

一、项目概况

四川省科协系统依托天府科技云平台持续“深化天府科技云服务”，为更好地服务于全省科技工作者、企事业单位和人民群众，省科协搭建了基于“公有云+政务云”的混合云，平台系统有实名认证和交易支付过程，其中包含敏感个人信息和移动支付安全，其信息安全问题不容忽视。本项目通过采购引入专业安全技术服务，评估平台系统风险，制定防范策略，配置安全设备，定期总结报告，全面负责平台信息安全防范，包括规范后台管理操作、防止黑客入侵、排除网络故障、修补安全漏洞等，确保平台用户数据、交易数据、网络通信数据等重要数据的信息安全，保障 2024 年度“天府科技云”平台信息系统稳定对外服务不中断，避免出现信息安全事故。

★二、服务内容

1. 云安全服务整体解决方案。云安全服务整体解决方案，按照公安部三级等保要求，提供公有云部分的云资源安全服务，包含云下一代防火墙、Waf 防火墙、Web 应用防火墙、Anti-DDoS 及抗 D 清洗、网页防篡改、日志审计、数据库审计、云堡垒机、防病毒、服务器安全卫士。并提供 1 人驻场服务，提供安全监测、网络安全维护工作；提供本年度重点时段（攻防演练、重点节假日等活动）运维保障服务。

2. 安全防护服务：

（1）安全加固服务：在移动应用发布前进行高强度安全加固保护，有效防止反编译、二次打包、内存注入、动态调试、数据窃取等恶意攻击行为，全面提升移动应用安全防护等级。

（2）信息合规检测服务：根据监管单位的相关要求和管理规范，进行合规检测评估服务，提供问题详情报告及修复建议，并完成问题修复，避免因不合规造成通报、下架风险。

（3）渗透测试服务：对整体网站信息管理系统进行全面漏洞检查和研究，通过模拟黑客攻击的形式来发现应用程序中的安全漏洞，并给出相应的解决方案，以提升应用程序的安全性。

3. 等保测评服务。根据《中华人民共和国网络安全法》等法律法规及相关文件要求，提供 2024 年度等保测评服务，保证天府科技云平台（公有云

及政务云环境）2024 年度达到等保测评三级要求。

4. 安全演练服务。提供一次信息安全应急演练、一次数据灾备演练。提供演练详情报告及修复建议，并协助完成相关问题修复。

三、功能和技术要求

1. 云安全服务整体解决方案：

（1）WEB 应用防火墙应覆盖 OWASP 最重要的 10 种常见安全威胁（具体为：SQL 注入、XSS 跨站脚本、远程溢出攻击、文件包含、Bash 漏洞攻击、远程命令执行、目录（路径）遍历、敏感文件访问、命令/代码注入、可以针对国外部分国家和国内省份的来源 IP 进行自定义访问控制），支持通过预置信誉库，对以上 10 种常见安全威胁进行检测和拦截。

（2）网页防篡改支持篡改监测自动恢复技术，在主机本地和远端服务器上实时备份已授权的用户所修改的文件，保证备份资源的时效性。当企业主机安全服务检测到非法篡改行为时，将使用备份文件主动恢复被篡改的网页。

（3）云下一代防火墙应具备监控统计功能，支持链路状态监控，可查看指定应用/应用组详情，支持选择多条链路进行对比分析。

（4）云下一代防火墙支持带宽管理，能够针对 IP 和应用进行流量控制，并相互嵌套；能够根据不同需求信息（例如安全域、接口、地址、用户/用户组、服务/服务组、应用/应用组、TOS、Vlan 等信息）划分管道。

（5）云下一代防火墙支持两层八级管道嵌套，能够同时做到两个维度的流量控制。

（6）日志审计支持采集 VPC/ELB/CTS/APIG/DDS/RDS 等云服务租户面日志。

（7）数据库审计支持审计时长、语句总量、风险总量、风险分布、会话统计、SQL 分布等多维度的快速分析。

（8）DDOS 高防支持对 IP 地址（段）黑洞路由服务，实现丢弃来自网络特定方向的包括攻击流量在内的所有去往该 IP 地址（段）的流量。

（9）云堡垒机支持 HTML5 远程登录资源，无需安装客户端，一键登录运维资源。

(10) 服务器安全卫士具有信息技术产品安全测评证书 (EAL3+)。

(11) 服务器安全卫士客户端支持使用非 root 账号运行。

(12) 服务器安全卫士支持 windows 补丁替换关系梳理, 逐级查询补丁替代关系。

(13) 服务器安全卫士支持自定义恶意进程名与进程参数检测, 实时监控服务器的恶意进程启动行为。

(14) 防病毒支持挖矿软件检测、支持恶意攻击木马检测、支持勒索病毒检测等其他常见病毒检测。

(15) 驻场人员要求: 提供驻场人员应为计算机类或网络安全相关专业, 至少具有 2 年相关工作经验。

2. 安全防护服务:

(16) Android 应用加固配置界面支持上传 *.apk 和 *.aab 文件进行加固, 且支持勾选自动生成多渠道加固包

(17) Android 应用加固策略支持 DEX 字符串加密、so 文件加密、u3d DLL 文件加密、防动态调试保护、资源加密、数据加密、完整性保护、运行环境保护 (包括防界面劫持、防截屏录屏)。

(18) iOS 应用加固配置界面支持调整控制流混淆强度从 0-100%; 配置界面支持勾选静态防调试分析功能项目 (包括: 字符串加密、静态防调试、静态完整性保护、静态防注入)、配置界面支持勾选动态防调试分析功能项目 (包括: 动态防调试、动态完整性保护、动态防 HOOK)。

(19) iOS 应用加固配置界面支持防二次打包、防设备越狱、防 Frida Hook 增强、APP 模糊化保护、防日志泄露、防 AirPlay 投屏、FishHook 关键函数防护、https 证书校验 (防中间人攻击)。

(20) 移动应用加固系统, 要求提供中国网络安全审查技术与认证中心授予的基于评估保障级 (EAL) 的信息安全认证 (EAL3) 证书。

(21) 支持监测操作者在手机上通过云手机管理 APP 发送操作指令行为; 支持监测移动端摄像头在拍摄人脸信息时被绕过的行为; 支持监测应用是否运行在 Win11 的环境中; 支持监测高频更换设备的异常行为。

(22) 信息合规检测服务应包括①APP 个人信息快速访谈或调研: 从隐

私政策文本、APP 收集使用个人信息行为、用户权利保障三个方面快速评估 APP 针对个人信息保护的现状；②APP 个人信息合规差距分析：基于法规要求以及 APP 现状，对 APP 进行合规差距分析，评估当前 APP 与法规现状的差距项；③APP 个人信息保护现状评估报告：基于快速访谈结果，以及差距分析结果，形成 APP 在个人信息保护方面的现状评估报告，报告中应提出 APP 存在的问题，并提供相应的整改建议；④整改过程中提供指导：基于现状评估报告中提出的问题及整改意见，协助完成 APP 的隐私合规整改并再评估。（提供承诺函）

（23）渗透测试服务应对整体网站信息管理系统进行全面漏洞检查和研究，通过模拟黑客攻击的形式来发现应用程序中的安全漏洞，并给出相应的解决方案，制定并提交相应测试报告。供应商应提供整体实施方案，包括项目概述、服务方案、项目实施方案、测试过程中需使用测试设备清单、时间安排、阶段性文档提交等。

3. 等保测评服务

（24）供应商应提供具有资质的的第三方专业测评机构名单，会同采购人确认同意的第三方专业测评机构按照等级保护相关标准对天府科技云平台系统进行信息安全网络等级测评并编制《网络安全等级保护测评报告》，确认天府科技云平台系统达到等保测评（三级）要求，完成等保备案手续，确保信息系统安全保护等级定级准确、备案完整。（提供承诺函）

4. 安全演练服务

（25）容灾演练：确保平台主站云服务器站点机房发生灾难事件时，异地容灾服务器能顺利接管平台主要业务功能服务。供应商应提供整体实施方案，包括项目概述、服务方案、项目实施方案、时间安排、阶段性文档提交等。

（26）信息安全应急演练：模拟信息安全事件发生后相关工作人员与各部门的安全事件协同处理的过程，并通过后续的演练总结，完善应急预案、改进应急操作及流程、全面提高网络与信息安全事件的应急响应能力。供应商应提供整体实施方案，包括项目概述、服务方案、项目实施方案、时间安排、阶段性文档提交等。

四、其他要求

1. 供应商需具有类似项目（平台/软件安全支撑服务或容灾运维服务类）履约经验；

2. 供应商需针对本项目提供实施方案，实施方案包括但不限于：①项目整体方案大纲；②项目进度计划；③拟投入本项目的人员团队及职责分工；④拟投入本项目的支撑服务设施设备方案；⑤公司内控管理制度；⑥信息安全保密方案；⑦服务质量保障方案。

3. 供应商需针对本项目提供后续服务方案，后续服务方案应包括但不限于：①后续服务团队配置；②设备维护服务方案；③故障响应时间；④应急响应方案；⑤重保响应；⑥后续服务保障；⑦设备保修运行监管计划。

★五、商务要求

1、服务期限：自合同签订之日起一年。因成交人原因提前终止服务的，根据法律法规和合同条款追究违约责任和法律责任。

2、服务地点：四川省成都市（采购人指定地点）。

3、付款方式：

① 合同签订后且收到成交供应商开具的合同金额 60%等额发票，达到付款条件起 10 个工作日，支付合同总金额的 60.00%。

② 云安全服务相关产品部署完成，驻场人员到位后，成交供应商提出初验申请并提供相关证明，经采购人验收合格后且收到成交供应商开具的合同金额 30%等额发票，达到付款条件起 10 个工作日，支付合同总金额的 30.00%。

③ 项目服务完成（合同期满）后，经采购人最终履约验收合格后且收到成交供应商开具的合同金额 10%等额发票，达到付款条件起 10 个工作日，支付合同总金额的 10.00%。

4、保密要求：未经采购人书面同意，成交供应商不得擅自将本项目服务内容相关的资料（包括协议、附件等）提供给任何第三方。（提供承诺函）

5、履约验收标准和方案

验收标准：按照《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》（财库〔2016〕205 号）要求、磋商文件的服务和技术指标要求、成交供应

商的响应文件及合同约定标准进行验收。

验收方案：

- 1) 验收组织方式：自行验收
- 2) 是否邀请本项目的其他供应商：否
- 3) 是否邀请专家：否
- 4) 是否邀请服务对象：否
- 5) 是否邀请第三方检测机构：否
- 6) 履约验收程序：分期验收
- 7) 履约验收时间：供应商提出验收申请之日起 30 日内组织验收
- 8) 验收组织的其他事项：项目建设完成，驻场人员到位后，成交供应商提出初验申请并提供相关证明后，采购人组织初步验收。在项目服务完成（合同期满）后，采购人组织对成交供应商开展最终履约验收。
- 9) 技术履约验收内容：采购文件规定的技术服务要求及响应文件
- 10) 商务履约验收内容：采购文件规定的商务服务要求及响应文件
- 11) 履约验收其他事项：履约验收各条款间有不一致时，按较高标准进行。

注：本章标注“★”条款为实质性要求，有任意一条不满足作无效响应处理。