服务内容及要求、商务条件说明

**一、项目概况**

四川省司法厅运维服务包括三个部分，分别为：**设施设备质保及人员驻场服务**，保障我厅计算机信息系统、指挥中心、视频会议系统、门禁安防系统等信息系统可靠、高效、持续、安全运行，为我厅的信息化建设提供科学的建议、技术支撑与保障；**网络安全专项服务**，保障重要时期网络安全、规避网络安全风险，增加网络安全产品和网络安全技术支撑力量，在重要时期组织有效的网络安全保障工作，满足年度网络安全的相关工作要求，同时持续强化本单位安全防护能力，加强安全保障；**政务云信息安全集成实施服务**，对我厅部署在省级政务云的业务系统进行安全检查，对关键业务系统进行有目的、有重点地安全评估与加固，进一步提高信息安全保障能力，降低信息系统安全运营风险，及时对网络安全事件进行有效应急响应；提高信息安全风险防范能力，保障业务系统安全稳定运行。

1. **服务内容及要求**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **运维内容** | | **技术要求** |
|
| **1** | 设施设备质保及人员驻场服务 | 计算机信息系统运维及驻场服务 | 主要负责维护机房、楼层弱电间的网络安全设备约54台、服务器104台（含国产服务器36台），计算机终端约428台、复印打印设备约250台、电话214台，提供正常运行所需的技术支持服务；具体内容如下：  1.现场专人驻守服务：安排现场驻守技术人员1人，技术能力满足驻场工作要求并得到采购人同意。  2.日常终端服务：对计算机终端软、硬件故障（如：线路不通、硬盘损坏、病毒侵入、系统故障等）进行维护；对系统维护（操作系统、办公软件等）；办公设备（打印机、扫描仪等）维护。出现问题以后恢复时间软件不超过一天，硬件故障处理不超过三天，更换不超过七天，特殊情况除外。  3.后台应急响应服务：主要是对主机和网络进行维护和应急：包括电话响应服务、7天\*8小时在线响应服务、7天\*24小时在线监控服务、现场应急响应服务。  4.资产管理服务：协助开展信息化资产管理，对所有的终端设备统一编号、管理。  5.检查服务：开展网络安全日常检测和软件正版化检查整改、电话检查服务，配合完成网络安全自查工作。  6.安全咨询及检测服务：协助进行等保、分保咨询服务、检查咨询服务、安全巡查服务（巡查服务范围涉及：互联网防火墙、互联网拒绝攻击服务系统、互联网入侵防御系统、政法专网防火墙、政法专网防病毒系统、电子政务外网防火墙、电子政务外网入侵检测系统，工作日每日巡检）、安全检测服务、信息系统安全风险评估服务。  7.安全管理制度完善：根据省安全管理现状及系统内部业务应用和使用情况的变化，健全和优化系统内的安全管理制度，并监督和督促相关厂商按照制度和规章执行。 |
| **2** | 指挥中心运维及驻场服务 | 主要对指挥中心所涉及的监控平台、点名系统、视频会议系统、大屏显示系统等进行管理和维护。根据司法部、省政法委及司法厅的指挥调度的需求，熟悉使用系统，完成系统操作，并开展视频上传日常性检查和指挥中心设备维护。具体内容如下：  8.现场专人驻守服务：安排现场驻守1人，技术能力应满足驻场工作要求并得到采购人同意。  9.对现场平台的正常使用开展技术支持工作，处理平台出现的各种问题，并对问题进行记录和跟踪。  10.负责对接和解答技术咨询工作，并提供技术资料。  11.指导指定的人员进行平台的日常操作和使用，保证业务的正常开展。  12.设备监控：管理监控体系，有效地对系统的监控设备运作情况和传输线路的性能、通断情况进行实时监控，及早发现问题，排除故障。  13.平台业务监控：驻场服务人员对平台的各业务功能是否正常进行主动监测，发现问题后，第一时间进行问题上报和处理，以减少故障时间。  14.故障修复：服务人员负责系统/设备发生故障的抢修任务。出现问题以后恢复时间软件处理不超过一天，硬件故障处理不超过三天，更换不超过七天，特殊情况除外。  15.软件平台优化：根据现场软件平台使用中的情况，进行软件平台优化，包括：版本升级、补丁更新；部署调整、配置变更、参数调校；大数据表清理；系统扩容建议；系统安全加固。  16.临时保障服务：当遇到重大活动需要提供临时保障服务时，驻场服务人员须在需要保障服务的前三天对现场平台软件、系统设备进行临时性安全检查，排除安全隐患，以做到万无一失。  17.技术指导培训：服务人员应提供必需的服务技能培训，并对相关技术问题进行充分交流，以提供客户技术水平，使客户能熟练使用现有系统。开展针对软件产品的操作、维护、以及相关知识的培训。 |
| **3** | 视频会议系统、门禁安防系统运维及驻场服务 | 主要保障3个音视频会议室的本地会议、全国视频会议、全省视频会议及门禁安防系统正常运行。具体内容如下：  18.现场专人驻守服务：安排现场驻守1人，技术能力应满足驻场工作要求并得到采购人同意。  19.提供全省视频会议系统管理软件，实现对全省视频会议系统分级分权的管理，对全省司法行政高清视频会议系统中MCU和终端进行统一管理。  20.对视频会议系统提供每周7天、每天24小时的及时响应服务；随时向服务方提供会议保障服务及疑难问题的解答，尽量向服务方提供好的的建议及最优的解决方案。  21.接受司法部、省政府每周点名，确保系统正常运行。  22.配合服务方的会议要求，完成全省视频会议的召开及会议保障工作。  23.根据司法部的相关会议要求，组建会议，并做好会议保障工作。  24.根据省政府、省委政法委的相关会议要求，组建会议，并做好会议保障工作。  25.配合服务方完成外出的视频会议需求，提供技术及相关服务，完成会议保障工作。  26.配合不同的会议需求，需完全能熟练操作3个会议室的音视频系统，顺利完成会议的保障工作。  27.对服务方涉及本项目使用的相关人员进行培训。  28.为全省市（州）、县（区）司法行政系统的高清视频会议系统建设提供技术支持，配合完成接入。  29.对2楼会议室、7楼会议室及2楼指挥中心中所包含音频视频系统及相关配套系统存在的问题提供改进建议，积极配合完成改进，提高会议质量。  30.提供新设备和软件加入系统的调试。  31.建立详细的档案记录，随时跟踪设备的运行情况及故障发生情况，并定期向服务方负责人提供项目中设备运行情况的调查报告；通过设备运行情况的分析，找出可能存在的潜在问题，预防故障的发生。  32.对现场工作做详细的记录，对设备运行情况、施工中遇到的问题进行备案，以便以后对故障情况进行正确的分析。 |
| **4** | 设备质保服务 | 33.信息化基础设备硬件维护服务：配合我单位开展计算机信息系统、指挥中心、视频会议系统等主要设备维护服务；开展网络及网络安全系统的网络调整、线路优化、防火墙、路由器、交换机、网闸等设备软件版本升级、设备搬迁等工作，并对调整、优化、升级、修复后的设备运行情况进行专项监控分析工作；开展视频会议系统的网络调整、线路优化、摄像头、MCU、终端、音频系统等设备软件版本升级、设备搬迁等工作，并对调整、优化、升级、修复后的设备运行情况进行专项监控分析工作，确保设备运行正常；开展安防设备系统的网络调整、线路优化、监控摄像头、流媒体服务器等设备软件版本升级、设备搬迁等工作，并对调整、优化、升级、修复后的设备运行情况进行专项监控分析工作，确保设备运行正常；开展各类控制器、指纹机、闭门器配置、维护和故障处理工作，并配合我单位开展线路优化、指纹机、闭门器等设备软件版本升级、链路割接、设备搬迁等工作，并对调整、优化、升级、修复、割接、搬迁后的设备运行情况进行专项监控分析工作，确保设备运行正常。  34.运维服务管理技术指导服务：根据运维服务管理工作要求，协助和配合开展技术指导服务，协助和配合开展信息化系统升级、搬迁、割接等工作的技术指导服务。  35.信息化系统备品备件服务：需建立的品备件库，配备足够种类和数量的备品备件，备品备件消耗后应当及时补充，以保证我单位信息化系统的最大无障碍使用时间。同时，维护服务涉及更换设备或零部件时，替换件应当为同等性能指标。补充备品备件所需费用由供应商自行负责。（提供承诺）  36. 为保证网络环境安全性，供应商提供信息化设施设备质保清单中终端安全管理、终端安全管理（国产）原厂售后服务承诺函。（提供承诺函）  37.维护服务等级调整服务：及时响应各类临时、应急或紧急状况下各类提升服务等级的要求，包括但不限于增加现场服务内容和现场技术支持人员以及提供应急设备、工具等，不得影响我单位工作的顺利开展。出现问题以后恢复时间不超过七天，特殊情况除外。  38.为保证网络环境安全性，供应商提供信息化设施设备质保清单中网闸、互联网边界安全网关(VPN)、入侵防御原厂售后服务承诺函。（提供承诺函） |
| **5** | 网络安全专项服务 | 资产梳理服务 | 39.供应商对我厅信息系统资产进行梳理，对我厅现有互联网和内网资产进行有效识别，通过对资产的识别收敛，将我厅现有所有资产纳入资产管理台账，便于我厅全面掌握资产的安全信息，为后续检查、评估奠定基础，从而一定程度上降低系统被攻击的可能。  40.服务结束后向我厅提交《资产梳理报告》。 |
| **6** | 网络安全专项检查服务 | 41.供应商利用对我厅信息系统资产梳理的结果，对我厅现有资产进行安全专项检查，将安全专项检查问题统一进行整改，避免由于低级的错误管理，导致我厅系统被攻击。  42.检查工作主要包括：漏洞风险评估、安全配置风险检查、弱口令检查、敏感信息泄露检查、违规外联检查、安全防护措施检查、资产暴露检查、远程安全接入检查、供应链安全风险排查、网络域间隔离措施检查等。  43.供应商对所发现的安全漏洞及安全风险，提出整改建议，并协助单位完成整改。 |
| **7** | 网络架构风险评估服务 | 44.供应商通过对我厅整个组织的网络体系进行深入调研，全面对网络架构安全性进行检查分析，从整体结构合理性、设计与实际符合性与优化调整给出评估建议。检测内容包括区域划分合理性、业务类型及分布安全分析、高可用性、安全策略等。 |
| **8** | 敏感信息排查服务 | 45.供应商根据我厅要求及对敏感信息排查的要求，对互联网中涉及我厅各类敏感信息进行安全排查，降低攻击者获取我厅敏感信息的可能，降低我厅被攻击的可能。 |
| **9** | 威胁建模服务 | 46.供应商对我厅核心业务系统的受攻击面进行建模分析，从攻击源、攻击路径等层面进行分析，尽可能的全面发现攻击源和攻击路径，通过对攻击源和攻击路径的分析，使防守人员可在各源头和攻击路径上进行封堵防护，保障我厅核心业务系统的安全。 |
| **10** | 红队测试服务 | 47.供应商提供不局限于传统的渗透测试，采用背靠背方式贴近真实攻击，侧重绕过防御体系，达成获取业务权限或数据的目标，以便我厅检验供应商在真实攻击中纵深防御能力、告警运营质量、应急处置能力。  48.供应商着重于针对单位的人员、业务系统、供应链、办公系统、物理安全等真实脆弱点进行攻击评估，根据评估结果结合我厅实际安全需求，给出梯度式安全防御方案，对易受攻击的核心节点进行优先防御，有效提高攻击者成本。 |
| **11** | 外网安全监测 | 49.供应商应对我厅互联网系统尤其是网站系统进行统一监测、防护，采用信息自主研发网站防御系统，对网站或web系统进行严格的监测和防护。 |
| **12** | 内网安全监测 | 50.供应商对我厅内部网络系统尤其是核心业务系统进行监测，内网安全监测将依托于我厅现有网络安全防护措施，依托现有安全设备，对整个内网安全态势进行监测分析。  51.在我厅不具备安全防护措施或安全设备缺失时，供应商在防守服务时期提供相应的安全防护产品，为我厅进行临时的安全防护保障。  52.内网安全监测主要从内网流量监控、恶意扫描监控、数据窃取监控、网络病毒监控、恶意行为监控及告警信息监控等层面对整个内网环境进行监测把控。 |
| **13** | 安全专家值守 | 53.在防守期间供应商提供安全专家值守，每天现场值守人数不低于4人，服务期内总服务天数不低于60天。指派高级安全工程师进行，对于监测发现的安全事件如：网络入侵事件、病毒爆发、遭受拒绝服务攻击等，现场值守人员将协助我厅进行应急处置，并溯源分析攻击源头，溯源分析将结合现有网络安全设备（监测和防护），对内外网流量进行分析、网络层流量分析、应用层流量分析、安全预警信息分析，进行整体事件的溯源。  54.同时提供整体加固修复方案。必要时，供应商配合第三方安全服务机构进行安全应急响应服务。安全值守期间，根据单位的要求，定期向我厅提交《安全值守报告》。 |
| **14** | 威胁情报共享服务 | 55.供应商利用威胁情报系统、漏洞管理系统以及大数据安全分析平台等服务工具，将在互联网侧捕捉到的最新的攻击行为以及攻击热点信息以及0day漏洞、高危漏洞等信息，以及供应商在其他防守工作中获取到的一些攻击手法和漏洞信息，及时同步到支撑单位，确保我厅在防守期间能够第一时间对行为和漏洞作出响应。 |
| **15** | 攻击诱捕与反制服务 | 56.供应商对我厅提供通过对模拟目标系统使得攻击行为在模拟环境中“打转”，延缓真正的攻击行为，为我厅防守提供时间保障。在监测的同时应对发现的攻击ip进行溯源以及敏感信息的反向获取。 |
| **16** | 防守工作复盘及总结 | 57.供应商在我厅防守工作结束后进行全方面的梳理，包括安全检查、安全加固、攻防演练、安全保障等内容。从威胁发现能力、威胁处置能力、安全防护能力、应急处置能力等角度，对整个防守服务期间的工作进行优势总结。对威胁发现能力、威胁处置能力、安全防护能力、应急处置能力、防护策略缺陷等角度进行劣势分析。对安全检查进行总结、安全防守进行总结、对安全防守成果进行汇报，为后续安全整改提出建议。  58.防守工作复盘及总结结束后向我厅提交《总结分析报告》。 |
| **17** | 安全优化整改建议 | 59.供应商针对防守工作中出现的安全风险及安全事件进行分析，对我厅现有防护体系进行调整和优化，提出整改建议，形成整改方案。向我厅提交《安全优化整改建议报告》。 |
| **18** | 提供技术培训服务 | 60.供应商对涉及红蓝对抗和重要时期保障工作的部门人员进行培训，内容主要是针对红蓝队在攻击和防守层面的注意事项以及如何配合单位完成演练活动。  61.服务期间在我厅指定时间和地点至少安排1次培训，总培训时长不低于6小时。培训结束向我厅提交《技术培训报告》。 |
| **19** | 服务工具 | 62.为保障服务效果，供应商应在防护期间提供必要的服务工具。服务工具在采购人机房部署时间不低于3个月。  63.服务工具支持大屏展示网络攻击态势，包括攻击地图、紧急事件数/总数、恶意文件数/扫描总数、风险趋势（高、中、低风险）、流量分析（吞吐量、HTTP流量、DNS流量）、高危风险类别排名、攻击源区域排名、紧急事件/高危事件。（提供功能截图）  64.服务工具具备针对数据库每张表、每个字段的内容进行敏感数据探测能力，敏感信息可由用户自定义。（提供功能截图进行证明）  65.服务工具具备数据库内核入侵隐藏用户的探测方法能力，并提供扫描报告。（提供功能截图进行证明）  66.服务工具具备沙箱功能，可动态执行可疑文件，分析代码进程、网络、文件等行为，并与进行关联分析。（提供国家认可的机构出具的证书或检验检测报告）  67.服务工具可实现沙箱逃逸检测。当恶意文件进行逃逸尝试，在沙箱报告中进行体现。（提供国家认可的机构出具的证书或检验检测报告）  68.服务工具可伪装的蜜罐类型包括但不限于：操作系统蜜罐、Web类蜜罐、中间件类蜜罐、数据库类蜜罐、工控类蜜罐、物联网类蜜罐、漏洞事件蜜罐等。（提供功能截图证明材料）  69.服务工具支持攻击者身份溯源，溯源维度包括但不限于：指纹溯源、社交账号、攻击工具、手机号、浏览器存储账号密码等。（提供功能截图证明材料）  70.提供应急处置服务工具。具备线索管理能力，可通过节点树的方式对关键线索进行管理，关联关键线索、IP路径。具备在开机、关机情况下都能一键提取安全事件相关信息的能力。（提供功能截图进行证明）  71.服务工具支持漏洞利用攻击的重放，重现渗透过程。（提供功能截图证明材料）  72.提供基于互联网公开的漏洞响应平台，方便漏洞信息的查验。（提供官网截图或知识产权相关证书的证明材料） |
| **20** | 政务云信息安全集成实施服务（互联网、电子政务外网各1套） | 云堡垒机防护服务 | 73.支持在IPV4,IPV6，IPV4与IPV6网络环境下部署。（提供产品功能界面截图证明）  74.管理员可根据目标资源设置不同角色：支持时间、命令、审批规则与资源角色关联，实现不同运维用户访问资源遵从不同的控制策略，超过资源角色中时间策略中的时间范围，系统将阻断运维会话，支持用户、资源帐号与资源角色关联，形成访问策略。（提供产品功能界面截图证明）  75.支持数据库协议自动改密，改密类型支持：Oracle、PostgreSQL、MySql、DB2、Informix 、SYBASE，Mssql。（提供相应的功能界面截图）  76.支持Oracle、Postgresql、Sybase、MySQL、SQL server数据库下行返回行数记录；支持在Oracle数据库运维，运维人员对变量进行绑定，执行SQL后，堡垒机系统可审计对应SQL中唯一标识符的具体值，协助审计员分析安全事件。（提供相应的功能界面截图）  77.支持审计查询关键字和结果显示支持多种编码(UTF-8,Big5,EUC-JP,EUC-KR,GB2312,GB18030,ISO-8859-2,KOI8-R,KS\_C\_5601\_1987,Shift\_JIS,Window-874)，由审计管理员自主选择。（提供相应的功能界面截图）  78.支持扫描本地运维工具并进行配置保存，简化运维人员使用配置过程。  79.支持客户端模式：提供客户端功能，用于运维人员和管理员通过客户端登录进行运维操作和管理操作，整个运维过程不依赖任何Active或Java控件。  80.支持用户以手机号码或邮箱地址作为用户身份登录。  81.支持通过应用发布开启运维屏幕水印，运维本地无法篡改水印内容，震慑不规范的运维行为，提升运维过程数据安全性。  82.支持基于消息队列的报警信号处理能力。（提供相应的功能界面截图或者提供相应的证明材料）  83.服务所涉及工具需具备有效的《IT产品信息安全认证证书》、《IPv6认证证书》。（提供证书复印件）  84.支持域名劫持防御功能、支持域名系统服务器缓存感染防御功能。（提供相应的功能界面截图或者提供相应的证明材料） |
| **21** | 云数据库审计防护服务 | 85.支持国产数据库人大金仓、达梦、南大通用、神通、高斯等数据库的审计。  86.支持netbios的审计，包括用户名、读写创建操作、响应时间、文件名等。（需提供截图证明）  87.支持对邮件协议的审计，包括smtp、pop3、imap协议，能够审计发件人、收件人、时间、返回码等。  88.内置多种规则分类，包括oracle、DB2、Mysql、Cache、Guass、shentong、Gbase、netbios、NFS等不低于26种协议分类，对于支持的规则分类，提供用户登陆、高风险操作、推荐审计命令等共计200余类出厂缺省规则集，用户无需自定义可直接引用。89.支持用户操作轨迹图展示，轨迹图维度可根据资源账号、源ip、客户端程序名、命令、表名、错误码等按需定义，可根据昨天、最近七天、最近30天以及自定义时间进行轨迹显示，可显示下一节点数量，可在某一维度中进行筛选，支持钻取功能。  90.支持基于场景的操作异常分析；可直观展现数据库异常、异常账号的访问、同账号多IP登录、上下班操作量对比异常、操作响应时间分析、用户变更、弱口令检测。（需提供截图证明）  91.支持疑似暴力破解分析、疑似撞库攻击分析；行为周期与阀值可按需定义。（需提供截图证明）  92.支持敏感数据访问独立大屏展示，可直观展示各类各级别敏感数据占比、敏感数据访问量与分布、敏感数据访问用户TOP5、敏感数据访问源IPTOP5、敏感数据增删改插操作分析等内容。  93.支持识别网络中的业务数据。（提供主管部门或具有CNAS/CMA认证的检测机构出具的证明材料）  94.服务所涉及工具需具备《信息技术产品安全测评证书》级别EAL3+及以上级别、IPv6 Readylogo Phrase 2认证证书，提供证书复印件。  95.支持对审计对象硬件状态的监测，提供相应的功能界面截图或者提供相应的证明材料。 |
| **22** |  | 云日志审计防护服务 | 96.支持日志源管理功能，对日志源进行增删改查、对断点日志源可以设置产生告警，单个日志源设备可查看该设备最近7天的事件趋势。  97.支持与Kafka、HDFS、ES、MongoDB大数据存储组件对接进行日志数据传输采集。（提供截图证明）  98.支持对国内主流国产化数据库进行日志数据采集，包括武汉达梦、人大金仓、南大通用、神州通用等；支持动态表名模式进行数据库采集，能按照时间或者数字的规则动态每天递增采集日志表。  99.支持对范式化字段进行枚举，范式化字段至少包括事件接收时间、用户名称、源地址、源端口、操作、目的地址、目的端口、对象、结果、持续时间、响应、归并条目、事件名称、事件内容摘要、事件分类、等级、原始等级、原始类型、产生时间、网络协议、网络应用协议、设备地址、设备名称、设备类型、程序名称、原始消息、厂商、产品、解析关联等字段，字段名称支持自定义。（提供截图证明）  100.支持日志加密压缩传输，支持加密压缩方式转发，加密方式支持SM4国密算法，支持定时转发。（提供截图证明）  101.支持对日志的过滤和合并；支持以秒、分钟、小时、天、周条件设定合并的时间范围。  102.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。  103.服务所涉及工具需具备《IT产品信息安全认证》、《信息技术产品安全测评证书》EAL3+级及以上级别，提供证书复印件。  104.服务所涉及工具需具备《IPv6认证证书》，提供证书复印件。 |
| **23** |  | 云统一监控平台服务 | 105.内置数据库版，包含统一展示、资产管理、告警管理、知识管理、报表管理、权限管理、系统管理功能，并提供网络拓扑自动发现与展示、机架拓扑等功能，以及对网络设备、安全设备、主机服务器的可用性与性能监控功能。该模块包括内置的本地性能采集器，用于采集各类设备及系统的性能信息。  106. 系统支持对性能及接口的数值指标设置上上限、上限、下限、下下限四项阈值，并分别采取不同的告警动作。（提供截图证明）  107.内置至少13类安全设备的监控，包括但不限于防火墙、IPS、IDS、WAF、VPN等，并支持通过自定义监控扩展监控类型。（提供截图证明）  108.支持显示链路的带宽、名称、轮询间隔、上下行流量、丢包率、带宽占用比等信息。（提供截图证明） |

**信息化设施设备质保清单**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **产品名称** | **品牌** | **规格型号** | **建设年份** | **单位** | **数量** | **备注** |
| 1 | 互联网入侵防御 | 网御 | V6000-P1320 | 2017年 | 台 | 1 |  |
| 2 | 互联网路由器 | 迈普 | MP7500 | 2014年 | 台 | 1 |  |
| 3 | 互联网流量控制 | 网康 | NI3200-50 | 2018年 | 台 | 1 |  |
| 4 | 互联网核心交换机 | 华为 | s5700 | 2017年 | 台 | 1 |  |
| 5 | 互联网服务器交换机 | 华为 | s5720s | 2018年 | 台 | 1 |  |
| 6 | 机房终端交换机 | 华为 | s2700 | 2014年 | 台 | 1 |  |
| 7 | 楼层汇聚交换机 | 华为 | S5700 | 2017年 | 台 | 1 |  |
| 8 | 楼层交换机 | 迈普 | s3220 | 2018年 | 台 | 7 |  |
| 9 | 互联网边界安全网关(VPN) | 网御星云 | v6030 | 2017年 | 台 | 2 |  |
| 10 | 终端安全管理 | 奇安信 | 360天擎终端安全管理系统V6.0 | 2018年 | 套 | 1 |  |
| 11 | 网闸（互联网、电子政务外网边界） | 网御 | Z4201 | 2015年 | 台 | 1 |  |
| 12 | 安全数据交换平台（互联网、电子政务外网边界） | 杭州合众 | DC-310 | 2018年 | 台 | 2 |  |
| 13 | 电子政务外网路由器 | 迈普 | MP7500 | 2014年 | 台 | 1 |  |
| 14 | 电子政务外网入侵防御 | 网御星云 | V6000-P3330 | 2015年 | 台 | 1 |  |
| 15 | 电子政务外网核心交换机 | 华为 | s5700 | 2018年 | 台 | 1 |  |
| 16 | 电子政务外网服务器群组防护 | 捷普 | S6300 | 2014年 | 台 | 1 |  |
| 17 | 电子政务外网网御-WAF | 网御 | Leadesc-7000WAF-S | 2018年 | 台 | 1 |  |
| 18 | 身份认证网关（国产） | 吉大正元 | SRJ1509-G | 2020年 | 台 | 7 | 新增 |
| 19 | 电子政务外网服务器交换机 | 迈普 | S6600 | 2012年 | 台 | 1 |  |
| 20 | 终端安全管理（国产） | 奇安信 | 网神终端安全管理系统V8.0 | 2020年 | 套 | 1 | 新增 |
| 21 | 网闸（政法专网、电子政务外网边界） | 网御 | Z2201 | 2014年 | 台 | 1 |  |
| 22 | 移动电子政务外网防火墙 | 启明 | USG-FW-2000D | 2013年 | 台 | 1 |  |
| 23 | 移动电子政务外网核心交换机 | 华为 | s2700 | 2014年 | 台 | 1 |  |
| 24 | 政法专网防火墙 | 网御 | V6000-NF2310 | 2017年 | 台 | 1 |  |
| 25 | 政法专网核心交换机 | 迈普 | S6600 | 2012年 | 台 | 1 |  |
| 26 | 政法专网安全网关 | 网御 | U7310 | 2014年 | 台 | 2 |  |
| 27 | 政法专网服务器交换机 | 华为 | S5720 | 2014年 | 台 | 2 |  |
| 28 | 政法专网楼层汇聚交换机 | 中兴 | ZXR10 5228 | 2014年 | 台 | 1 |  |
| 29 | 安全数据交换平台（政法专网、电子政务外网边界） | 杭州合众 | DC-310 | 2017年 | 台 | 2 |  |
| 30 | 安全数据交换平台（政法专网、政法共享平台边界） | 杭州合众 | DC-310 | 2015年 | 台 | 2 |  |
| 31 | 网闸（政法专网、政法共享平台边界） | 网御 | Z4201 | 2015年 | 台 | 1 |  |
| 32 | 机房空调 | 精密空调 | P1030FAPMS1R | 2011年 | 台 | 2 |  |
| 33 | 机房UPS | 易事特 | EA8960 | 2011年 | 台 | 2 |  |
| 34 | 机房监控 | 大华 | / | 2011年 | 套 | 1 |  |
| 35 | 机房气体灭火控制盘 | 营口山鹰 | XMP-YKS4372 | 2011年 | 套 | 1 |  |
| 36 | 机房动环监控 | 九能网络 | / | 2011年 | 套 | 1 |  |
| 37 | 机房KVM | 宏正KVM器 | KH2516a | 2011年 | 台 | 2 |  |
| 38 | 混音器 | audio-technica | AT-DMM828 | 2015年 | 台 | 1 |  |
| 39 | 数字处理器 | Symetrix | ZoneMix 761 | 2013年 | 台 | 1 |  |
| 40 | 拼控电视机 | VEWELL/唯瑞 | V46-S49B | 2013年 | 台 | 9 |  |
| 41 | 无线话筒接收器底座 | audio-technica | ATW-RC13 | 2019年 | 台 | 2 |  |
| 42 | 接收器 | audio-technica | ATW-RU13 | 2019年 | 个 | 4 |  |
| 43 | 无线话筒底座 | audio-technica | ATW-T1007 | 2019年 | 个 | 4 |  |
| 44 | 鹅颈会议话筒 | audio-technica | ES917aH | 2019年 | 支 | 4 |  |
| 45 | 智能混音器 | audio-technica | AT-MX341B | 2019年 | 套 | 1 |  |
| 46 | 中控主机 | GREATOR | / | 2010年 | 台 | 1 |  |
| 47 | 8路电源时序器 | TOPPPRO | M8000 | 2015年 | 台 | 1 |  |
| 48 | 数字处理器 | CLEARONE | SR1212 | 2015年 | 台 | 1 |  |
| 49 | 可移动高清电视 | sharp/夏普 | ZC371WJ | 2010年 | 台 | 2 |  |
| 50 | 高清壁挂电视 | LG | 42LK460-CC | 2010年 | 台 | 4 |  |
| 51 | 思科高清摄像头 | cisco/思科 | TTC8-20 | 2015年 | 台 | 1 |  |
| 52 | 高清摄像头 | Sony/索尼 | EVI-H100V | 2013年 | 只 | 2 |  |
| 53 | 摄像机 | Sony/索尼 | PMW-EX330K | 2013年 | 台 | 1 |  |
| 54 | 高清切换台 | Sony/索尼 | MCS-8M | 2013年 | 台 | 1 |  |
| 55 | 高清摄像头控制台 | Sony/索尼 | RM-BR300 | 2013年 | 台 | 1 |  |
| 56 | 液晶监视器 | 大华 | 43寸液晶监视器 | 2015年 | 台 | 1 |  |
| 57 | 消费机 | / | C6CN | 2015年 | 台 | 2 |  |
| 58 | 发卡机 | / | C6-SC | 2015年 | 台 | 1 |  |
| 59 | USB-IC发卡器 | 微耕 | WG1028 | 2015年 | 台 | 1 |  |
| 60 | 机箱电源 | 新爱 | 12V5A | 2015年 | 套 | 50 |  |
| 61 | 视频会议MCU | CISCO/思科 | 4515 | 2014年 | 台 | 1 |  |
| 62 | 高清视频会议终端 | CISCO/思科 | C40 | 2014年 | 台 | 3 |  |
| 63 | 高清录播服务器 | VMediaX/超然 | MRS | 2015年 | 台 | 2 |  |
| 64 | 室内红外高清网络半球 | 大华 | DH-IPC-HDW2225C | 2015年 | 台 | 63 |  |
| 65 | 室外红外高清网络枪机 | 大华 | DH-IPC-HFW2225B | 2015年 | 台 | 8 |  |
| 66 | 室外红外高清网络球机 | 大华 | DH-SD-6C82E-GN | 2015年 | 台 | 6 |  |
| 67 | POE供电交换机 | 丰润达 | PS1080 | 2015年 | 台 | 6 |  |
| 68 | POE供电交换机 | 丰润达 | PS1016G | 2015年 | 台 | 4 |  |
| 69 | 网络硬盘录像机 | 大华 | DH-NVR816-128 | 2015年 | 台 | 1 |  |
| 70 | 门禁控制器 | 微耕 | 四门篮板 | 2015年 | 套 | 100 |  |
| 71 | 门禁读卡器 | 微耕 | WG1060 | 2015年 | 台 | 150 |  |
| 72 | 单门磁力锁 | / | NBX-280KG | 2015年 | 套 | 130 |  |
| 73 | 双门磁力锁 | / | NBX-280KG | 2015年 | 套 | 40 |  |
| 注：如更换的设备涉及信息安全产品实施强制性认证、《网络关键设备和网络安全专用产品目录》的网络安全专用产品应当满足相关国家标准的强制性要求，供应商在更换前应提供相关信息安全产品强制认证证书、具备资格的机构安全认证或者安全检测合格证明。**（提供承诺函）** | | | | | | | |

**三、★商务要求**

**（1）履约时间（期限）**：合同签订生效后一年（具体生效时间以合同签订为准）。

**（2）履约地点**：四川省司法厅。

**（3）包装和运输**：本项目为服务项目，不涉及包装和运输。

**（4）付款条件（进度和方式）**：

4.1合同签订后采购人收到供应商开具的真实有效、合法、合同金额90%的等额发票及其他相关支付凭证材料之日起20个工作日内通过银行转账支付至合同金额的90%；

4.2服务考核完毕采购人收到供应商开具的真实有效、合法、合同金额10%的等额发票及其他相关支付凭证材料之日起20个工作日内通过银行转账支付尾款；

4.3若供应商未按采购人要求提供或迟延提供发票及相关支付凭证材料，则采购人有权延迟或拒绝支付合同相应款项且不承担任何违约责任 。

**（5）验收、交付标准和方法**：服务期满9个月后开始组织考核。

5.1考核办法细则：

5.1.1采购人组织年度考核，按照《质量考核评分表》对供应商的服务进行考核。

5.1.2考评等次分为：合格（80分及以上）、不合格（80分以下）。

5.1.3考核结果的运用：以年度考评结果为依据，如供应商年度考核不合格，采购人有权扣除合同总金额5%的违约金，并由供应商承担违约责任。

**质量考核评分表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 一、人员驻场服务（共38分） | | | | |
| 项目 | 序号 | 考评内容 | 考评总分 | 评分标准 |
| 计算机信息系统运维及驻场服务 | 1 | 安排驻守人员1人，主要负责维护机房、楼层弱电间的网络安全设备台、服务器台（含国产服务器台），计算机终端约台、复印打印设备约台、电话台，按要求驻场运维，提交月运维报告。 | 10 | 未按时提交或不符合要求的，每次扣1分。 |
| 指挥中心运维及驻场服务 | 2 | 安排驻守人员1人，主要对指挥中心所涉及的监控平台、点名系统、视频会议系统、大屏显示系统等进行管理和维护。根据司法部、省政法委及司法厅的指挥调度的需求，熟悉使用系统，完成系统操作，并开展视频上传日常性检查和指挥中心设备维护。按要求驻场运维，提交月运维报告。 | 10 | 未按时提交或不符合要求的，每次扣1分。 |
| 视频会议系统、门禁安防系统运维及驻场服务 | 3 | 安排驻守人员1人，主要保障3个音视频会议室的本地会议、全国视频会议、全省视频会议及门禁安防系统正常运行。按要求驻场运维，提交月运维报告。 | 10 | 未按时提交或不符合要求的，每次扣1分。 |
| 设备质保服务 | 4 | 按要求提供设备质保。 | 8 | 未按甲方要求做好相关工作每次扣1分。 |
| 二、网络安全专项服务（共30分） | | | | |
| 项目 | 序号 | 考评内容 | 考评总分 | 评分标准 |
| 资产梳理服务 | 5 | 乙方对甲方信息系统资产进行梳理，对甲方现有互联网和内网资产进行有效识别，通过对资产的识别收敛，将甲方现有所有资产纳入资产管理台账，便于甲方全面掌握资产的安全信息，为后续检查、评估奠定基础，从而一定程度上降低系统被攻击的可能 | 2 | 服务结束后向甲方提交《资产梳理报告》，未按要求提供报告扣2分。 |
| 网络安全专项检查服务 | 6 | 乙方对所发现的安全漏洞及安全风险，提出整改建议，并协助单位完成整改。 | 2 | 提供整改建议，未按要求提供扣2分。 |
| 网络架构风险评估服务 | 7 | 乙方通过对甲方整个组织的网络体系进行深入调研，全面对网络架构安全性进行检查分析，从整体结构合理性、设计与实际符合性与优化调整给出评估建议。 | 2 | 提供评估建议，未按要求提供扣2分。 |
| 敏感信息排查服务 | 8 | 按要求提供服务。 | 2 | 未按甲方要求做好相关工作每次扣1分。 |
| 威胁建模服务 | 9 | 按要求提供服务。 | 2 | 未按甲方要求做好相关工作每次扣1分。 |
| 红队测试服务 | 10 | 按要求提供服务。 | 2 | 未按甲方要求做好相关工作每次扣1分。 |
| 外网安全监测 | 11 | 按要求提供服务。 | 2 | 未按甲方要求做好相关工作每次扣1分。 |
| 内网安全监测 | 12 | 按要求提供服务。 | 2 | 未按甲方要求做好相关工作每次扣1分。 |
| 安全专家值守 | 13 | 在防守期间乙方提供安全专家值守，每天现场值守人数不低于4人，服务期内总服务天数不低于60天。  提供整体加固修复方案。必要时，乙方配合第三方安全服务机构进行安全应急响应服务。安全值守期间，根据单位的要求，定期向甲方提交《安全值守报告》。同时完全按照要求提供服务。 | 2 | 未按甲方要求做好相关工作每次扣1分。  未按要求提供安全专家值守扣0.5分。  未按时提供《安全值守报告》，扣0.5分。 |
| 威胁情报共享服务 | 14 | 按要求提供服务。 | 2 | 未按甲方要求做好相关工作每次扣1分。 |
| 攻击诱捕与反制服务 | 15 | 按要求提供服务。 | 2 | 未按甲方要求做好相关工作每次扣1分。 |
| 防守工作复盘及总结 | 16 | 按要求提供服务。同时防守工作复盘及总结结束后向甲方提交《总结分析报告》。 | 2 | 未按甲方要求做好相关工作每次扣1分。  未按时提交《总结分析报告》扣1分。 |
| 安全优化整改建议 | 17 | 乙方针对防守工作中出现的安全风险及安全事件进行分析，对甲方现有防护体系进行调整和优化，提出整改建议，形成整改方案。向甲方提交《安全优化整改建议报告》。 | 2 | 提供整改建议，未按要求提供扣2分。 |
| 提供技术培训服务 | 18 | 按技术要求提供服务。  在甲方指定时间和地点至少安排1次培训，总培训时长不低于6小时。培训结束向甲方提交《技术培训报告》。 | 2 | 未按甲方要求做好相关工作每次扣1分。  未按要求提供培训服务每次扣0.5分。  未按要求提供《技术培训报告》扣0.5分。 |
| 服务工具 | 19 | 未按时提供符合要求的服务工具 | 2 | 未按时提供服务工具扣2分。 |
| 三、政务云信息安全集成实施服务（共32分） | | | | |
| 项目 | 序号 | 考评内容 | 考评总分 | 评分标准 |
| 云堡垒机防护服务 | 20 | 详见云堡垒机防护服务要求 | 8 | 未按时提供符合要求的服务工具扣8分。 |
| 云数据库审计防护服务 | 21 | 详见云数据库审计防护服务要求 | 8 | 未按时提供符合要求的服务工具扣8分。 |
| 云日志审计防护服务 | 22 | 详见云日志审计防护服务要求。 | 8 | 未按时提供符合要求的服务工具扣8分。 |
| 云统一监控平台服务 | 23 | 详见云统一监控平台服务要求 | 8 | 未按时提供符合要求的服务工具扣8分。 |

**（6）服务响应**：驻场人员应立即响应，并提供7\*24小时响应服务。

**（7）保险**：供应商应按照相关规定为本项目所有工作人员购买社会保险，履约期间供应商工作人员因差旅、调查等发生意外伤害的，均由供应商负责。

**（8）责任与解决争议的方法**：

1.如因成交供应商在履行职务过程中的疏忽、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，成交供应商对此均应承担全部的赔偿责任。

2.成交供应商提供的服务不符合采购文件、响应文件或本合同规定的，每出现一次违约（合同涉及“日期”和“天数”的，每逾期一天或少一天，视为一次违约），供应商须向采购人支付本合同总价1%的违约金并且按采购人要求进行整改，出现违约3次以上或未按采购人要求整改的，采购人有权无条件解除本合同并要求供应商退还已收取的费用。

3.采购人无正当理由逾期未按照合同约定付款的，则每日按未付款金额的5‰向供应商偿付违约金，但累计违约金总额不超过未付款总额的1％。

**（9）知识产权**：供应商所提供的服务或其任何一部分均不会侵犯任何第三方的专利权、商标权、著作权或其他合法权益，否则视为供应商违约，由此产生的一切损失由供应商承担；采购人享有本项目实施过程中产生的知识成果及知识产权，未经采购人书面允许供应商不得另做他用。

**（10）保密要求**：供应商应对项目实施过程及实施过程中获取的所有相关数据、信息、企业资料、研究成果等材料保密，未经采购人书面允许，不得以任意形式传播或泄露相关信息。 **（提供承诺函）**

**注：本项目标注“★”条款均为实质性要求，不允许负偏离，否则视为无效投标。**