**2025年西湖区电子政务网络安全保障服务项目采购需求**

1. **项目背景**

2022年以来，省大数据发展管理局先后印发《浙江省电子政务外网安全评估指标体系》、《一体化智能化公共数据平台县（市、区）综合评价指标》等文件以及近年来相关省市考核要求，需依托政务外网、互联网常态化对IRS系统、云主机、“浙里办”、“浙政钉”等政务应用开展安全监测，监测内容包括是否存在弱口令、存在高危漏洞等安全隐患，并要求开展安全自查自纠工作，同时伴随着随着数字化改革不断深入，政务网络广泛延伸和深度覆盖，政务数据规模高速增长，安全漏洞、数据泄露、零日攻击等网络安全威胁日益凸显。

1. **项目需求**

项目整体服务内容包括以下：

1. 专业安全服务，依据上级主管部门网络安全、数据安全考核要求及工作实际，续购第三方服务，针对全区重点业务系统提供涵盖漏洞管理、渗透测试、攻防演练、应急处置、安全值守、安全测评、数据安全防护等方面，主动消除安全风险及隐患。
2. 防护能力补充，依据《浙江省公共数据安全管理总则》、《2024年数安之江浙江省重要行业网络数据安全专项行动方案》等指导文件要求，现有数据安全防护体系还存在防护盲区和脆弱环节，应查漏补缺、进行完善和重点防护，提升政务业务系统数据安全性。
3. 设备维保服务，对部分政务外网安全设备、网络设备、机房UPS、精密空调、机房消防系统、机房柜式气体灭火装置等过保设备续购运行维护服务，包括设备规则库、软件能够及时更新，购买设备保修服务，确保发生故障后能够得到及时修复，确保设备稳定、可靠运行。
4. 运维人员服务，立足我区工作实际，配置政务网络安全监测服务，政务终端外设运维服务，政务网络安全处置服务，浙里办高质量运行、政务服务增值化改革支撑服务，数据流通支撑及相关服务，确保运维服务工作接续开展。
5. 监理服务，采用第三方监理对服务进行全过程精细化管控。
6. **采购清单**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 名称 | | 详细描述 | 单位 | 数量 |
|  | 专业安全服务 | “三高一弱”专项服务 | 服务方自备服务工具，对irs上西湖区电子政务应用主机高危端口、高危漏洞、高危外联、弱口令等安全隐患开展检测工作，每次完成IRS上所有政务网主机检测，检测完成提交检测报告，对检测情况提出修复建议，指导、协助开发商完成修复，并对修复结果进行复测，确保整改完成，服务期：一年。 | 年 | 1 |
|  | 渗透测试服务 | 对业务系统进行渗透测试，通过真实模拟黑客攻击，对信息系统进行模拟攻击，重点验证业务系统业务流程和逻辑上安全漏洞，输出渗透测试报告，每年4次，每年累计服务系统数量不少于100个，服务期：一年。 | 年 | 1 |
|  | 攻防演练服务 | 组织开展网络数据安全攻防实战演练，组织不少于10支攻击队伍，检验全区政务外网和社会面网站系统（不少于140个）的网络数据安全防护水平，提升各单位网络数据安全防护意识和实战能力。 | 项 | 1 |
|  | 等级保护测评服务 | 对西湖区重要政务系统（由区数据资源管理局统筹），依据网络安全等级保护标准规范提供等级测评复评工作，出具符合要求的等级保护测评报告。服务数量：6个(等保二级)。 | 项 | 1 |
| 对西湖区重要政务系统（由区数据资源管理局统筹），依据网络安全等级保护标准规范提供等保测评复评工作，出具符合要求的等级保护测评报告。服务数量：2个(等保三级)。 | 项 | 1 |
| 对西湖区重要政务系统（由区数据资源管理局统筹）提供等级保护测评，依据网络安全等级保护标准规范实施测评工作，协助进行备案，出具符合要求的等级保护测评报告。服务数量：6个(等保二级)。 | 项 | 1 |
|  | 密码应用测评服务 | 依据《信息系统密码应用基本要求》，对2个定级为等保三级系统政务信息系统开展密码应用安全性评估（复测评），出具符合要求的密码应用安全性评估报告。 | 项 | 1 |
|  | 非工作时段7\*24小时值守服务 | 复用5名服务人员，提供国家法定节假日（13天）、指定重要时期（30天）等非工作时段值班值守服务，监控西湖区政务安全设备、安全态势运行情况，发生安全突发情况时，进行及时处置，保障重要时期基础设施以及信息系统的安全运行。年度服务时间不少于43天，服务期：一年。 | 年 | 1 |
|  | 政务外网安全评估服务 | 1、网络安全评估服务：围绕资产管理、脆弱性管理、威胁管理、事件管理、人员管理、身份权限管理等内容，通过提供网络安全评估服务，完善相关安全管理制度，明确技术落实及人员能力差距，并对电子政务外网网络安全建设工作进行优化建议，提供《网络安全评估报告》。2.数据安全评估服务：围绕数据全生命周期，聚焦可能影响数据的保密性、完整性、可用性和数据处理合理性的安全风险，掌握数据安全总体状况，发现数据安全隐患，提出数据安全管理和技术防护措施建议，提升数据安全防攻击、防破坏、防窃取、防泄露、防滥用能力，提供《数据安全风险评估报告》。3.以SAAS化服务形式，提供外部攻击暴露面管理，服务以攻击者视角出发，对提供的IP（不超过10000）、域名（不超过1000）、关键字（不超过100），进行互联网资产测绘、资产暴露面检测、敏感数据泄露检测、边界脆弱性检测、社工利用风险服务，并提供处置建议，提供《外部暴露面管理报告》，服务期：一年。 | 年 | 1 |
|  | 浙里办应用安全检测服务 | 服务方自备应用安全扫描工具，对西湖区浙里办所有应用按需开展扫描；扫描完成后对发现的应用漏洞进行人工核验，研判确认是否存在该隐患，输出安全运维检测报告；提出修复建议，指导、协助应用单位完成高危漏洞修复，并对修复结果进行复测，确保漏洞整改完成。服务频次：每月4次，每年不少于48次，服务期：一年。 | 年 | 1 |
|  | 防护能力补充 | 数据访问安全系统 | 提供数据访问安全功能，形成覆盖数据访问安全、数据交换与传输安全、访问控制安全、数据使用申请与管理的数据安全管控能力，防止开发、运维场景中账户冒用、违规使用、数据泄露、数据篡改、非法截屏等安全事件发生，实现数据安全管控和隔离，质保期：三年。  1.针对第三方运维开发人员接入数据资源的场景，可能存在数据泄露、违规访问的情况，主要通过细粒度数据授权控制、数据审批、计算审批等，保证数据安全和保护隐私。  2.核心运维开发数据资源运行在完全独立的安全域，限制安全域的网络访问，采用白名单机制，仅授权用户才可以访问。  3.支持面向运维研发人员远程容器管理、Telnet远程登录、虚拟网络控制、Linux远程管理、windows远程桌面、远程浏览器、远程数据库连接等应用的数据安全管控，在确保便捷访问核心研发数据的同时，确保数据的共享、传输和使用安全。  4.实现运维开发数据资源安全的管控，通过安全数据盘、下载审批、数据水印和拷贝权限限制进行数据资源的管控。  5.运维开发人员可直接访问和使用分布在不同网络的研发资源，并进行多维度的数据资源访问安全审计，包含登录日志、操作日志、连接日志、文件操作、图形审计、系统日志等。  6.提供3年开发运维终端用户正式版软件授权数量50个，虚拟环境数20个。  7.须按用户上云需求适配各类省、市云资源上部署（质保期内支持免费迁移）。 | 项 | 1 |
|  | ODPS数据水印 | 对政务云西湖区ODPS空间数据，配置数据水印服务，通过在数据库表中嵌入不易察觉的标识信息，来保护版权、追踪溯源和验证数据完整性的效果，须按用户上云需求适配各类省、市云资源上部署（质保期内支持免费迁移）。质保期：三年。   1. 支持水印信息的嵌入与提取，并支持多种水印注入算法，包括但不限于数值型（lSB最小位数修改算法、伪列算法）、字符型（空格算法、不可见字符算法、地址标准化映射算法） 2. 水印算法具有良好的鲁棒性，数据进行字符移位、编辑、转换格式后水印信息不会丢失。数据被攻击后，能够通过数据片段上的水印信息提取出完整信息，保证数据完整性不受攻击影响。 3. 支持记录数据分发的信息，包括数据类型、数据量、文件数量、版权、用户、发单编号、领取人员、领取用途、时间等，并可对记录的信息进行浏览、查询、统计、可视化表达、导出与自动备份等。   提供三年软件正式版授权License。 | 项 | 1 |
|  | ODPS数据加解密 | 对政务云西湖区ODPS空间数据，配置数据加解密服务，实现对ODPS空间敏感数据目录L3、L4字段进行加密，通过对数据传输转换过程进行加密保护，确保数据在传输过程中不被窃取或篡改，须按用户上云需求适配各类省、市云资源上部署（质保期内支持免费迁移）。质保期：三年。  1、支持国密算法（SM2、SM4等）以及AES、3DES等常见数据加密交换功能，能够实现数据加解密；  2、支持数据日期类型、INT类型等非字符串类型字段的数据加解密；  3、支持数据传输通道加密功能(SSL)。  4、提供三年软件正式版授权License。 | 项 | 1 |
|  | 设备维保服务 | 运维操作审计系统维保 | 思福迪LogBase-B4600原厂维保，服务期：一年 | 年 | 1 |
|  | SSL VPN设备维保 | 深信服SJJ1813 SSLVPN原厂维保，服务期：一年 | 年 | 1 |
|  | 边界安全监测系统维保 | 远望ABPS1700-2H4X-S原厂维保，服务期：一年 | 年 | 1 |
|  | 负载均衡设备维保 | 深信服AD-1000-F680原厂维保，服务期：一年 | 年 | 1 |
|  | 负载均衡设备维保 | 深信服AD-4000原厂维保，服务期：一年 | 年 | 1 |
|  | 漏洞扫描设备维保 | 天融信TSC-71232-WVS原厂维保，服务期：一年 | 年 | 1 |
|  | 上网行为管理设备维保（有线）维保 | 深信服AC1000原厂维保及规则库升级服务，服务期：一年 | 年 | 1 |
|  | VPN2 WAF设备维保 | 深信服AF-2000-B2150原厂维保及规则库升级服务，服务期：一年 | 年 | 1 |
|  | 数据库审计设备维保 | 安恒明御DAS-A1000原厂维保，服务期：一年 | 年 | 1 |
|  | 态势感知系统维保 | 深信服SIP-1000-A600、探针STA-100-B420原厂维保及规则库升级服务，服务期：一年 | 年 | 1 |
|  | 核心路由器维保维保 | 2台H3C CR16006-F设备原厂维保，服务期：一年 | 年 | 1 |
|  | 核心交换机维保维保 | 2台H3C S10506 设备原厂维保，服务期：一年 | 年 | 1 |
|  | 插卡防火墙维保 | 1块H3C SecBladeIV-Lite原厂维保，服务期：一年 | 年 | 1 |
|  | 机房ups维保 | 中达电通（台达） 主机Modulon HIFT（1台）以及 GES-HIFT80C 蓄电池12V100AH（32\*2节），提供1年的原厂维保服务，提供4次巡检服务（每季度1次） | 年 | 1 |
|  | 机房消防系统维保 | 海湾消防报警系统(消防气体除外)，负责网络机房和服务器机房消防系统设备的维保服务，设备出现故障时候负责维修，每月一次巡检。服务期：一年 | 年 | 1 |
|  | 机房环境监控系统维保 | 源久供配电监控系统、UPS 监控系统、空调监控系统、漏水监测系统、消防检测系统、温湿度监控系统，按季度上门对环境监控系统运行情况进行检查。服务期：一年 | 年 | 1 |
|  | 机房强电维保 | 机房配电柜、强电线路、插座、机房防雷器、接地网系统每季度巡检和故障维护。服务期：一年 | 年 | 1 |
|  | 机房柜式气体灭火装置维保 | 机房内原柜式七氟丙烷气体灭火装置换新，提供一年原厂维保，一年4次巡检服务（每季度1次），服务期：一年 | 年 | 1 |
|  | 机房空调维保 | 1台佳力图CANATAL MEAU201，3台大金DAIKIN RY125FQA3C，3台格力KFR-120W，设备维保，服务期：一年 | 年 | 1 |
|  | 运维人员服务 | 政务网络安全监测运维服务 | 依据全区政务网络安全工作开展的需要，提供政务外网网络安全风险监控、告警日志分析、事件分析、隐患监控、技术指导等工作内容，配置1人驻现场的政务网络安全监测运维服务。 | 人 | 1 |
|  | 政务终端外设运维服务 | 依据终端运维工作开展的需要，对政务外网终端、外设、系统及办公软件提供系统、应用软件安装、软硬件设置及优化、软硬件故障处置、日常使用指导等工作内容，配置1人驻现场的政务外网终端外设运维服务。 | 人 | 1 |
|  | 政务网络安全处置服务 | 依据全区政务网络安全工作开展的需要，提供政务外网网络安全策略配置、事件响应、应急处置、隐患修复、工单督办等工作内容，配置1人驻现场的政务网络安全处置服务。 | 人 | 1 |
|  | 浙里办高质量运行、政务服务增值化改革支撑服务 | 依照浙里办应用考核要求，做好上线资料初审、应用状态监测、应用使用推广、应用质量统计等工作，落实应用规范管理、运维安全等工作要求；依照省市政务服务增值化改革工作要求，对接协调相关业务部门，下发通知，统计汇总每月办件明细，完成企服平台事项更新及企业诉求跟进，督促相关业务部门完成数据板块相关工作，配置1人驻现场的浙里办高质量运行、政务服务增值化改革支撑服务。 | 人 | 1 |
|  | 数据流通支撑及相关服务 | 依照省市区数据流通相关工作安排，参与开展企业数据场景及产品对接，协调各部门、企业推进有关工作落实，推进数据运营、流通、交易等相关工作落实及重要事项的办理。配置1人驻现场的数据流通支撑及相关服务。 | 人 | 1 |
|  | 监理服务 | | 配置监理服务，对项目实施全过程进行管理、协调及监督，确保项目实施过程规范，规避潜在风险。 | 项 | 1 |