合同编号：ZJSXA2504443CGN00

绍兴市公安局越城区分局2025年越城区网络安全运维服务项目服务合同

合同编号：

确认书号：

甲方（甲方）：绍兴市公安局越城区分局

乙方（供应商）：中国电信股份有限公司绍兴分公司

甲、乙双方根据（浙江筑脸全过程工程咨询有限公司）项目编号为[2025]1417号的（标项一及名称：绍兴市公安局越城区分局2025年越城区网络安全运维服务项目）项目的政府采购交易结果，签署本合同。

一、服务内容及标准

序号	服务名称	服务内容
1	绍兴市公安局越城区分局2025年越城区网络安全运维服务项目	主机和应用漏洞扫描服务、网站系统安全检测服务、网络数据安全检查服务、驻场服务人员驻场、驻场服务人员重保、网络安全培训和宣传、网络安全演练

二、服务价格

序号	服务项目或其他报价项	单价（人民币元）	数量	金额（人民币元）	备注
1	绍兴市公安局越城区分局2025年越城区网络安全运维服务项目	1556000	1	1556000	
投标报价	大写：壹佰伍拾伍万陆仟元整				
	小写：1556000元				

三、技术资料

1.乙方应按采购文件规定的时间向甲方提供与本项目有关的技术资料。

2.没有甲方事先书面同意，乙方不得将由甲方提供的有关合同或任何合同条文、规格、计划、图纸、样品或资料提供给与履行本合同无关的任何其他人。即使向履行本合同有关的人员提供，也应注意保密并限于履行合同的必需范围。

四、知识产权

1、乙方应保证所提供的货物与服务均不会侵犯任何第三方的知识产权。如若发生侵权事件，所产生的责任和费用由乙方承担。

2、乙方保证所交付的服务的所有权完全属于乙方且无任何抵押、查封等产权瑕疵。

五、验收要求、标准

1、验收以采购文件和技术文件、投标文件、合同及安装技术要求为依据，验收必须符合国家、地方有关规范、标准及设计要求。乙方应该向甲方提交申请验收报告，并且提供技术档案资料（包括但不限于扫描，检测，检查等相关报告），若乙方未能按照上述要求履行的，导致无法及时验收的，则须由乙方承担一切责任。

2、符合验收条件的，由甲方组织有关部门按照国家、地方有关规范、标准及设计要求进行验收。验收后乙方应按照验收中提出的意见整改。

3、整改完毕且复验合格后将本项目交给甲方使用，完成日期以通过复验日期为准。

4、验收按国家有关规范标准（国家无验收规范标准的按双方合同规定的要求）进行。甲方保留邀请参加本项目的其他供应商或者第三方机构或相关技术专家参与验收的权利。参与验收的供应商或者第三方机构的意见作为验收书的参考资料一并存档。

六、转包或分包

不允许转包。

允许分包部分__/__。

如乙方将项目转包或将不允许分包部分进行了分包，甲方有权解除合同并追究乙方的违约责任。

七、项目服务期限及实施地点

1.服务期限：签订合同之日起1年

2.实施地点：绍兴市越城区世纪街107号

八、付款

付款方式：

1. 合同签订生效并具备实施条件后，乙方提供符合甲方要求的发票后 7 个工作日内，甲方向乙方支付 40%的合同款；

2. 阶段性验收合格后支付第二笔费用，乙方提供符合甲方要求的发票后 7 个工作日内，甲方向乙方支付 50%的合同款；

3. 服务期满项目验收合格后，乙方提供符合甲方要求的发票后 7 个工作日内，甲方向乙方支付 10%的合同款。

九、商品包装和快递包装要求

本次项目采购所涉及的商品包装和快递包装建议按《关于印发《商品包装政府采购需求标准（试行）》、《快递包装政府采购需求标准（试行）》的通知》（财办库〔2020〕123 号）文件要求执行。

十、税费

本合同执行中相关的一切税费均由乙方负担。

十一、违约责任

1. 甲方无正当理由拒绝验收项目的，甲方向乙方偿付拒收合同总价的百分之五违约金。

2. 甲方无故逾期验收和办理合同款项支付手续的，甲方应按逾期付款总额每日万分之五向乙方支付违约金。

3. 乙方逾期提供服务的，乙方应按逾期交付部分每日千分之六向甲方支付违约金，由甲方从合同款项中扣除。逾期超过约定日期 10 个工作日不能交付的，甲方可解除本合同。乙方因逾期交付或因其他违约行为导致甲方解除合同的，乙方应向甲方支付合同总值 5%的违约金，如造成甲方损失超过违约金的，超出部分由乙方继续承担赔偿责任。

4. 乙方所履行的服务质量或服务数量不符合合同规定及采购文件规定的，甲方可要求乙方进行整改，整改后还不达标，甲方有权扣除相应服务的价款。如发生乙方拒不配合的，甲方有权单方面解除合同，且相关损失由乙方承担。

5. 解除合同应向财政备案。

十二、不可抗力事件处理

1. 在合同有效期内，任何一方因不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响期相同。

2. 不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。

3. 不可抗力事件延续 120 天以上，双方应通过友好协商，确定是否继续履行合同。

4. 因自然灾害、政策变化等不可抗力导致违约时双方责任免除。

十三、诉讼

双方在执行合同中所发生的一切争议，应通过协商解决。如协商不成，可向甲方所在地法院起诉。

十四、合同生效及其他

1. 合同经甲、乙双方签名并加盖单位公章后生效。若使用电子印章的，自双方盖章之日起生效。若乙方加盖电子印章的，以加盖乙方电子印章的本合同电子文档所载内容为准。

2. 合同执行中涉及采购资金和采购内容修改或补充的，须经财政部门审批，并签书面补充协议，经报政府采购监督管理部门备案后，方可作为主合同不可分割的一部分。

3. 乙方需要定期开展信息安全宣传活动，增强甲方全体的安全意识、提升全员的网络及信息安全知识，组织不少于 2 次的专业安全培训，宣传内容包括但不限于：网络及信息安全法律法规、全员安全意识、网络及信息安全制度等。每年进行至少为期两天的网络及信息安全专项“护航”系列培训，培训范围为甲方全员，要求与甲方商定培训主题内容后提供相应培训素材，并提供经甲方认可的培训授课讲师”。

4. 采购文件、投标文件与本合同具有同等法律效力。

5. 本合同未尽事宜，遵照《民法典》有关条文执行。

6. 本合同一式五份，具有同等法律效力，甲、乙双方各执二份，采购代理机构一份。

甲方（盖章）：绍兴市公安局越城区分局

地址：绍兴市越城区世纪街107号

法定（授权）代表人：

签名日期：2025年6月30日

乙方（盖章）：中国电信股份有限公司绍兴分公司

地址：浙江省绍兴市四马路9号

开户行：中国工商银行绍兴市分行营业部

开户账号：1211012029905480251

法定（授权）代表人：

签名日期：2025年6月30日

服务附件清单：

（一）主机、应用漏洞扫描服务

服务名称	服务说明	单位	数量
主机、应用漏洞扫描服务	服务描述：1，通过扫描工具针对服务器、网络设备等对象的系统漏洞开展漏洞扫描，查找系统中存在的高、中、低危漏洞，进行包含但不限于以下检测服务：系统帐号检测；组帐号检测；系统日志检测；主机信任关系检测；系统配置文件检测；关键系统文件的基线检测；口令强度检测；系统安全漏洞检测；系统脆弱性分析；有控制的渗透检测；日志文件检查；提供分析报告及安全建议。2，建立全新的漏洞管理流程，建立包括漏洞检测、漏洞验证、报告分发、漏洞跟踪、漏洞数据管理、漏洞修复、修复验证以及人员协同工作等。漏洞管理是以资产为核心，并对漏洞状态进行持续跟踪，提高漏洞检测、漏洞数据管理、漏洞运维各个环节的自动化程度。	资产 IP/次	2200
	服务范围：越城辖区内企事业单位		
	服务方式：现场服务		
	成果输出：《漏洞扫描报告》		
	备注：辖区主机、应用资产 IP 现场检查不少于 2200 个次。		

（二）网站系统安全检测服务

服务名称	服务说明	单位	数量
网站系统安全检测服务	服务描述：1，对越城辖区内所有网站系统提供监测和有效报警。能够在第一时间对所有网站进行 7*24 小时网站监测，包含：“篡改、黑链/挂马、敏感文件、敏感词、可用性、域名劫持”等 6 个维度开展实时监测，并可通过邮件、飞书、钉钉、企业微信等告警形式提供网站风险预警服务，有效对区域内企业提供网络安全预警、监测和处置服务。2，针对全区的资产进行识别并登记台账，完善漏洞库信息，支持网站漏洞评估能力，	域名	1000

	提供多种 Web 应用漏洞的安全检测，如“SQL 注入、跨站脚本、文件包含、CSRF、目录遍历”等网站脆弱性漏洞，对漏洞状态进行在线处置，并记录处置状态，后续若多次对同个目标进行复查扫描，可根据漏洞历史处置状态进行自动跟踪处置。3，敏感文件检测，对发布到网上的 pdf、word、excel 文件中是否包含“身份证号、邮箱、手机号码、用户名/密码”等敏感信息，可在系统上查看泄露的信息以及敏感文件下载链接。4，事件溯源分析：深入分析安全事件的成因，发现存在的薄弱点，溯源攻击路径。		
	服务范围：越城辖区内企事业单位		
	服务方式：远程服务		
	成果输出：《网站系统监测报告》		
	备注：辖区域名监测不少于 1000 个。		

具体要求如下：

序号	指标		规格参数
1	互联网主机资产识别	主机资产识别	支持自动扫描 IP 资产信息，包括：“存活 IP、设备厂商、操作系统、端口、应用、数据库、中间件、服务版本”等资产指纹特征。
2		精细化识别	可识别精细化识别主机的硬件信息（包括 cpu、线程、内存、磁盘等使用率信息），网卡信息，运行进程、自启动服务、安装软件等
3	网站资产识别	▲网站资产识别	支持自动识别网站资产信息，包括：“中间件信息、web 框架信息、CMS&OA、程序语言”等指纹信息，支持爬取网站后台、ICP 备案编号、网站标题、网站返回码等属性。
4		▲二级域名扫描	支持二级域名扫描功能，输入一级域名进行一键扫描，通过搜索互联网数据，自动获取到该域名的二级域名、网站标题、解析 IP 地址；
5		▲IP 反查域名监测	输入 IP 或者网段，通过搜索互联网数据，自动获取到 IP 对应的域名、url 链接、网站标题、返回状态码；
6		▲网站资产相关度分析	通过爬取企业单位已知的网站页面，分析网页中是否包含企业单位相关的网站链接，从而发现未知网站；可配置“网段、域名”等命中规则，自动判断是否属于企业单位的网址；

7	资产管理	互联网主机资产台账	系统应具备互联网主机资产台账功能。包括： 1、支持通过主机资产测绘，自动识别资产开放端口、端口服务、资产指纹等信息，形成主机资产台账。 2、支持通过导入现有资产信息，或在线编辑方式，录入主机资产的管理信息，比如系统所属部门、负责人、联系方式、资产价值、物理位置等。 3、支持对 IP、资产组、部门、责任人、应用系统、设备类型、主机名称、操作系统、宿主机 ip、资产价值、等级保护等进行精准搜索或模糊搜索 4、可自定义展示列，可排序、选择是否显示。 5、支持添加自定义的资产属性。
8		网站资产台账	系统应具备网站资产台账功能。包括： 1、支持通过网站资产测绘，自动识别网站中间件、web 框架、程序语言、网站标题、ICP 备案编号、网站返回码，等形成网站资产台账。 2、支持通过导入现有资产信息，或在线编辑方式，录入网站资产的管理信息，比如网站所属部门、负责人、联系方式、资产价值、物理位置等。 3、支持添加自定义的资产属性。 4、支持对状态码、IP、资产组、部门、责任人、URL、子域名、易危组件、中间件、ICP 备案号、公安备案号、归属地等进行精准搜索或模糊搜索 5、可自定义展示列，可排序、选择是否显示。
9	网站安全监测	web 漏洞监测	支持网站漏洞评估能力，提供多种 Web 应用漏洞的安全检测，如“SQL 注入、跨站脚本、文件包含、CSRF、目录遍历”等网站脆弱性漏洞。
10		web 漏洞跟踪管理	支持对漏洞状态进行在线处置，并记录处置状态，后续若多次对同个目标进行复查扫描，可根据漏洞历史处置状态进行自动跟踪处置。
11		黑链/篡改事件监测	高频率监测站点是否存在被黑客植入黑链、篡改的事件，系统需要保留植入黑链、篡改的快照页面，监测频率低至 5 分钟/次
12		可用性异常事件监测	模拟浏览器访问，监测站点的可用性情况，监测频率低至 5 分钟/次
13		域名劫持事件监测	监测站点的 DNS 解析是否异常，监测频率低至 5 分钟/次
14		全站敏感词事件监测	用户可对不同网站自定义不同的敏感词库，并对企业、单位的网站进行全站页面爬取，发现敏感词字眼。
15		▲敏感文件事件泄露监测	可监测发布到网上的 pdf、word、excel 文件中是否包含“身份证号、邮箱、手机号码、用户名/密码”等敏感信息，可在系统上查看泄露的信息以及敏感文件下载链接。

16		▲渗透测试台账	支持以 excel 报表格式导入渗透测试报告，形成渗透测试台账。可在系统查看渗透测试结果，以图表形式可视化展现漏洞风险级别比例、风险应用比例，可对渗透报告中的漏洞进行跟踪确认，处置漏洞状态：未整改、已整改、忽略、未整改。
17	应用服务器主动安全监测	▲主动威胁监测	可以根据需要，在用户的服务器、业务系统上安装安全监控插件，主动监测 webshell、暴力破解、异常登录成功、反弹 shell、挖矿检测等，发现可疑的入侵事件，并实时将告警同步到服务平台。
18		▲Web 日志分析	可输入最新的 web 日志文件以及对应 web 端口号，后续会自动跟踪相同目录下的 web 日志，发现各类 web 入侵攻击，包括但不限于目录穿越、SQL 注入、XSS 跨站脚本攻击 、web 路径遍历漏洞攻击，高亮显示攻击特征。
19		▲文件篡改检测	可检测文件的篡改行为，包括：“创建、写入、修改权限、重命名、删除”等篡改行为。
20		▲漏洞攻击屏蔽	精准检测恶意攻击源、扫描源，并可基于告警风险值、或者定向源进行屏蔽，使漏洞扫描器、恶意攻击源无法扫描到主机存在的漏洞，包括可利用漏洞、版本漏洞。
21	互联网主机漏洞管理	完善的漏洞库	漏洞库漏洞信息大于 320000+条，提供详细的漏洞描述和对应的解决方案描述。支持通过多种维度对漏洞进行检索，包括：CVE ID、CNNVD ID、漏洞名称、漏洞风险等级等维度。
22			通过 4000+POC 验证过的漏洞，扫描结果需包含漏洞利用证明，包括但不限于攻击 Payload、目标响应结果、漏洞利用点、关键参数等内容。
23		▲漏洞生命周期管理	支持漏洞跟踪管理，能够自动对漏洞状态进行处置，自动识别“新增、已修复、未修复”的漏洞，同时支持人工方式进行漏洞状态处置，以及编写漏洞备注，
24	报表	站点报表	支持输出单独的系统漏扫报表，报告中的漏洞应具备统一的 CVSS 国际标准评分，以准确衡量漏洞的危险级别，为漏洞修补工作的优先级提供指导。
25			支持生成网站安全监测综合报表和各个网站的安全监测报表，报表类型包括：excel、word、html。
26	▲监测范围		用户指定辖区内 290 个单位。
27	▲数据留存与报告要求		1、所有信息必须留存在用户侧，不得在厂家设定的存储设备做数据任何形式的中转和留存。 2、按月出具《用户指定单位网站风险监测报告》。

（三）网络数据安全检查服务

服务名称	服务说明	单	数

		位	量
网络数据安全检查服务	服务描述：涉及国家关键基础设施、重要行业领域或涉及大量敏感信息，如能源、交通、金融、政府部门等，对应的网络数据安全检查，主要包含数据安全检查，数据安全检测可以确保这些敏感数据得到妥善保护，防止因安全事故或恶意攻击导致国家关键基础设施受损、重要信息泄露等，从而保障国家的安全和稳定，到企事业单位现场技术检查支撑；对绍兴市越城辖区的安全评估关键系统出具数据安全检查报告及整改建议，对重要关键应用系统提供各类检查，有效提高辖区内应用系统的安全性。 检查内容包括但不限于 （1）对被检查单位的网络数据安全工作开展情况，进行现场评估，检查内容包括： 1、数据安全管理：对相关人员进行访谈，核查制度规章、防护措施、安全责任落实情况，查验数据安全相关管理制度、数据安全风险评估报告、等保测评报告等有关材料及制度落实情况的证明材料。 2、数据处理活动:通过专业安全技术、方法从数据所处的业务相关活动的维度，评估数据的收集、存储、使用、加工、传输、提供、公开等活动过程中存在的现状和安全风险。 3、数据安全技术:核查网络环境、数据库和大数据平台等相关系统和设备安全策略、配置、防护措施情况。 4、个人信息保护：从管理、技术、合规等层面对被检查单位的个人信息保护开展全面的检查。 （2）技术支撑单位使用数据安全检查工具进行检测，检测内容包括核心交换机镜像流量敏感数据传输监测、数据库脆弱性检测。	系统/次	280
	服务范围：越城辖区企事业单位		
	服务方式：现场服务		
	成果输出：《数据安全检查报告》		
	备注：辖区系统数据安全检查不少于 280 个次。		

（四）驻场服务人员驻场

服务名称	服务说明	单位	数量
驻场服务人员驻场	服务描述：1，为越城区公安局提供常态化网络安全应急保障、现场技术检查，负责安全设备及安全检测系统的日常运维，包括运行状态日检、检测，对安全设备及安全监测系统的策略调优、每天对安全设备日志信息和安全监测系统告警信息进行深入分析，及时发现安全威胁，并进行验证、处置及报告。2，结合实际业务发展及安全现状，协助后端支持人员对网络及信息安全进行持续的风险评	人	1

	估，以风险结果为依据，协助后端支持人员进行应急预案及安全体系建设的补充完善。对外部发生的信息安全事件（如系统或软件高危漏洞、病毒变种等），快速分析，结合实际情况提供处置方案并协助实施，以防同类事件发生。3，具备专业的远程专家服务团队，支持驻场人员进行以上工作的实施解决。协助人员进行其他网络及信息安全相关工作。		
	服务范围：越城区公安局		
	服务人数：1人		
	服务方式：现场运维		
	使用系统：安全检查工具箱、等级保护工具箱		

（五）驻场服务人员重保

服务名称	服务说明	单位	数量
驻场服务人员重保	服务描述1，在重要会议或重大活动期间从梳理网络资产，并通过网络层面、服务器层面、数据层面为用户构建全方面的重要敏感时期的安全保障服务。保障网络基础设施、重点网站和业务系统安全，提供全方位的安全防守建设咨询以及事前、事中、事后的全面安全建设托管服务，确保越城区公安局的业务系统能够在重大活动期间安全平稳运行。2，提供高级安全专家、安全服务工程师特殊时期提供人员保障服务。特殊时刻人员值守：两会、国庆等重要时期，提供人员值守服务对安全事件进行预防、监测、处置，保障信息系统安全稳定运行。	天/人	140
	服务范围：越城区公安局		
	服务方式：现场运维（7*24小时重保值守服务）		
	成果输出：《重保值守日报表》、《重保总结报告》		
	服务人数：至少2人（具体需求根据活动的规模和业务单位实际需求进行安排）		

（六）网络安全培训、宣传

服务名称	服务说明	单位	数量
网络安全培训、宣传	服务描述：一、网络安全培训：通过邀请网络安全专家（人员具有中级及以上职称或具有网络安全培训讲师专业资质的讲师）授课对安全管理人员的培训，讲解国家相关部门对系统信息安全管理和建设的相关标准，研讨建立具有针对性和适用性的安全管理办法，培训的目的是使培训对象了解信息系统所面临的严峻安全威胁和挑战、如何进行全面有效的安全防护措施以及提高网络安全意识等，从而有	次	10

	效避免网络安全事故的发生以及有效处置网络安全事件。（培训方向包括但不限于网络安全法、数据安全法等法律法规普及、最新网络安全技术交流等）。培训课时累计不少于 12 节。 二、网络安全宣传：1. 在报刊杂志、媒体网站等载体开展宣传案件、事件、活动等涉及有关网络安全的报道。2. 开展网络安全宣传活动，至少策划搭建宣传场地 1 场次，包含制作至少 10000 册宣传手册或传单，至少 10 张海报、至少 5 条宣传横幅等网络安全宣传材料。		
	服务范围：越城辖区企事业单位、辖区民众		
	服务方式：现场服务		
	成果输出：培训课件、报道链接、活动台账等		

（七）网络安全演练

服务名称	服务说明	单位	数量
网络安全演练	服务描述：1，安排专业团队对单位的各类信息系统进行全面梳理，包括但不限于操作系统、数据库管理系统、网络架构、应用程序等，详细记录系统的版本信息、配置参数、运行状态以及各系统之间的关联关系。与相关部门和技术人员进行深入沟通，了解单位的业务需求、工作流程以及在信息安全方面的特殊要求和关注点，确保对单位系统有全面且深入的认识。2，针对不同类型和级别的信息安全突发事件，如网络攻击、数据泄露、系统故障等，分别设计相应的演练场景，确保演练方案具有针对性和实用性。3，根据演练结果和总结讨论中提出的改进措施和建议，对应急演练方案进行进一步修订和完善。优化演练流程、调整人员分工、补充技术手段和资源保障等内容，提高预案的科学性、合理性和可操作性。定期对应急预案进行审查和更新，确保其与单位系统的变化、业务发展以及信息安全形势的变化相适应。同时，将修订后的预案及时传达给相关人员，并进行再次培训和宣贯，确保所有人员熟悉最新的应急预案内容。	次	4
	服务范围：全区企事业单位或本单位内部		
	服务方式：现场服务		
	成果输出：《XXXX 网络及信息安全应急预案》、《XX 事件应急演练报告》、《XX 事件应急响应处置分析报告》		