# 采购内容及要求

**一、项目概况**

为保障新区智慧城市建设中各信息系统的稳定运行，满足国家网络安全基本要求，建立西咸新区网络安全态势感知体系。本服务涵盖范围为西咸新区智慧城市建设的各信息化系统提供整体安全数据采集和监控分析。通过项目持续的运营服务，保证新区智慧城市的各信息化系统网络安全事件的及时发现和处置，推动西咸新区整体网络安全平稳运行。项目包含新区一体化云平台机房、西咸大厦、创新大厦、艺墅大厦、产投大厦等范围。

**二、服务内容**

本次网络安全运营服务主要由各专项服务组成，服务中涉及一套运营管理平台、一套态势感知系统、硬件探针设备和一套舆情监控系统由本项目供应商提供，本项目具体工作包括但不限于以下服务内容：网络安全数据分析服务、网络安全检查服务、网络安全风险评估服务、网络安全应急演练服务、网络安全攻防演练服务、网络安全渗透测试服务、网络安全重要时期保障服务、网络安全防护服务、网络安全设备策略梳理及更新服务、网络安全风险报告服务、网络安全事件通报处置服务、网络安全应急响应服务、网络安全培训服务、网络安全咨询服务、网络安全可视化展示服务、网络安全舆情监控服务、网络安全知识库管理服务、网络安全现场值守服务等，详见下表：

| **序号** | **功能模块** | **具体服务** | **平台安全运营服务点介绍** | **备注** |
| --- | --- | --- | --- | --- |
| 1 | 现场值守服务 | 一体化云平台安全监测 | 1. 现场部署运营管理平台一套，平台功能满足：
2. 信息系统管理，对新区新城各单位信息系统及资产进行实时管理；
3. 网络安全预警通报，对接省级平台，展示新区安全事件整体态势，安全预警及安全事件在线处置办理；
4. 日常运维管理，具备安全设备管理、运维巡检、网站监测、重保值守等运营能力；
5. 网络安全知识库，包含规章制度、应急处置办法，漏洞信息库，安全知识库，热点信息库等；
6. 网络安全考核，可在平台进行网络安全检查和考核，可在线考试、答题学习；
7. 网络安全态势，可对全网安全进行可视，帮助用户看清业务、看到威胁、看懂风险，并辅助用户决策等功能。

2.驻场服务（7\*24h）：提供并现场部署态势感知系统、上述运营管理平台，梳理新区一体化云中心信息化资产信息并形成系统台账、对信息化资产进行系统归档；负责态势感知系统、运营管理平台的代码级运维、需求定制、系统开发等服务，日常平台升级、故障处理、告警处理、平台日常运维工作等，保障平台正常稳定运行；负责新区一体化云平台现场安全告警处置、日志信息监测，态势感知系统运维、探针设备及各信息安全设备运维。 |  |
| 2 | 通报处置 | 事件通报及处置 | 全年7\*24小时协助新区处理新区一体化云平台安全事件的通报和处置，通过运营管理平台进行新区辖区内预警、风险、事件通报下发，对安全事件处置进行闭环管理。运营管理平台需与陕西省网络安全协调指挥平台进行级联对接，实现与上级平台的互联互通，新区级重大风险、事件上报至省级。 | 需提供运营管理平台功能截图证明1 |
| 3 | 安全扫描 | 安全扫描服务 | 每月扫描新区一体化云平台服务器以及其他网络设备和安全设备，寻找安全漏洞（每年扫描不少于12次）。 |  |
| 4 | 弱口令专项检查 | 弱口令检查 | 检查新区一体化云平台上各业务系统存在的弱口令隐患，提供每月检查和复查报告。 |  |
| 5 | 信息安全风险评估 | 风险情况评估 | 全年2次，对新区一体化云平台现有的网络、系统、应用等资产进行全面的安全评估，出具风险评估报告，通过运营管理平台进行评估结果上传以及在线流转,配合新区完成风险内容的整改,对整改结果进行闭环管理。 |  |
| 6 | 安全演练 | 应急演练 | 全年2次，编制信息安全、网络安全应急演练预案和计划,进行应急演练环境的搭建，配合新区组织开展应急演练工作。通过运营管理平台，对在线知识库进行预案维护管理。 |  |
| 7 | 安全培训 | 安全意识及技术培训，培训考核及题库维护 | 全年开展4次安全意识及安全技术培训,通过运营管理平台进行培训考核、统计管理等内容，对题库试题进行定期维护和更新，以保证试题的质量和时效性，培训提供宣传资料及教材。 | 需提供运营管理平台功能截图证明2 |
| 8 | 安全报告 | 安全工作报告及处置报告 | 总结分析新区一体化云平台安全数据，通过运营管理平台统一管理、在线查看预览，包括项目月报、工作周报、工作日报、网络安全态势分析研判报告（月度）、人工智能和数据领域风险研判报告、业务系统安全监测月报等。 | 需提供运营管理平台功能截图证明3 |
| 9 | 安全策略梳理 | 设备技术策略梳理及更新（硬件设备更新） | 协助建立新区一体化云平台资产台账（安全设备），整理所有设备网络安全技术策略档案（第三方单位托管设备除外），每月定期优化维护安全防护及检测策略，更新相关库特征及白名单策略，保证相关信息安全监测及防护设备为最新版本（设备在厂商免费升级服务期内），并对安全设备协助开展策略配置调优。 |  |
| 10 | 渗透测试 | 渗透测试 | 对新区辖区范围网站及业务系统、新区一体化云平台部署的业务系统全年进行2轮渗透测试；并将漏洞风险通过运营管理平台完成通报下发、修复验证反馈，实现阶段时间内漏洞风险及漏洞整改情况的统计分析。 | 需提供运营管理平台功能截图证明4 |
| 11 | 重大节假日及关键时期保障 | 重保工作 | 编写各重要时期安全保障方案及总结报告，进行重保安全检查，协助各业务系统做好安全加固工作。重保期间通过运营管理平台对各单位网站、应用系统进行重保实时监测。 | 需提供运营管理平台功能截图证明5 |
| 12 | 应急响应 | 应急响应 | 为新区提供7\*24小时紧急安全事件技术支持服务，根据安全事件的严重程度，迅速组织相应等级的应急响应团队进行处置，确保平均5分钟内响应，对于重大事件30分钟内有效遏制其扩散，并实现100%的闭环处理率，尽力减轻安全事件对新区业务造成的影响，具体服务内容包括：1.现场技术支持服务：一旦遭遇紧急安全事件，立即派遣经验丰富的专业技术人员前往现场，迅速进行故障诊断、处理及系统恢复工作，确保问题得到及时、有效的解决。2.远程技术支持服务：若现场技术人员在处置过程中遇到难以解决的问题或专业知识不足，提供远程技术支持服务。可通过电话、视频通话或在线聊天等方式，即时接入高级工程师团队，获取专业的技术指导和支持。 |  |
| 13 | 系统上线检测 | 系统上线检测 | 对接入新区一体化云平台的新上线系统进行安全检测评估，编写安全评估报告，并提供技术支持。 |  |
| 14 | 安全咨询 | 安全咨询 | 对新区各单位、新城、街道及系统第三方厂家提供网络安全技术咨询服务。 |  |
| 15 | 攻防演练 | 攻防演练 | 根据公安、网信部门组织参加攻防演练并完成演练后的工作报告总结等。 |  |
| 16 | 数据分析服务 | 开展数据分析服务 | 开展数据采集、治理、融合、事件分析服务。 |  |
| 17 | 可视化展示 | 整体安全态势可视化展示 | 对安全态势可视化展示大屏重要数据进行维护，对整体资产进行补充，展示威胁态势变化，更新涉及新区安全数据；与西咸新区城市运行综合管理中心系统进行对接，完成大屏展示安全态势数据推送；根据可视化展示需求进行数据接口的定制开发。 |  |
| 18 | 知识库 | 知识库服务 | 建立新区一体化云平台资产、威胁、事件、漏洞、通报和安全模型知识库服务，通过运营管理平台对知识库进行管理，定期维护更新，保障知识库的全面性、准确性、及时性。  | 需提供运营管理平台功能截图证明6 |
| 19 | 安全防护 | 安全防护服务 | 做好安全配置检查服务、日志备份分析服务、恶意代码检测服务、主机监测服务、网站安全监测服务、资产运维管理服务。监测的风险事件经关联分析、人工验证后，通过运营管理平台发布预警/事件通报，完成处置反馈。 |  |
| 20 | 现场值守服务 | 西咸新区网信办网络安全工作协调运维 | 驻场服务（5\*8h）：派驻西咸新区网信办现场工作，负责协助进行网络安全工作的协调处置，融媒体中心局域网络（政务网）的运行维护工作。 |  |
|  | 西咸新区先促局网络安全工作协调运维 | 驻场服务（5\*8h）：派驻西咸新区先促局现场工作，负责协助先促局进行网络安全工作的协调处置，西咸大厦、创新大厦局域网络（政务网）的安全维护工作。 |  |
| 21 | 舆情监控 | 舆情监控 | 提供一套舆情监控系统，对互联网上涉及西咸新区的网络安全舆情进行监测跟踪。 |  |

表1 西咸新区网络安全态势感知服务项目服务内容

1. **服务人员要求**

本项目要求服务人员9人，其中驻场人员6人，其余1人为项目经理，2人为技术支持人员。项目经理需具备高级信息系统项目管理师证书，技术支持人员至少1人需具备中级信息安全工程师证书。本项目驻场人员6人，其中：

（1）1名工程师7\*8h驻场一体化平台现场，其余3名工程师7\*24h轮值驻场一体化平台现场，早中晚班，每次轮班时间为8小时，负责一体化平台现场安全告警日志信息监测，态势感知系统运维、探针设备及各信息安全设备运维。

（2）1名工程师5\*8h驻场在西咸新区网信办，负责协助网信办进行网络安全工作的协调处置，融媒体中心局域网络（政务网）的运行维护工作。

（3）1名工程师5\*8h驻场在西咸新区先促局，负责协助先促局进行网络安全工作的协调处置，西咸大厦、创新大厦局域网络（政务网）的安全维护工作。

1. **服务考核**

从项目合同生效后，项目通过服务准备合规验收后签署服务启动确认单，之

后项目进入一年服务期，服务期每满3个月为一个考核周期，采用评分方式按4个考核周期进行服务考核。从网络安全运营服务质量（60分）、网络安全运营服务合规性（10分）、用户满意度（30分）和加分项（10分）四方面进行服务考核评分。项目服务考核满分100分+10分，考核得分为60分以上为合格，根据考核得分情况，按照以下方式付款：

（1）若90≤考核得分≤100+10，足额支付本考核周期服务费。

（2）若60≤考核得分<90，每低一分，扣罚本考核周期服务费的1%款项。

（3）若考核得分＜60，扣罚本考核周期服务费的50%款项，同时采购方有权暂停供应商服务资格并提出整改要求，供应商需按采购方提出的整改要求及期限进行整改并经采购方确认整改后是否考核合格，若供应商拒不整改或连续两次考核不合格，采购方有权要求解除服务合同，并有权不支付剩余款项。

具体评分标准如下：

**项目运营服务考核标准**

| **考核项** | **网络安全运营服务质量** | **网络安全运营服务合规性** | **用户满意度** | **加分项** | **总分** |
| --- | --- | --- | --- | --- | --- |
| 满分 | 60分 | 10分 | 30分 | 10分 | 100分+10分 |
| 得分 |  |  |  |  |  |

注：服务考核满分100分+10分，得分60分以上为合格。

| **一级指标** | **二级指标** | **三级指标** | **考核指标说明** | **考核得分** | **评分说明** |
| --- | --- | --- | --- | --- | --- |
| 网络安全服务质量（60分） | 服务进度完成情况（30分） | 实施计划进度完成情况（15分） | 安全服务是否按方案进度完成（15分） |  |  |
| 安全服务产出物完成情况（15分） | 是否提交安全服务工作产出物（10分） |  |  |
| 安全服务产出物的质量（5分） |  |  |
| 风险控制及响应型服务质量（20分） | 安全事件响应时间达标情况（5分） | 要求服务商在10分钟内响应，并按照要求到达现场应急处理。 |  |  |
| 安全事件处理达标情况（10分） | 安全事件发生后，要及时到达现场，配合相关维护人员判定故障原因、修补风险点及时解决问题。 |  |  |
| 重要工作完成情况（5分） | 对用户布置的重要任务，如临时突发任务、网信办文件响应等的完成情况。(规定时间内未完成一次扣1分) |  |  |
| 例行服务质量（10分） | 态势感知监测情况（5分） | 出现以下任何一种情况一次扣1分:1、没有按要求进行日常态势感知监测;2、报告没有如实反映存在的问题。 |  |  |
| 日常服务质量（5分） | 日常检查、巡检监控不到位影响到后台运转及前台的对外服务，造成事故。用户方发现一次扣1分。被后台用户投诉扣2分。被公众发现或投诉扣3分。 |  |  |
| 网络安全服务合规性（10分） | 工作规范性（5分）  | 日常工作要求（5分） | 遵守用户各项规章制度、现场工作纪律、安全生产要求等，违反一次扣1分。 |  |  |
| 出勤情况（5分） | 日常考勤（5分） | 驻场人员不得无故缺勤。驻场人员出勤率：低于60%（扣4分）;低于80%（扣3分）;低于90%（扣2分);低于100%（扣1分)。(出勤率＝本月驻场人员实际出勤天数/当月驻场人员应出勤天数） |  |  |
| 用户满意度（30分+10分） | 预期效益实现效果、事件与问题解决满意度(10分） | 事件与问题解决满意度（10分） | 满分10分 |  |  |
| 工程师技术能力满意度（10分） | 工程师技术娴熟能力评估（10分） | 满分10分 |  |  |
| 工程师服务态度（5分） | 协作性、责任心、积极性等（5分） | 满分5分 |  |  |
| 工程师解决事件后向用户陈述说明（5分） | 书面/口头陈述（5分） | 出现用户投诉未陈述说明（每次扣1分) |  |  |
| 加分标准（10分） | 处理临时重大突发事件、提交报告结果、提出建设性意见等额外服务（10分） | 额外服务加分项 |  |  |

**五、商务要求**

1、服务期限

项目通过服务准备合规验收后一年。

2、款项结算

付款方式：本项目款项分两笔支付。

**第一笔付款：**项目通过服务准备合规验收后签署服务启动确认单，之后项目进入一年服务期，供应商持服务启动确认单、当期付款金额的增值税发票，与采购人结算合同总额的50%款项，采购人自收到合格的增值税专用发票后30个工作日内支付本笔款项。

**第二笔付款：**供应商完成全部服务内容，项目经采购人验收合格后，由供应商持项目验收通过凭证、当期付款金额的增值税发票，与采购人结算供应商合同总额50%余款，采购人自收到合格的增值税专用发票后30个工作日内支付本笔款项，如有扣罚，按照服务考核结果将对应款项进行扣罚。

**六、其他**

（一）成果交付要求

包括但不限于服务方案、培训记录、安全报告、巡检记录、风险评估报告、应急演练报告、渗透测试报告等资料。

（二）质量验收标准或规范

1、项目团队人员就绪及项目用到的平台或系统部署工作结束后，由供应商发起项目服务准备合规验收申请，采购人根据招标文件、投标文件及合同，组织服务准备合规验收，确认服务准备是否满足服务合规要求。

2、采购人组织供应商,必要时请有关专家进行考核验收，验收合格后，填写政府采购项目验收单（一式伍份）作为对项目服务的最终认可。

3、供应商向采购人提供服务过程中的相关资料。

4、验收依据

（1）招标文件、投标文件、澄清表（函）；

（2）本合同及附件文本；

（3）合同签订时国家及行业现行的标准和技术规范。

5、在得到供应商验收申请后，采购人应积极组织验收，验收合格后出具验收报告。