|  |  |  |
| --- | --- | --- |
| 参数性质 | 序号 | 技术参数与性能指标 |
|  | 1 | 服务范围1.重要信息系统网络安全运维（1）对高速公路联网收费省级中心系统、高速公路网综合监控省级中心系统进行专业安全检测和排查整改；对陕西省高速公路省级视频云联网监测系统、陕西交通服务热线12122系统、陕西12328交通运输服务监督电话系统进行专业安全检测，并对安全设备（详见维护清单）问题进行整改。（2）对高速公路联网收费省级中心系统、高速公路网综合监控省级中心系统、陕西省高速公路省级视频云联网监测系统、陕西交通服务热线12122系统4个系统的安全设备（详见维护清单）进行日常安全运维服务。2.安全设备特征库升级。对高速公路联网收费省级中心系统、高速公路网综合监控省级中心系统、陕西省高速公路省级视频云联网监测系统、陕西交通服务热线12122系统4个系统进行1年授权升级，确保安全设备特征库更新至最新版本。3.高速公路联网收费省级中心系统和ETC发行服务系统数据异地备份。对系统数据进行异地备份，确保系统遭受攻击或损坏时，能尽快恢复数据，将业务损失降至最低。（三）服务依据1.《中华人民共和国网络安全法》（[中华人民共和国主席令第53号](https://baike.baidu.com/item/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E4%B8%BB%E5%B8%AD%E4%BB%A4%EF%BC%88%E7%AC%AC%E4%BA%94%E5%8D%81%E4%B8%89%E5%8F%B7%EF%BC%89/23119921%22%20%5Ct%20%22https%3A//baike.baidu.com/item/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E7%BD%91%E7%BB%9C%E5%AE%89%E5%85%A8%E6%B3%95/_blank)）2.《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）3.《收费公路联网收费系统网络安全管理暂行办法》（交科技发〔2019〕86号）4.《陕西省交通运输厅网络安全管理暂行办法》（陕交发〔2019〕12号）5.《陕西省高速公路联网收费系统网络安全总体方案》（陕交发〔2019〕88号）二、服务内容（一）重要信息系统网络安全运维为保障中心重要信息系统安全、稳定运行，按照国家信息安全等级保护制度要求，依据部、省相关信息安全政策、技术标准及安全文件要求，结合系统业务实际情况及安全现状，对中心重要信息系统提供安全运维服务。1.专业安全服务（1）漏洞扫描每季度定期采用漏洞扫描工具，完成对系统的网络设备、安全设备、服务器、虚拟化主机、终端设备等资产的安全扫描工作，并根据扫描结果形成漏洞跟进表，协助中心完成安全漏洞整改，并根据扫描结果进行分析，每季度提供一份系统安全扫描报告。（2）渗透测试应通过现场结合远程的方式，模拟黑客从外网、内网对系统开展至少1次渗透测试工作，测试完毕生成详细的渗透测试报告，并提供改进建议。实施人员需熟练掌握渗透测试技能，具备丰富的渗透测试经验，渗透测试过程中不得进行影响业务系统稳定运行的操作。（3）完善配置通过配置检查工具或人工的方式对系统安全设备、服务器、终端电脑等设备的安全配置进行核查，及时发现不合理、不安全的安全配置，持续完善安全配置，加固整改系统安全隐患。（4）系统上线安全检测服务系统若有增加、升级新的业务功能等，应在功能上线前进行安全检测，检测内容包括漏洞扫描、配置核查等，出具相应上线安全检测报告，并协助完成整改。（5）App（公众号、小程序）安全评估应对服务系统现有APP（公众号、小程序等）及新增APP（公众号、小程序等）应用进行安全扫描、检测，有效评估APP中存在的安全隐患，测试完毕应生成APP（公众号、小程序等）应用安全检测报告。实施人员需熟练掌握移动APP（公众号、小程序等）的测试技能，应具有针对各类APP（公众号、小程序等）进行安全评估的丰富经验，安全评估过程中不得进行影响业务系统稳定运行的操作。（6）应急处置（含重要活动护网工作）应针对系统制定应急响应快速服务流程，包括设备故障响应和安全事件响应。日常故障或一般事件4小时内响应处置，重大故障或重大事件以上2小时响应处置。在发生安全事件时，应提供安全技术团队对事件进行分析研判，采取应急措施保障业务正常运行，并协助中心快速协调相关厂家解决设备故障问题。重大会议、重大活动、节假日及专项护网期间，加强值班值守，强化安全防护措施，采取技术手段监测网络安全状况，严防网络安全攻击行为。（7）安全演练包括但不限于应急演练或攻防演练（攻击测试），制定网络安全演练方案，协助开展网络安全演练活动。根据演练活动结果，完善应急措施，服务期内提供不少于一次网络安全演练活动，并保留安全演练记录。（8）安全检查供应商应配合中心完成不少于1次的网络安全检查服务，及时发现网络安全管理落实及安全技术实施中存在的不足及风险，出具安全检查报告，对检查中发现的完全问题，应给出合理的安全整改建议。本项要求安全实施人员至少2名工程师（具体人员配备按照实际抽检工作量予以增加），且需理解高速公路联网系统安全规范、检查要求。（9）安全培训对系统安全运维人员和安全管理人员进行网络安全培训，完成网络安全政策宣贯，提高网络安全意识，提升网络安全技能。培训包括全省联网系统网络安全培训和中心1人次CISP DSG认证培训，同时应保障已获得证书的有效延续认证，确保长期有效。全省联网系统网络安全培训总时间2天，参加人员不少于50人不多于100人，应制定有针对性的信息安全培训教材，明确培训课程，讲授安排。本次培训服务费用含讲课费、教室租用、教材、食宿。中心1人次CISP DSG认证培训，包含教材、培训费、考试费、食宿等所有由于培训产生的费用。2.日常安全运维服务日常安全维护工作主要包括以下4个方面：（1）安全巡检对系统安全设备进行现场安全巡检，及时了解安全设备运行情况，观察各个安全节点的可靠性。机房巡检每日2次，线上巡检每日1次（即设备管理平台状态检查），遇重要活动或会议期间要加大巡检频次，并提供巡检日报。对巡检中发现的安全问题或异常情况，应及时报告中心有关人员，不得擅自处理，并协助中心对问题进行整改。（2）信息资产台账维护定期维护更新安全设备资产台账，包括资产类别、型号、用途、位置、端口使用状态、责任归属等。并重点记录资产在遭受泄密、中断、损害等破坏时所遭受的影响，以及后续状态。（3）安全运行监测充分利用现有安全运行监测平台或借助第三方运行监测平台，对中心部署的防火墙、网闸、日志审计系统、堡垒机、漏洞扫描、防病毒系统等安全设备（软件）运行状况进行监测，及时发现安全异常情况。对服务期限内新增的系统安全设备，也应做好安全运行监测工作。（4）其它安全信息服务应在安全技术团队保障的基础上，协助编制（修订）全省和中心相关网络安全管理制度、安全检查（通报）、安全技术要求、专项方案等相关文件。应梳理现有网络安全配置策略，针对服务中出现的问题，提交本年度安全运行分析报告，提出安全管理及技术方面需要完善的意见建议，包括但不限于整体系统架构的可靠性、冗余性、安全性、可扩展性方面，同时规划下一年度的安全完善计划。3.服务报告要求本服务项目的交付物包含但不限于以下内容：《日巡检安全报告》《月度风险分析报告》《季度漏洞扫描报告》《重要时段护网总结报告》《渗透测试报告》《安全演练报告》《安全检查报告》《安全培训报告》《年度安全运行分析报告》其他需要的报告或者材料。4.重要信息系统网络安全运维服务维护清单如下：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 系统名称 | 类别 | 设备名称 | 数量 | 单位 |
| 1 | 高速公路联网收费省级中心系统 | 硬件 | 部省交互区防火墙 | 1 | 台 |
| 2 | 发行业务交互防火墙 | 1 | 台 |
| 3 | 安全管理区防火墙 | 1 | 台 |
| 4 | 支撑平台防火墙 | 2 | 台 |
| 5 | 路网接入防火墙 | 2 | 台 |
| 6 | 服务器区防火墙 | 2 | 台 |
| 7 | 第三方接入防火墙 | 1 | 台 |
| 8 | 站部防火墙 | 1 | 台 |
| 9 | 数据库防火墙 | 1 | 台 |
| 10 | 普通公路防火墙 | 1 | 台 |
| 11 | 普通公路VPN | 2 | 台 |
| 12 | 部省交互防病毒网关 | 2 | 台 |
| 13 | 堡垒机 | 1 | 台 |
| 14 | 网络准入控制 | 1 | 台 |
| 15 | 安全漏洞扫描 | 1 | 台 |
| 16 | 普通公路入侵防御 | 1 | 台 |
| 17 | 软硬一体 | 内网安全管理系统 | 1 | 套 |
| 18 | 日志收集与审计 | 1 | 套 |
| 19 | 数据库安全审计系统 | 1 | 套 |
| 20 | 网络安全态势感知平台 | 1 | 套 |
| 21 | 软件 | 防病毒系统 | 1 | 套 |
| 22 | 高速公路网综合监控省级中心系统 | 硬件 | 路网边界防火墙 | 1 | 台 |
| 23 | 业务区防火墙 | 2 | 台 |
| 24 | 安全管理区防火墙 | 1 | 台 |
| 25 | 互联网防火墙 | 1 | 台 |
| 26 | 专网接入防火墙 | 1 | 台 |
| 27 | 网闸 | 2 | 台 |
| 28 | 堡垒机 | 1 | 台 |
| 29 | 安全漏洞扫描 | 1 | 台 |
| 30 | 网络准入控制 | 1 | 台 |
| 31 | 入侵检测 | 1 | 台 |
| 32 | RA网关 | 1 | 台 |
| 33 | PKI加密机 | 1 | 台 |
| 34 | 数字签名系统 | 1 | 台 |
| 35 | 软硬一体 | 日志收集与审计 | 1 | 套 |
| 36 | 软件 | 防病毒系统 | 1 | 套 |
| 37 | 证书接入系统RA | 1 | 套 |
| 38 | 陕西省高速公路省级视频云联网监测系统 | 硬件 | 视频上云防火墙 | 2 | 台 |
| 39 | 陕西交通服务热线12122系统 | 硬件 | 网闸 | 1 | 台 |
| 40 | 防火墙 | 1 | 台 |
| 41 | WEB应用防护系统 | 1 | 台 |

（二）安全设备特征库升级按照国家信息安全等级保护制度要求，依据部、省相关信息安全政策、技术标准及安全文件要求，结合系统业务实际情况及安全现状，对高速公路联网收费省级中心系统、高速公路网综合监控省级中心系统、陕西省高速公路省级视频云联网监测系统、陕西交通服务热线12122系统4个系统购买1年升级授权服务。1.服务要求。服务期内需每周进行防病毒系统升级，其余安全设备特征库需每月进行设备特征库升级，如遇重要时段（重要节假日、重大活动等）或当有新型蠕虫、病毒、漏洞等范围性安全事件发生时，也需及时进行设备特征库升级，确保及时更新至最新版本，安全策略有效，期间不能收取任何费用。本次安全设备特征库升级清单如下：

| 序号 | 系统名称 | 品牌 | 产品名称 | 待升级数量 | 单位 |
| --- | --- | --- | --- | --- | --- |
| 1 | 高速公路联网收费省级中心系统 | 天融信 | 防火墙 | 8 | 台 |
| 2 | 网御星云 | 入侵防御 | 1 | 台 |
| 3 | 启明星辰 | 防火墙 | 2 | 台 |
| 4 | 绿盟 | 安全漏洞扫描 | 1 | 台 |
| 5 | 亚信 | 防病毒网关 | 2 | 台 |
| 6 | 防病毒系统 | 1 | 套 |
| 7 | 安恒 | 态势感知平台 | 1 | 套 |
| 8 | 高速公路网综合监控省级中心系统 | 天融信 | 防火墙 | 1 | 台 |
| 9 | 迪普 | 防火墙 | 5 | 台 |
| 10 | 安全漏洞扫描 | 1 | 台 |
| 11 | 奇安信天擎终端安全管理系统V10.0 | 防病毒系统 | 1 | 套 |
| 12 | 陕西省高速公路省级视频云联网监测系统 | 奇安信 | 防火墙 | 2 | 台 |
| 13 | 奇安信天擎终端安全管理系统V10.0 | 防病毒系统 | 1 | 套 |
| 14 | 陕西交通服务热线12122系统 | 深信服 | 防火墙 | 1 | 台 |
| 15 | 绿盟 | WEB应用防护系统 | 1 | 台 |

2.服务报告要求本服务项目的交付物包含但不限于以下内容：《授权升级报告》《月度升级服务报告》《年度升级总结报告》（三）联网收费省级中心系统数据异地备份服务高速公路联网收费省级中心系统业务复杂、结构化数据量大，供应商应充分理解现网情况，对系统业务架构、数据情况、安全等级等理解清晰后提供异地数据备份技术服务。供应商应提供一整套系统核心数据库异地数据热备份所需的软硬件环境（包括机房设施等），在有效保护原有已备份到异地的历史数据安全的同时，对核心业务的新增数据库实例进行实时的异地数据备份、数据保护、数据恢复功能。数据异地备份服务允许供应商租用其它第三方机房及线路。1.配置要求（1）硬件备份资源（非国产或国产配置要求满足其中一种即可）非国产配置要求：机架式2U高度；Intel 8核CPU，处理器主频≥2.1GHz；内存≥32G,≥16个内存槽位；240G 2.5寸企业级SSD系统硬盘≥2；数据盘可用存储空间不小于180TB；板载Inteli350双千兆网口；RAID级别：0，1，5，10，50，2GB缓存；冗余电源和风扇模块。国产配置要求：机架式2U高度；国产 16核CPU，处理器主频≥2.1GHz；内存≥64G,≥16个内存槽位；240G 2.5寸企业级SSD系统硬盘≥2；数据盘可用存储空间不小于180TB；万兆光接口≥2，万兆多模光模块≥2；RAID级别：0，1，5，10，50，2GB缓存；冗余电源和风扇模块。必须保证所有历史数据及本服务期内新增数据的完整性和一致性，若存储空间需要扩容以满足数据备份存储，供应商应及时进行扩充，不得影响数据备份，中心无需额外支付费用。（2）备份软件要求在有效保护原有已备份到异地机房的历史数据安全的同时，能从已建成的本地平台中提取数据并对核心业务的新增数据库实例进行实时的异地数据备份、数据保护、数据恢复功能。要求不通过RMAN进行全库增量数据扫描，具备自动记录增量数据变化的功能，减少备份时对生产数据库的影响。具备Oracle数据库的非归档模式的在线热备功能。具备Oracle数据库全库、单表、表空间、文件、数据块、存储过程、对象、索引、函数的恢复。2.线路及机房租赁服务（1）机房要求距离中心大于200公里专业化运营商级别机房，提供不少于两路市电冗余输入，配置N+1冗余备份UPS系统，满足系统容量放电30分钟，具备发电机组，可支持机组满载运行大于24小时。（2）线路要求联网收费省级中心系统数据备份服务为中心机房和异地数据备份机房之间不少于100Mbps的MSTP专线一条。确保数据通过该链路高质量、实时传输至异地数据节点。（3）接入设备业务内所需的安装线缆、接入设备等由供应商免费提供，并保障服务期内免费维修或更换。3.数据恢复演练服务应设计系统数据备份和恢复演练预案，制定数据备份和恢复策略、备份程序和恢复程序，制定相关的操作手册。每年度提供不少于一次数据恢复演练服务，确保数据的完整性和一致性。演练结束后，对演练结果进行评估，并进一步完善数据备份和恢复演练方案。4.运维保障服务（1）异地节点定期巡检每季度安排厂家工程师对异地节点提供至少一次定期巡检服务，内容包括数据备份状态分析、系统健康状态分析、系统日志分析、系统诊断、性能分析等，梳理系统运行隐患、优化系统配置，提供系统运行报告。同时提供异地节点现场技术支持响应服务，当异地节点软硬件系统发生故障时，工程师须第一时间（4小时内）赶赴现场处理故障，对系统故障进行定位、排查和解决。（2）运行监测在服务期内，每日需对异地备份系统软硬件备份状态进行监测，检查系统运行状况、报警信息等，对系统出现的异常现象及时联系厂家处理。每周1次需从异地备份系统随机抽取若干张表或日志文件进行数据恢复，将异地恢复的数据与生产数据进行对比验证，确保数据完整备份至异地、本地和异地数据一致，异地数据具有可用性。服务期每季度末，应提供系统运行报告。供应商应定期监测备份空间使用情况，当剩余存储空间小于10TB时，应及时向采购人报告情况，制定磁盘扩容方案，于发现问题的5个工作日内完成磁盘扩容，不得影响数据备份，采购人无需额外支付费用。5.服务报告要求本服务项目的交付物包含但不限于以下内容：《日监测报告》《周巡检报告》《周数据恢复演练报告》《季度系统运行报告》《数据恢复演练预案及报告》《年度报告》其他需要的报告或者材料。（四）ETC发行服务系统数据异地备份服务ETC发行服务系统业务复杂、结构化数据量大，供应商应充分理解现网情况，对系统业务架构、数据情况、安全等级等理解清晰后提供异地数据备份技术服务。供应商应提供一整套系统核心数据库异地数据热备份所需的软硬件环境（包括机房设施等），在有效保护原有已备份到异地的历史数据安全的同时，对核心业务的新增数据库实例进行实时的异地数据备份、数据保护、数据恢复功能。数据异地备份服务允许供应商租用其它第三方机房及线路。1.配置要求（1）硬件备份资源（非国产或国产配置要求满足其中一种即可）非国产配置要求：机架式2U高度；Intel 8核CPU，处理器主频≥2.1GHz；内存≥32G,≥16个内存槽位；240G 2.5寸企业级SSD系统硬盘≥2；数据盘可用存储空间不小于180TB；板载Inteli350双千兆网口；RAID级别：0，1，5，10，50，2GB缓存；冗余电源和风扇模块。国产配置要求：机架式2U高度；国产 16核CPU，处理器主频≥2.1GHz；内存≥64G,≥16个内存槽位；240G 2.5寸企业级SSD系统硬盘≥2；数据盘可用存储空间不小于180TB；万兆光接口≥2，万兆多模光模块≥2；RAID级别：0，1，5，10，50，2GB缓存；冗余电源和风扇模块。必须保证所有历史数据及本服务期内新增数据的完整性和一致性，若存储空间需要扩容以满足数据备份存储，供应商应及时进行扩充，不得影响数据备份，中心无需额外支付费用。（2）备份软件要求在有效保护原有已备份到异地机房的历史数据安全的同时，能从已建成的本地平台中提取数据并对核心业务的新增数据库实例进行实时的异地数据备份、数据保护、数据恢复功能。要求不通过RMAN进行全库增量数据扫描，具备自动记录增量数据变化的功能，减少备份时对生产数据库的影响。具备Oracle数据库的非归档模式的在线热备功能。具备Oracle数据库全库、单表、表空间、文件、数据块、存储过程、对象、索引、函数的恢复。2.线路及机房租赁服务（1）机房要求距离中心大于200公里专业化运营商级别机房，提供不少于两路市电冗余输入，配置N+1冗余备份UPS系统，满足系统容量放电30分钟，具备发电机组，可支持机组满载运行大于24小时。（2）线路要求ETC发行服务系统数据备份服务为中心机房和异地数据备份机房之间不少于50Mbps的MSTP专线一条。确保数据通过该链路高质量、实时传输至异地数据节点。（3）接入设备业务内所需的安装线缆、接入设备等由供应商免费提供，并保障服务期内免费维修或更换。3.数据恢复演练服务应设计系统数据备份和恢复演练预案，制定数据备份和恢复策略、备份程序和恢复程序，制定相关的操作手册。每年度提供不少于一次数据恢复演练服务，确保数据的完整性和一致性。演练结束后，对演练结果进行评估，并进一步完善数据备份和恢复演练方案。4.运维保障服务（1）异地节点定期巡检每季度安排厂家工程师对异地节点提供至少一次定期巡检服务，内容包括数据备份状态分析、系统健康状态分析、系统日志分析、系统诊断、性能分析等，梳理系统运行隐患、优化系统配置，提供系统运行报告。同时提供异地节点现场技术支持响应服务，当异地节点软硬件系统发生故障时，工程师须第一时间（4小时内）赶赴现场处理故障，对系统故障进行定位、排查和解决。（2）运行监测在服务期内，每日需对异地备份系统软硬件备份状态进行监测，检查系统运行状况、报警信息等，对系统出现的异常现象及时联系厂家处理。每周1次需从异地备份系统随机抽取若干张表或日志文件进行数据恢复，将异地恢复的数据与生产数据进行对比验证，确保数据完整备份至异地、本地和异地数据一致，异地数据具有可用性。服务期每季度末，应提供系统运行报告。供应商应定期监测备份空间使用情况，当剩余存储空间小于10TB时，应及时向采购人报告情况，制定磁盘扩容方案，于发现问题的5个工作日内完成磁盘扩容，不得影响数据备份，采购人无需额外支付费用。5.服务报告要求本服务项目的交付物包含但不限于以下内容：《日监测报告》《周巡检报告》《周数据恢复演练报告》《季度系统运行报告》《数据恢复演练预案及报告》《年度报告》其他需要的报告或者材料。 |