事件等紧急安全问题，需协调后场专家（非驻场）提供技术支持，必要时1.5小时内需到达现场进行处理，控制事态发展，保护或恢复财政厅主机、网络服务的正常工作，事件处置要求如下：特别重大事件，5分钟响应及报告，30分钟完成前期处置，每隔30分钟通报一次直至事件结束；重大事件，10分钟响应及报告，30分钟完成前期处置，每隔60分钟通报一次直至事件结束；较大事件，20分钟响应及报告，60分钟完成前期处置，每隔120分钟通报一次直至修事件结束；一般事件，20分钟响应及报告，60分钟完成前期处置，每隔120分钟通报一次直至事件结束。事件结束后提供事后分析，找出系统的安全漏洞，根据现场保留情况尽可能对入侵者进行追查，应急保障结束后，提供应急响应总结报告。

专项保障服务

攻防演练防守服务

根据财政厅安排，做好财政部、公安部门、网信部门等主管部门组织的攻防演练防守服务和省级单位组织的攻防预演练防守服务，提供安全技术专家做好防护保障，服务频次不超过每年200人天。

1)每次参与攻防演练（24小时值守）不少于5人，其中2人为驻场团队外攻防演练专家负责进行综合研判和溯源工作，具体天数按攻

防演练组织单位的要求确定，财政厅可根据现场实际需求再进行调整；

2)协助财政厅制定防守方案，包括组织架构、人员调配、资产梳理、工具支持、监测预警、响应处置等。

3)及时提供国内外安全威胁情报，并协助财政厅开展前期的资产梳理、风险排查及系统加固。

对攻防演练结果进行总结，包括但不限于防守监测、响应及时性、处置过程协调性、应急响应有效性、追踪定位准确性等网络安全监测预警、研判处置能力，提供《网络攻防演练复盘报告》。

重大活动保障服务

对于全年各重点时期如：元旦、春节、两会、建党节、国庆及其他特殊时期等重要时期开展重点安全保障服务，加强重要时期的安全服务人员数量与人员专业度保障，重点监控各类安全攻击/事件的发生，尤其是财政厅政务云互联网区业务系统、金财专网核心业务系统等，做好攻击监控、响应、处置、溯源分析、记录和事件提交等相关工作，并提供安全事故应急响应技术保障。

在任一系统、任一安全隐患发生时，及时启动相应的应急预案，并在每次重点保障时期统筹各技术支持单位进行安全保障工作开展，完成安全保障工作后整合各技术支持单位重点时期的安全保障报告，针对性的提供后续安全防护整改建议。若进行全天24小时保障，每次值班人数不少于2人。

网站安全监测保障服务

通过专用网站安全监测平台对财政厅互联网信息系统网站（目前有12个）URL进行7*24小时不间断监测，结合安全专家的专业分析，及时发现网站存在的安全隐患和问题，包括：远程网站漏洞扫描服务；网站可用性监测服务；页面篡改监测服务；网站域名解析监测服务；敏感内容监测服务；网站挂马监测服务；钓鱼网站监测服务;网站黑链监测服务。每周提交监测报告。

日常安全运维保障服务

资产梳理更新

通过定期核实和梳理财政厅的 IT 资产（如 IP 地址，对应的端口及服务、操作系统、数据库、中间件、第三方插件等），特别是政务云互联网区暴露 IT 资产的核实和梳理，持续完善财政厅信息系统资产台账清册，关联资产风险情况，并进行动态维护实时更新，每月定期更新输出财政厅资产总表。

日常监测分析

通过对财政厅各类安全产品的持续日志分析、告警监控，结合漏洞检测情况，基于人工分析研判，排查梳理安全威胁线索，实时监测财政网络安全情况，依据网络扫描、木马蠕虫、WEB 攻击、暴力破解等攻击场景，基于源/目的 IP、源/目的端口、协议类型、事件类型、事件发生频率、用户名、事件优先级、事件可信度等进行关联分析，形成监测分析、通报预警机制，编制网络安全月报。

对安全威胁的追踪、采集、分析、研判的处理机制做进一步的改进与优化。

设备安全运维

财政厅本地机房设备安全运维，包括设备巡检，设备部署优化，设备策略优化，配置防护，升级维护。

目前设备：堡垒机、TDA、防毒墙、防火墙、日志审计、EDR、数据库审计、WAF、漏洞扫描、态势感知、IPS、IDS、蜜罐、DDOS、全流量监测、威胁感知系统，总计70余台。

设备巡检：为保障业务应用正常运行，需要开展日常巡检工作，及时发现隐患、减少故障，包括对网络、主机、安全设备的 CPU、内存、硬盘、日志空间容量进行检查，同时对网络日志、系统日志等进行收集、整理、归纳、分析相关情况，每月输出安全运行维护报告。

部署优化：根据财政实际业务应用需求及网络安全防护薄弱点，对安全设备进行部署方式及部署位置提出优化建议，保障网络安全防护设备发挥最大作用。

策略优化：根据现场业务应用需求以及日常安全设备防护效果监测分析结果，对安全设备进行策略优化设计（包括交叉策略、冗余策略、冲突策略、过期策略等），保证网络安全防护设备高可靠、高效率运行。输出安全策略调整记录表单。

配置防护：设备配置管理是各类安全设备及系统日常维护必不可少的环节。通过建立配置维护流程，记录设备配置策略，跟踪配置变更操作情况，以及备份设备配置文件等工作，确保设备维护工作有据可循、有迹可查。

升级维护：为保障各类安全设备及系统处于最新技术状态和最优运行状态，减少系统漏洞隐患，增强设备健壮性及稳定性，安全服务人员需要密切关注厂商所发布的软件升级信息，对设备升级的必要性和可行性进行评估，尽快以稳定可靠的周全方案对安全设备执行升级操作，以持续优化安全设备运行状态。

同时更新完善日常运维问题处理流程，并对处理过程进行持续跟踪闭环，进行有效反馈，形成处置记录报告。

安全信息报送

定期收集整理网络安全方面的相关信息进行报送。主要包括互联网网络安全态势整体评价，全国范围或省级行政是否发生安全事件，如发生分析其原因、处理过程和总结，病毒、漏洞、威胁信息等安全事件以及分析针对政府、企业以及广大互联网用户的主要安全威胁来源。遇重大安全漏洞或事件时，实时通报事件预警，提供安全防护或规避建议，报送频率不低于每月2次。

政务云运维支撑

进行政务云财政业务的安全防护策略、实时响应处置策略的优化指导，充分发挥基础安全服务的安全防护能力，满足财政个性化安全防护需求。

根据政务云下发的安全告警单，配合信息中心完成告警单的及时处置，安全事件排查及安全加固。实现财政厅政务云多云环境下的安全监管、通报预警、应急处置等安全服务闭环能力。

3网络安全培训及安全宣传周服务

（1）网络安全培训服务：每年提供至少1次全省财政信息化干部网络安全工作实践技能培训，不少于2天，主要内容为网络安全设备日常运维操作、常见故障排查思路、安全软件使用等内容，组织方式和场地由财政厅提供。

（2）网络安全宣传周：在网络安全宣传周之际，配合采购方做好网络安全宣传工作，准备安全宣讲PPT、彩页等资料。组织高级安全讲师，进行网络安全意识宣讲，提升全员网络安全意识。

服务团队

组织架构

安全服务人员是整体保障服务实施过程中最为关键的资源，保证合适的人员以足够的精力参与财政厅网络安全整体保障服务项目，是落实安全服务效果的重要保证。

为有效保障财政厅网络安全整体保障服务项目资源投入的合理有效，安全服务作用达到实际效果，本次牵头财政整保服务项目的安全公司须要安排具备丰富安全服务项目经验的专业安全服务人员，组建一线服务团队、二线支撑团队，由项目经理统一管理，统筹协调，协同财政厅相关人员，建立财政网络安全整保服务保障团队，完善组织架构，明确角色职责，切实保障安全服务质量。

角色职责

n **项目经理**

项目经理1名，现场驻场，负责统筹服务工作的开展，完成服务安全服务进度管理、质量管理工作以及沟通协调财政厅第三方安全服务厂商工作。

n**一线服务团队**

一线服务团队为现场驻场团队，主要负责现场安全服务工作，听从财政厅日常工作安排，开展日常安全运维服务，如日常安全巡检、

安全优化及日常安全事务处置等安全运维工作；负责安全基线检查、渗透测试等安全保障工作。由3名驻场安全运维工程师、1名驻场攻防（渗透）工程师、2名驻场安全工程师组成。

n**二线支撑团队**

二线服务团队主要通过远程或现场服务方式为财政厅提供相关安全服务，由咨询专家、攻防专家等成员组成。负责安全咨询、规划设计等相关服务，为财政厅提供安全建设、安全管理、运维流程等相关咨询设计服务；负责网络安全事件应急保障类相关服务，具体负责应急响应体系建设、攻防演练、安全事件应急响应处置、追踪溯源及重大活动保障等特殊时段技术支撑工作。

服务清单

整体保障服务清单						
1、安全服务清单						
服务类别		序号	服务子项	服务频率/年	服务交付成果	备注
安全咨询服务		1	安全建设咨询	按需	按需提交安全建设咨询文档等	详见招标要求
		2	安全管理咨询	按需	按需提交安全管理咨询文档等	详见招标要求
		3	商用密码咨询	按需	按需提交商用密码咨询文档等	详见招标要求
		4	**安全加固咨询**	按需	按需提交安全加固咨询文档等	详见招标要求
	安全	5	安全基线核查	12次/年	按需提交《信息系统基线整改记录单》	详见招标要求
		6	系统漏洞扫描	12次/年	按需提交《信息系统漏洞整改记录单》	详见招标要求
		7	渗透测试	不超过20次/年，一次一个系统	按需提交渗透测试报告、复测报告	详见招标要求

							系统		
				检测保障服务	8	APP安全测试	不超过1个/年	按需提交安全测试报告	详见招标要求
					9	**代码审计**	按需	按需提交代码审计报告	详见招标要求
					10	**应急预案演练**	1次/年	按次数提交应急预案、应急演练总结	详见招标要求
					11	**全省网络安全风险评估及问题整改服务**	不超过80人天/年	按需提交《风险评估报告》	详见招标要求
			安全保障服务	应急响应保障服务	12	**应急响应保障服务**	不超过20人天/年	按需提交应急响应总结报告	详见招标要求
				专项保障服务	13	**攻防演练防守服务**	不超过200人天/年	按需提交《网络攻防演练复盘报告》	详见招标要求
					14	重大活动保障服务	不超过50人天/年	按需提交重点时期的安全保障报告	详见招标要求
					15	**网站安全监测保障服务**	7*24h/年	每月定期提供安全监测报告	详见招标要求
				日常安全运维保	16	资产梳理更新	12次/年	每月定期更新输出财政厅资产总表	详见招标要求
					17	日常监测分析	实时	每月非输出网络安全月报	详见招标要求
					18	设备安全运维	每工作日	定期形成处置记录报告	详见招标要求
					19	安全信息报送	24次/年	按需提供安全信息报送报告	详见招标要求

	障	20	政务云运维支撑	按需	按需提供处置记录	详见招标要求
网络安全技能实训服务及安全宣传周服务		21	**网络安全培训服务**	1次/年	按次数提交培训方案、培训课件	详见招标要求
		22	**网络安全宣传周**	1次/年	按次数提交宣传周材料	详见招标要求

2、运维服务团队人员清单		
人员团队	人员类别	人员数量
项目经理	项目经理（驻场）	1
一线驻场团队	渗透工程师（驻场）	1
	安全工程师（驻场）	2
	运维工程师（驻场）	3
二线支撑团队	攻防专家（不驻场，按需调配）	6
	咨询专家（不驻场，按需调配）	4

安全保密要求

供应商需提供安全保密承诺书，承诺在服务期限内，遵守采购人的安全保密规定，保护采购人的系统、数据、信息的安全，保密期限自服务开始日始至本项目约定的信息全部成为公开信息止。由于供应商违反保密规定而导致的泄密或破坏，由供应商负全责，并由供应商赔偿采购人所有损失。

违反保密规定的，采购人有权终止合同，并有权要求供应商向采购人支付合同金额 20%的违约金，对由于供应商泄密给采购人造成的经济及声誉损失，采购人有权依照合同和相关保密法律法规追究供应商的法律责任。

履约及项目验收

服务期限

本项目一招3年，合同一年一签，合同期满验收通过且绩效考核合格后，续签下一年度合同

服务地点

四川省成都市锦江区南新街16号

服务考核办法

中标供应商对招标文件内容的响应，视为具备相应服务能力。采购人在服务期结束后根据《四川省财政信息中心运维服务管理办法》和考核细则（详见《网络安全技术支撑服务考核表》）对服务质量进行考核评价，考核结果作为第二次付款（绩效服务费）依据。

网络安全技术支撑服务考核表

1、安全咨询服务考核					
服务类别	序号	服务子项	服务频率/年	服务考核分项分值	总分
安全咨询服务	1	安全建设咨询	按需	服务态度（0-3 分） 服务方案完整性（0-6 分） 服务效果评价（0-6 分）	15
	2	安全管理咨询	按需		
	3	商用密码咨询	按需		
	4	**安全加固咨询**	按需		
2、安全保障服务考核					
		5 安全基线核查	12次/年		
		6 系统漏洞扫描	12次/年		

			安全检测保障服务	7	渗透测试	不超过20次/年，一次一个系统	服务次数（0-9 分） 服务报告完整性（0-9 分） 服务响应（0-6 分） 服务满意度评价（0-6 分）	30分
				8	APP安全测试	不超过1个/年		
				9	代码审计	按需		
				10	应急预案演练	1次/年		
				11	全省网络安全风险评估及问题整改服务	不超过80人天/年		
		安全保障服务	应急响应保障服务	12	应急响应保障服务	不超过20人天/年	1、在上级单位或网络安全监管部门组织网络安全攻防演习中被控制系统权限，按被控制系统数量，每1 个系统扣除 2 分；如同时被绩效扣分的，每发生1 件次扣除 4 分。 2、重点保障期间发生网络安全事件被上级单位或监管单位通报，或发生影响财政系统正常运行的安全事件，每发生一次扣除专项保障服务 8 分。 3、服务次数每少一次，扣除专项保障绩效 2 分，	20
				13	攻防演练	不超过200人		

				专项保障服务		**防守服务**	天/年	因上级单位或监管单位当年取消的重保及护网行动除外。 4、因网络安全防护措施有力，在上级单位或网络安全监管部门组织的网络安全检查、攻防演习等活动中，未出现问题被通报、被绩效扣分情况的，按件次加专项保障服务 4 分。 备注：专项保障考核分值为负值时，扣除其它项服务考核分值作为填补，直至当年期整体保障服务分值为0。	分
					14	重大活动保障服务	不超过50人天/年		
					15	**网站安全监测保障服务**	7*24h/年		
				日常安全运维保障	16	资产梳理更新	12次/年	1、因日常安全运维服务不力，发生被上级单位或网络安全监管部门通报的网络安全事件，每发生 1 件次扣除 3-12 分。 2、发生网络安全事件导致财政信息系统不能正常运行的，如恶意软件扩散、安全运维误操作、网页被篡改等，每次扣除12分。 3、在日常运维工作中表现突出，发现网络安全工作重大缺陷，及时向采购人提出建议并配合整改，且受到上级单位或网络安全监管部门表扬的；或安全运维工作受到厅领导表扬的；按件次加安全运维服务 4 分。 备注:安全运维服务考核分值为负值时，扣除其它项服务考核分值作为填补，直至当年期整体保障服务分值为 0。	30分
					17	日常监测分析	实时		
					18	设备安全运维	每工作日		
					19	安全信息报送	24次/年		
					20	政务云运维支撑	按需		
			3、网络安全技能实训服务及安全宣传周服务考核						
			网络安全技能实训服务		21	**网络安全培训服务**	1次/年	培训满意度评价（3 分） 培训材料完整性（1 分） 培训体验（1 分）	5分

及安全宣传周服务	22	**网络安全宣传周**	1次/年	培训样验（1 分） 备注：培训次数每少一次，扣除服务绩效分值 2.5 分	3分

说明：1.服务期内发生特别重大（Ⅰ级）或重大网络安全（Ⅱ级）事件，采购人有权不支付绩效服务费用。

2.供应商考核分数大于等于 90 分，采购人支付绩效服务费用全款；大于 70 分且小于 90 分时，按照（年度考核分数-70）%*5*服务绩效费用支付绩效服务费用；小于等于 70 分时，采购人不支付绩效服务费用。

项目验收

供应商于服务期限到期前 7 个工作日向采购人提出验收申请，采购人在收到验收申请后组织信息化专家，按照政府采购相关法律法规、《四川省财政信息中心运维服务管理办法》以及服务考核办法进行验收，验收结果作为第二次付款依据。

付款方式

1、每年合同金额的 60%作为首付款，40%为绩效服务费用。合同金额分两期支付。

2.合同签订后，采购人在收到供应商出具的等额且合法有效发票 ，支付合同总金额的60.00%。

3.项目服务期结束并通过项目验收后，采购人根据验收结果向供应商支付剩余合同款，最高为40%。

4.上述款项由采购人在收到供应商出具的等额且合法有效发票后 30 日内汇入供应商指定账户。

3.2.3人员配置要求

采购包1：

详见3.2.2服务要求

3.2.4设施设备配置要求

采购包1：

详见3.2.2服务要求

3.2.5其他要求

采购包1：

1、服务期限：本项目一招3年，合同一年一签，合同期满验收通过且绩效考核合格后，续签下一年度合同，预算：189.6万元/年。2、合同支付约定： 1、 付款条件说明： 合同签订后，采购人在收到供应商出具的等额且合法有效发票 ，达到付款条件起 30 日，支付合同总金额的 60.00%。2、 付款条件说明： 项目服务期结束并通过项目验收且采购人在收到供应商出具的等额且合法有效发票后后，采购人根据验收结果向供应商支付剩余合同款，最高为40%。 ，达到付款条件起 30 日，支付合同总金额的 40.00%。3、成本补偿和风险分担约定：中标供应商对招标文件内容的响应，视为具备相应服务能力。采购人在服务期结束后根据《四川省财政信息中心运维服务管理办法》和考核细则（详见《网络安全技术支撑服务考核表》）对服务质量进行考核评价，考核结果作为第二次付款（绩效服务费）依据。4、知识产权归属和处理方式：供应商保证所提供的服务以及支撑服务所需产品、设备均为 合格、正版，且均不会侵犯任何第三方的专利权、商标权或著作权。供应商保证所提供的服务的所有权完全属于供应商且无任何抵押、查封等产权瑕疵。若因专利权、商标权、著作权或产权瑕疵而引起法律和经济纠纷，视同供应商违约，且由供应商承担所有相关责任和费用。若供应商采用第三方拥有知识产权的服务、产品、设备等时，则供应商必须承担合法获取该知识产权的所有相关费用。 供应商及采购人双方在本合同履约实施过程中所产生的所有文件、记录、 资料、数据、源代码、成果等的知识产权归采购人所有。5、合同其他条款：（四）合同解除后，尚未履行的部分采购人及供应商不再履行。由于采购人原因造成的合同终止，采购人须向供应商支付截至本合同协议解除时交付成果已被接受的所有已提供服务的费用，对于采购人已支付费用但供应商尚未开始或尚未完成的工作，供应商应按照尚未开始或尚未完成部分占采购人已支付费用而应当完成的全部工作的比例，退还采购人已支付的费用。由于供应商原因造成的合同终止，供应商应当退还采购人已支付的尚未开始或尚未完成部分的费用，并赔偿采购人因此而遭受的损失。：

3.3商务要求

3.3.1服务期限

采购包1：

自合同签订之日起1095日

3.3.2服务地点

采购包1：

四川省成都市锦江区南新街16号，驻场场地由采购人提供。

3.3.3考核（验收）标准和方法

采购包1：

供应商于服务期限到期前 7 个工作日向采购人提出验收申请，采购人在收到验收申请后组织信息化专家，按照政府采购相关法律法规、《四川省财政信息中心运维服务管理办法》以及服务考核办法进行验收，验收结果作为第二次付款依据。

3.3.4付款进度和支付方式

采购包1：

分期付款

3.3.5违约责任与解决争议的方法

采购包1：

违约责任： （一）采购人违约责任 采购人在本合同约定的时间内无故拖延付款，每逾期一个工作日，采购人应按应付金额的0.2‰支付滞纳金。 （二）供应商违约责任 1.供应商不履行或不按合同约定履行的，采购人可向供应商投诉，在接到采购人投诉后，供应商应三日内立即采取补救措施，提供本合同约定的服务。超过三日，供应商未能及时采取补救措施并有效解决时，采购人有权另行聘请第三方进行运维服务，由此产生的所有费用由供应商承担。 2.供应商在本合同约定的保密期内泄密的，视同供应商违约，供应商应向采购人支付违约金，违约金金额为本合同总金额的20%，并承担由此产生的其他法律责任。 3.如因供应商的疏忽、失职、过错等故意或者过失原因给采购人造成损失或侵害，包括但不限于采购人本身的财产损失、由此而导致的采购人对任何第三方的法律责任等，供应商均应承担全部的赔偿责任和法律责任。 争议解决办法：本合同适用中华人民共和国法律并应根据中华人民共和国法律解释。凡因本合同引起的或与本合同有关的任何争议，双方应协商解决，协商不能解决时，均可向采购人所在地人民法院提起诉讼，诉讼费用由败诉方承担。 在诉讼期间，除正在进行诉讼部分外，本合同其他部分应继续执行。