连云港市政府采购合同

（合同编号：　　）

甲方：（买方）连云港市财政局

乙方：（卖方）中电鸿信信息科技有限公司

甲、乙双方根据 2025 年 11 月 06 日 连云港市财政局网络安全保障技术服务 项目（项目编号：JSZC-320700-XHZX-C2025-0036）竞争性磋商采购的结果，签订本合同。

一、合同内容

1.1 服务内容：

序号	服务项	服务内容描述	数量	频次
1	重要事件安全保障服务	安全保障工作主要为客户解决因人员经验以及安全技术方面和人员配置方面存在的缺陷。主动去配合及协助客户，处理在信息系统安全工作中出现的故障、安全事件以及安全管理方面的问题。弥补客户存在的缺陷，从而使客户业务系统具有高效的持续能力以及保证业务完整性、保密性。 具体服务内容： 1、保障前：“重保前”事先防御：联网资产探测梳理、应用系统漏洞扫描、渗透测试方案，为客户全面梳理资产信息，并减少客户应用系统安全隐患。 2、保障中：提供 7×24 小时远程安全监测和预警响应：应用系统可用性监测、重大安全事件预警； 3、保障后：“重保后”总结处置：将向客户提供重保时期应用系统监测报告、漏洞扫描报告和重大安全事件处置报告等。 4、合同期内重保期内需有两名专业安全工程师提供驻场服务，响应文件中提供承诺函并加盖供应商公章。	1	20 天
2	攻防演练服务	针对各业务信息系统进行模拟攻防演练，包括：漏洞扫描、渗透测试、模拟攻击、防护加强、攻击识别、系统加固建议等攻防全过程，可通过攻防演练提高安全事件的识别能力，发现网络安全防护体系的薄弱环节，并开展修补加固工作。可检验网络安全防护体系能否抵御强力攻击，完善互联网安全攻击事件应急处置措施及方案，提升安全事件的应急处理能力，增强客户内部相关技术人员的攻防能力和安全意识，多方位地提高客户信息系统的安全性和业务连续性。（含连云港市及下辖各区财政局） 具体服务内容以国家级攻防演练为时间节点，分为备战、决战及总结三个阶段： 一、备战阶段 1、发现安全检测、防护短板	1	1 次

		对客户现有防护体系进行全面地评估及分析，评估安全检测能力覆盖度。 2、补齐安全检测、防护短板 为客户提供设备租赁，补齐安全检测及防护能力，并对现有安全设备的防护策略进行梳理及优化，形成高效、高质的防护协同机制。 二、决战阶段 1、7*24 小时无缝隙监控 值守人员对安全设备异常流量及告警实时监控，快速报送给研判分析团队。 2、研判处置及溯源 对告警进行研判分析，快速定位被攻击服务器，并及时处置，同时对攻击方式、路径、结果进行溯源，绘制攻击者画像。 3、威胁情报共享 根据已建立的威胁情报共享机制，将攻击者攻击特征同步给各分支机构，统一下发，统一处置。 三、总结阶段 对攻防演练过程中发现的攻击行为进行复盘，发现演练过程中防守方各角色组之间配合的薄弱环节，固化攻防演练过程中的有效策略，进一步完善客户的安全防护体系。		
3	基线核查服务	安全基线是指 IT 资产(包括网络设备、安全设备、操作系统、中间件、数据库等)最低安全要求的配置。参考 ISO27001、等级保护 2.0 等标准，依托行业最佳实践和多年安全服务经验，针对不同 IT 资产的基线 checklist。通过自动化脚本或人工审核的方式对目标系统的安全基线进行合规性核查。 具体服务内容： 阶段一：实施方案授权：向客户提交《信息系统安全风险点项目核查实施方案》，使客户对风险点核查项目实施的所有细节和流程的知晓、所有过程都在客户可知可控下进行。 阶段二：信息收集确认：收集风险点核查项目的主机及网络设备资产的信息情况，填写《信息资产调查表》，完成信息资产信息收集。 阶段三：核查分析验证：核查信息系统信息业务系统脆弱状态，生成结果记录；完成目标信息系统技术与管理风险点核查操作实施；完成目标信息系统安全风险点核查结果分析验证； 阶段四：核查报告输出：提交汇报信息系统安全风险点核查成果与风险点解决方案；交付《信息系统安全脆弱核查报告》；	1	4 次

4	渗透测试服务	渗透测试是在用户授权和监督情况下，模拟黑客攻击流程，对目标信息系统进行攻击性测试，以外网服务为切入点，尝试逐步获取内网权限的过程，可披露信息系统在运行过程中可能被黑客成功利用的安全缺陷。 具体服务内容： 阶段一：实施方案授权：向客户提交《信息系统渗透测试实施方案》，与客户签订《信息系统渗透测试实施申请书》。使客户对信息系统渗透测试项目实施的所有细节和流程的知晓，所有过程都在客户可知可控下进行。 阶段二：渗透信息收集：对目标系统信息的网络架构分析，完成目标信息系统系统信息收集； 生成目标系统状态检测日志记录，完成目标信息系统安全状态扫描。 阶段三：渗透操作验证：对扫描发现的安全漏洞进行验证，验证各安全漏洞是否可以利用，执行渗透测试后，同时完成《渗透测试实施记录》，实施记录为在渗透测试过程中发现的安全隐患记录结果保存 阶段四：渗透报告输出：编写信息系统渗透测试实施报告，汇报信息系统风险测评结果与解决方案。 合同期内需提供一套便携式漏洞扫描系统给甲方使用。响应文件中提供承诺函并加盖供应商公章。	1	4 次
5	应急响应服务	应急响应服务主要包括应急处置力量的部署，对客户现有安全保障人员进行应急响应技能的培训，并建立应急响应机制，在客户无法以自身力量完成网络安全事件的处置时，安全服务团队以最快的速度到达现场提供专业支持。 具体服务内容： 阶段一：应急预案编制步骤：对单位或者部门的各项业务功能及各项业务功能之间的相关性进行分析，确定支持各种业务功能的相应信息系统资源及其它资源，明确相关信息的保密性、完整性和可用性要求。制定应急响应策略，提供了在业务中断、系统宕机、网络瘫痪等信息安全事件发生后快速有效地恢复信息系统运行的方法。输出《应急响应安全预案与附件》。 阶段二：应急演练实施步骤：根据客户现有应急响应计划预案，编写演练计划或脚本。输出《应急响应演练计划》 阶段三：应急事件处理步骤：在安全事件得到适当处理后，会为客户提交一份报告，详细描述安全事件的	1	年

		起因、造成的损失以及以后对这类安全事件所应采取的防范措施和步骤。输出《应急响应事件处理实施方案》《应急响应事件处置结果报告》		
6	安全通告服务	每周向客户提交一份安全通告，包括（不限于）最新网络基本安全态势、最新网络漏洞、最新安全威胁、最新安全资讯	1	每周
7	外网安全运营服务	服务期间由服务方提供安全设备对财政外网进行全流量收集，提供边缘侧的数据分析能力，该安全设备无需向安全服务平台上报业务流量，通过本地 AI 算法进行安全检测，并将检测结果以日志形式上报给云服务平台。安全设备将处理过的数据上传安全服务平台后，安全服务平台具有AI 计算中心，全球威胁情报库，智能算法，会对该数据进行威胁情报库对比，来检测数据中心是存在威胁数据，如果监测到威胁数据，平台会全自动对安全设备下达阻断或者隔离指令，进行威胁情况隔离。 服务期间发现用户网络或系统突发安全事件时，第一时间安排运营中心安全专家进行响应，安全服务平台对重点漏洞和木马进行智能判断进行阻断，运营中心响应人员进行线上或线下处置，进行规避风险操作，使得安全事件有可能引发的安全事故、风险概率、危害损失降到最低。	1	年

1.2 服务要求：

服务内容		具体内容
安全运营服务周期		提供本地安全防御节点，本地安全防御节点与云端安全分析作为安全服务整体交付。安全服务实际服务周期 1 年，服务包含：安全防御节点 1 年在本地的防护+云端分析服务以及 7*24 小时监测预警与线下问题处置服务。响应文件中提供承诺函并加盖供应商公章。
安全服务工具	安全规则功能	▲安全防御节点系统预定义 IPS 签名数量≥11000，支持用户自定义签名规则，支持正则表达式。（响应文件中提供功能截图并加盖供应商公章）
	应用防护	▲安全防御节点支持对常见应用服务（HTTP、FTP、SSH、IMAP）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能。（响应文件中提供功能截图并加盖供应商公章）
		▲安全防御节点支持恶意域名过滤，实现对 C&C 进行阻断。（响应文件中提供功能截图并加盖供应商公章）
	自动阻断	▲基于情报库与本地特征，进行威胁源匹配并实现威胁事件自动阻断。（响应文件中提供功能截图并加盖供应商公章）
	日志采集	▲基于数据流量进行分解与回传，匹配关键特征与动作，识别恶意风险。实时上传本地事件与日志。（响应文件中提供功能截图并加盖供应商公章）
安全运营中心	运营服务界面	▲提供可通过互联网访问的用户注册界面，用户可进行服务的自助正式上线注册。（响应文件中提供提供注册服务的互联网地址及注册界面截图并加盖供应商公章）

	运营中心能力	▲提供基于安全分析服务能力，无需在客户处部署任何软件平台，服务基于上送的安全日志能够进行日志的聚合、分析、判定动作，去除安全日志的噪音，可在安全日志分析后标注为“确认为攻击”、“已下发告警”等状态，为用户提供精准的安全威胁事件展示。（响应文件中提供提供云端安全服务分析运营平台操作界面截图并加盖供应商公章）
	监测预警	▲提供基于安全运营服务平台的针对终端用户的 7*24 小时的监测预警服务。并基于用户终端界面所产生的日志与告警，进行指导闭环与跟进处理等工作。（响应文件中提供证明材料并加盖供应商公章）
	应急响应	▲针对失陷主机、重大攻击威胁等关键安全告警，安全运营服务平台将给用户发送告警短信及告警邮件，及时指导进行响应。（响应文件中提供功能截图并加盖供应商公章）
	应急处置	▲提供当用户网络或系统突发安全事件时，通过应急响应服务提前规避风险，并进一步进行现场处置，通过技术角度或者解决方案的形式，解决安全风险。（响应文件中提供证明材料并加盖供应商公章）
	服务报告	▲需按周、按月为用户提供安全服务报告，安全服务报告将以邮件形式发送至用户注册邮箱。通过安全服务报告，客户可清晰了解以下信息：1、服务时间；2、失陷主机数量及详情；3、威胁防护次数及趋势；4、攻击源数量及趋势；5、恶意文件数量及趋势；6、网络应用层流量基于用户、应用维度的分布情况。（响应文件中提供功能截图并加盖供应商公章）
用户服务平台	数据总览	▲用户可登陆部署在互联网的用户安全运营服务平台界面，查看现网外部威胁、失陷主机、威胁文件传输等安全事件，并可对外部威胁进行黑名单下发、可对失陷主机进行手工封禁。（响应文件中提供功能截图并加盖供应商公章）
	工单系统	对现网问题支撑、咨询线下人工服务等需提交工单场景，用户可通过安全运营服务平台的工单功能，提交工单并跟踪工单处理进度。
	全局白名单	▲可通过用户安全运营服务平台下发全局白名单，对多台本地安全防御节点统一下发白名单。（响应文件中提供功能截图并加盖供应商公章）
	资产梳理	可查看资产风险分布（正常资产、失陷资产等）统计。
	服务订阅	可通过用户安全运营服务平台续订服务，并可通过平台查看服务开通状态。

1.3 服务标准：详见采购文件。

1.4 补充条款：服务期内，未经甲方书面同意，供应商不得擅自更换项目组人员。

二、合同金额

2.1 本合同金额为人民币（大写）：柒拾万肆仟元整元整（¥704000）。

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约定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 乙方应按采购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：自合同签订之日起一年。

九、合同内容的交付

9.1 交 付 期：自合同签订之日起一年。

9.2 交付方式：项目需求单位指定方式。

9.3 交付地点：项目需求单位指定地点。

9.4 乙方应保证合同标的安全运达甲方指定地点，合同标的在交付甲方前发生的风险均由乙方负责。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。使用说明书、质量检验证明书等（如有）一并提交甲方。

9.5 乙方在合同标的交付甲方 48 小时前通知甲方准备接收。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、合同款支付

10.1 付款方式：合同签订后，服务人员进场后支付合同总价的 50%，服务满一个月，并出具服务报告，支付合同总价的 45%，服务期满验收合格后支付合同总价的 5%。

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 乙方应按采购文件规定和响应文件承诺的性能、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 48 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、

验收标准见采购文件验收内容。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《中华人民共和国民法典》。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、违约责任

14.1 甲方无正当理由拒收的，甲方向乙方偿付拒收标的总额 百分之五 的违约金。

14.2 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 万分之五 向乙方支付违约金。

14.3 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额 百分之五 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。

14.4 乙方交付的产品或服务不符合采购文件规定标准、乙方响应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。

十五、不可抗力事件处理

15.1 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的，则合同履行期可延长，其延长期与不可抗力影响期相同。

15.2 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。

15.3 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。

十六、解决争议的方法

16.1 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（2）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。

十七、保密条款

17.1 未经甲方的事先书面批准，乙方不得以任何形式或任何方式将实施过程中接触到的信息和/或其中的任何部分，披露或透露给任何第三方。乙方有义务妥善保管保密信息，不得复制、泄漏或遗失。乙方亦不得依据保密信息，就任何问题，向任何第三方做出任何建议。

17.2 本保密条款在双方合作项目变更、解除、终止后十年内依然有效。本保密协议效力不因双方合作项目主协议的无效、撤销或变更而改变。甲方保留在甲方认为必要的情况下收回所提供的保密信息及其使用权的权利。

17.3 如任何一方违反本协议，违约方应按照《中华人民共和国民法典》的相关规定承担违约责任，另一方有权根据其违反的程度以及造成的损害后果要求对方赔偿因此遭受的损失。

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 陆 份，具有同等法律效力，甲方执 肆 份、乙方执 贰 份，甲方报一份至政府采购监督管理部门。

甲方：连云港市财政局　　乙方：中电海信信息科技有限公司

地址：连云港市海连中路 99 号　　地址：南京市玄武大道 699-1 号

法定代表人或授权代表：　　法定代表人或授权代表：

联系电话：　　联系电话：

签订日期：　2025　年　12　月　1　日