连云港市政府采购合同（服务）

甲方：（买方）连云港市大数据管理中心

乙方：（卖方）中国电信股份有限公司连云港分公司

甲、乙双方根据2025年11月13日连云港市大数据管理中心市政府网站群安全运维服务（2025年）项目（项目编号：JSZC-320700-JZCG-G2025-0157）公开招标的结果，签订本合同。

一、合同内容

1.1 服务内容：我市已建成政府网站群，主要涵盖市政府门户网站、县区（功能板块）门户网站和市政府组成部门单位网站、其他部门单位网站等。政府网站群内的网站数量多，应用发展不断深化，对网站群平台运行安全提出了越来越高的要求。为进一步强化网站群安全保障，需要对现有防护系统进行优化升级，提高网站群云端安全防御能力。

1.2 服务要求：在服务期限内对市政府门户网站群平台系统提供不少于70个子域名服务，具体域名由采购人指定，配有一套专门服务于政府网站群的防御、监测平台，拥有软件版权或使用授权，具体要求见附件。

1.3 服务标准：合同上线后15天交付运行。

1.4 补充条款：/。

二、合同金额

2.1 本合同金额为人民币（大写）：柒拾捌万玖仟元（¥789000）。

2.2 本合同价款包含所有乙方提供合同约定产品和服务的报酬及乙方提供合同中产品和服务所支出的必要费用，甲方在上述合同价款之外不再向乙方支付其他任何费用。

三、技术资料

3.1 乙方应按招标文件规定的时间向甲方提供有关技术资料。

3.2 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

4.1 乙方应保证甲方在使用、接受本合同产品和服务或其任何一部分时不受第三方提出侵犯其专利权、版权、商标权和工业设计权等知识产权的起诉。一旦出现侵权，由乙方负全部责任。

五、产权担保

5.1 乙方保证所交付标的的所有权完全属于乙方且无任何抵押、查封等产权瑕疵。

六、履约保证金

6.1 本合同不收取履约保证金。

七、合同转包或分包

7.1 本合同范围内产品或服务，应由乙方直接供应，不得转让他人供应或部分分包给他人供应。

7.2 如有转让和未经甲方同意的分包行为，甲方有权终止合同。

八、服务时间

8.1 服务时间：1年（合同约定时间起算）。

九、交付期、交付方式及交付地点

9.1 交 付 期：甲方指定 。

9.2 交付方式：甲方指定 。

9.3 交付地点：甲方指定 。

十、合同款支付

10.1 付款方式：合同签订后支付合同总金额的50%；合同履约结束，经采购人验收合格后支付合同总金额的50%（不计利息） 。

10.2 当采购数量与实际使用数量不一致时，乙方应根据实际使用量提供产品和服务，合同的最终结算金额按实际使用量乘以中标单价进行计算。

十一、税费

11.1 本合同执行中相关的一切税费均由乙方负担。

十二、质量保证及售后服务

12.1 乙方应按招标文件规定和投标文件承诺的性能、技术要求、质量标准向甲方提供产品或服务。

12.2 乙方提供的产品或服务在服务期内因其本身出现质量问题，根据实际情况，经双

方协商，可按以下办法处理：

（1）更换：由乙方承担所产生的全部费用。

（2）合同终止处理：合同终止，乙方退还甲方支付的合同款，同时承担由此产生的全部费用，甲方不承担任何产生费用。

12.3 如在使用过程中发生质量问题，乙方在接到甲方通知后在小时内到达甲方现场。

12.4 在服务期内，乙方应对产品或服务出现的质量及安全问题负责处理解决并承担一切费用。

十三、项目验收

13.1 甲方依法组织履约验收工作。

13.2 甲方在组织履约验收前，将根据项目特点制定验收方案，明确履约验收的时间、方式、程序等内容，并可根据项目特点对服务期内的服务实施情况进行分期考核，综合考核情况和服务效果进行验收。乙方应根据验收方案内容做好相应配合工作。

13.3 对于实际使用人和甲方分离的项目，甲方邀请实际使用人参与验收。

13.4 如有必要，甲方邀请参加本项目的其他供应商或第三方专业机构及专家参与验收，相关意见将作为验收书的参考资料。

13.5 甲方成立验收小组，按照采购合同的约定对乙方的履约情况进行验收。验收时间、验收标准见招标文件验收内容。验收时，甲方按照采购合同的约定对每一项技术、商务要求的履约情况进行确认。验收结束后，验收小组出具验收书，列明各项标准的验收情况及项目总体评价，由验收双方共同签署。验收结果与采购合同约定的资金支付及履约保证金返还条件挂钩。履约验收的各项资料存档备查。

13.6 验收合格的项目，甲方根据采购合同的约定及时向乙方支付合同款项、退还履约保证金。验收不合格的项目，甲方依法及时处理。采购合同的履行、违约责任和解决争议的方式等适用《民法典》。乙方在履约过程中有政府采购法律法规规定的违法违规情形的，甲方将及时报告本级财政部门。

十四、合同内容的交付

14.1 乙方应保证合同标的安全运达甲方指定地点。合同标的涉及包装的应符合《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）》的规定。

14.2 使用说明书、质量检验证明书等一并提交甲方。

14.3 乙方在合同标的交付甲方 48 小时前通知甲方准备接收。

14.4 合同标的在交付甲方前发生的风险均由乙方负责。

14.5 合同标的在规定的交付期限内由乙方送达甲方指定的地点视为交付，乙方同时需通知甲方已送达。

十五、违约责任

15.1 甲方无正当理由拒收的，甲方向乙方偿付拒收标的总值的违约金。

15.2 甲方无故逾期验收和办理合同款支付手续的，甲方应按逾期付款总额每日向乙方支付违约金，最高限额为本合同总额的。

15.3 乙方逾期交付合同标的的，乙方应按逾期交付总额每日千分之六向甲方支付违约金，由甲方从待付合同款中扣除。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。

15.4 乙方交付的产品或服务不符合项目需求要求、乙方投标文件承诺及国家有关质量标准的，甲方有权拒收，乙方愿意更换但逾期交付的，按乙方逾期交付处理。乙方拒绝更换的，甲方可单方面解除合同，并由乙方赔偿由此造成的甲方全部损失。

十六、不可抗力事件处理

16.1 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。

16.2 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。

16.3 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。

十七、解决争议的方法

17.1 甲乙双方因合同签订、履行而发生的一切争议，应通过友好协商解决。如协商不成，按下列第（1）种方式解决：

（1）向连云港仲裁委员会申请仲裁。

（2）向合同签订地法院起诉，合同签订地在此约定为连云港市。

十八、合同生效及其他

18.1 合同经双方法定代表人或授权代表签字并加盖单位公章后生效。

18.2 本合同未尽事宜，遵照《中华人民共和国民法典》、《中华人民共和国政府采购

法》有关条文执行。

18.3 本合同正本一式两份，具有同等法律效力，甲方、乙方各执一份。

甲方：连云港市大数据管理中心

地址：连云港市海州区凌州东路9号政务服务中心3楼

法定代表人或授权代表：

联系电话：

2015.12.1

乙方：中国电信股份有限公司连云港分公司

地址：连云港市海州区兴隆路1号

法定代表人或授权代表：

联系电话：

附件：技术要求

云防护技术要求
▲1. 国内外云防护集群节点 IP 段≥25 个、线路类型≥70 个，且覆盖移动、电信、联通国内三大运营商； （投标文件中提供 IP 段及线路类型明细表证明材料并加盖投标人公章） ▲2. 可隐藏被防护网站的真实 IP； （投标文件中提供功能界面截图并加盖投标人公章） 3. 能有效防止 SQL 注入、命令注入、跨站脚本、代码执行、文件包含、远程命令、特殊攻击、恶意采集、WEB 服务器漏洞防护、路径遍历、文件保护、防篡改、防盗链、缓冲区溢出、防扫描等 Web 攻击； 4. 对使用 WebShell 进行攻击尝试和试图访问 WebShell 的 IP 地址支持屏蔽，并支持屏蔽时间的设置； 5. 能识别出各种 Web 扫描器的自动化扫描和攻击行为，并进行阻断； 6. 支持对防护的网站进行管理，包括：防御配置、站点的增删、站点 IP 地址的修改等； ▲7. 为了满足业务需要，能够对网站除 80、443 以外的非标准端口提供防护，并可以自助配置； （投标文件中提供管理平台自助配置的功能界面截图并加盖投标人公章） ▲8. 为了满足业务需要，能够支持的 http 协议防护端口不少于 300 个，https 协议防护端口不少于 100 个； （投标文件中提供防护平台端口支持统计表功能截图并加盖投标人公章） 9. 能根据 IP 地址，建立黑名单库或白名单库，阻止或者允许特定 IP 进行访问，支持禁止非授权 IP 访问网站后台管理地址或重要页面； 10. 支持提供网站安全报表，能够实时展示网站的总请求数、总流量、网站浏览人数、搜索引擎次数、缓存率和遭攻击次数，并能支持统计每小时网站的总请求数、总流量和网络浏览人数等； 11. 支持查看网站 WEB 应用攻击统计，实时展示 WEB 应用攻击次数、WEB 应用攻击 IP 数，支持展示高危攻击和低危攻击的比例。支持展示攻击地域分布，并展示地域对应攻击的攻击量和攻击量占比； 12. 支持查看总攻击次数以及各攻击类型的攻击的次数。攻击类型包括：恶意扫描、xss 跨站、文件注入、代码执行、文件包含、cc 攻击、远程命令、SQL 注入、webshell、恶意采集、特殊攻击； 13. 网站防护系统中，支持对黑客扫描尝试或定点攻击进行实时展示，内容至少包括攻击时间、攻击网址、攻击 IP、IP 归属地、攻击类型、攻击次数和处理结果等； ▲14. 支持微信或短信等实时告警，能够实时推送每天网站总请求数、总流量、网站浏览人数、遭受攻击次数； （投标文件中提供功能界面截图并加盖投标人公章） ▲15. 能够提供实时攻击视图，视图支持中国地图显示和全球地图显示。实时攻击视图中，要求实时显示内容至少包括：TOP5 攻击来源国家，TOP3 攻击来源国内 IP，TOP3 攻

击来源国外 IP，攻击类型，实时攻击数据等； **（投标文件中提供加盖投标人公章的承诺函，须明确承诺内容，格式自拟）** ▲16. 支持检查网站全部内容（不限制网站目录层级），如敏感信息、反动言论和淫秽等内容； **（投标文件中提供加盖投标人公章的承诺函，须明确承诺内容，格式自拟）** ▲17. 根据《网络安全法》需留存网站访问的日志，需提供日志下载功能，并区分原始日志，攻击日志和 CC 攻击日志下载； **（投标文件中提供平台功能界面截图并加盖投标人公章）** ▲18. 支持在不改变网站既有配置得情况下，无缝提供访客 IPv6 访问，提供 IPv6 DNS 解析服务，该 IPv6 DNS 具有抗 DNS DDoS 能力； **（投标文件中提供加盖投标人公章的承诺函，须明确承诺内容，格式自拟）** ▲19. 提供 IPV6 攻击防护能力，可抵御常见得 WEB 攻击类型； **（投标文件中提供加盖投标人公章的承诺函，须明确承诺内容，格式自拟）** ▲20. 网站安全加速服务： （1）基于 CDN 的基础网络架构，可以通过缓存、压缩、智能 DNS 解析等方式提升访问速度； **（投标文件中提供功能界面截图并加盖投标人公章）** （2）自动对未开启 Gzip 压缩的页面进行压缩，减少页面传输大小 90%以上，加快网页访问速度； **（投标文件中提供功能界面截图并加盖投标人公章）** （3）将页面缓存到节点上让访客就近访问，提升网页访问速度； **（投标文件中提供功能界面截图并加盖投标人公章）** （4）在浏览器中执行键盘操作刷新缓存。 **（投标文件中提供功能界面截图并加盖投标人公章）**
云监测技术要求
1. 主机漏洞检测，包含但不限于以下漏洞检测：浏览器服务漏洞、DNS 服务漏洞、FTP 服务漏洞、Web 服务漏洞、RPC 服务漏洞、SNMP 服务漏洞、弱口令漏洞、NFS 服务漏洞、路由器/交换机漏洞、DoS 攻击漏洞、文件共享漏洞； 2. Web 漏洞检测，包含但不限于以下漏洞检测：注入漏洞、XSS 漏洞、CSRF 漏洞、信息泄露、不安全的配置、未授权访问、反序列化、目录枚举、任意跳转、Struts2 漏洞、SSRF 漏洞、XML 实体注入（XXE）、jsonp 漏洞、弱口令漏洞和 ThinkPHP 漏洞。
渗透测试服务要求
从内部和外部分别进行测试，内部测试：经过用户授权后，测试人员根据站群站点的目标，利用专业手段进行测试从而对网络到系统访问、数据调取、存储等一系列的操作进行测试，主要用于检测外部威胁源和路径。具体要求如下： 1. 按照用户要求进行白帽人工测试服务。不仅要在系统中发现问题，而且要验证问题，并对应的整改技术方法和建议，如果是代码层面的漏洞，应在采购人单位整改时配合进行相关答疑；

▲2. 全年对网站群进行四次全面深入的白帽人工渗透测试服务，每季度一次； （投标文件中提供加盖投标人公章的承诺函，须明确承诺内容，格式自拟） 3. 白帽子人工测试安全服务成果输出物：《人工测试综合报告》，其中包含站点目标情况、漏洞情况、整改方案。
DDOS 防护服务
▲1. 网站正常访问带宽不低于 2G，保证网站的可用性； （投标文件中提供加盖投标人公章的承诺函，须明确承诺内容，格式自拟） ▲2. 能够防御每小时 CC 攻击不少于 300 个 IP，保证网站能正常使用； （投标文件中提供界面截图并加盖投标人公章） 3. 具备 HTTPGETflood、HTTPPostflood、HTTP 代理型攻击、慢速攻击、连接耗尽攻击、空连接攻击、SIPflood 等的防护； 4. 可提供网站实时攻防展示功能，以动态地理信息图等方式展示包括攻击 IP 所在地、被攻击 IP 所在地、目标端口、攻击方法等信息，并提供文本信息。
等级保护测评服务
对市政府门户网站开展等级保护测评。测评机构和测评规范等须符合我市公安部门要求。