合同编号：（2025）SJ011

福田区政府计算机网络安全和信息安全服务项目合同（2025－2026 年）

甲方：深圳市福田区民意速办和智慧城市建设中心

统一社会信用代码：124403046610332564

负责人：

地址：深圳市福田区华富街道深南大道 1006 号国际创新中心 F 座 3 层

乙方：北京启明星辰信息安全技术有限公司

统一社会信用代码：911101088020115538

负责人：

地址：北京市海淀区东北旺西路 8 号 21 号楼启明星辰大厦 102 号

根据《中华人民共和国民法典》、2025 年 4 月 8 日福田区政府计算机网络安全和信息安全服务项目（2025-2026 年）（项目编号：FTCG2025000030）”招标结果（中标通知书）和“招标文件”，就乙方承担福田区政府计算机网络安全和信息安全服务的相关事宜，经双方协商一致，达成本合同。

第一条、合同金额

1、本合同总金额为人民币大写：**贰佰玖拾贰万陆仟圆整（￥2,926,000.00 元）**，本合同服务期自 2025 年 4 月 24 日至 2026 年 4 月 23 日，共计 12 个月。本合同以人民币进行结算。

2、乙方的开户银行资料：

乙方开户银行：

乙方开户名称：北京启明星辰信息安全技术有限公司

乙方银行帐号：

第二条、合同的服务内容

乙方承担福田区政府政务网络内运行的网络设备、服务器、政府门户网站、数据库及其存储系统、业务应用系统、区机关各单位互联网网站、移动应用等为期 12 个月的网络安全及信息安全服务。本合同的具体服务要求如下：

一、安全服务的主要内容

（一）总体服务要求：

在福田区政府政务网络安全系统集成防护的情况下，保障在线运行的信息系统安全，实现计算机网络主干不因安全原因而瘫痪，重要数据不被非法窃取，区政府网站页面不被篡改，保障互联网网站及信息系统的安全运行，信息系统安全管理有序进行的安全服务目标。

（二）具体工作内容：

主要包括日常安全服务、信息安全等级保护服务、渗透测试服务、应急保障服务、专项安全服务、设备维保服务、SSL 域名证书使用服务、其他服务要求等八个方面。

1.日常安全服务

（1）常规安全漏洞检测。每月对福田区机关单位政务网络应用系统、服务器、计算机终端等信息化资产完成不少于一轮安全扫描，出具漏洞检测报告。

（2）上线安全检测。根据各机关单位福田区政务云业务申请，在应用系统上线前对拟上线系统进行一次全面的安全检测，包含但不限于源码检测、漏洞扫描、逻辑漏洞检测等方式，指导开展测试问题修复并复测，确保应用系统上线时安全风险最小化。

（3）信息化资产管理。协助采购人对福田区机关单位信息系统和服务器等信息化资产进行管理，包括对福田区机关单位信息系统和服务器资产做好备案登记，在资产入库、变更、退库等环节执行调整。

（4）防病毒管理。每月对防病毒软件病毒库确认更新情况，对福田区政务网主机服务器、终端电脑进行病毒查杀。

（5）安全加固指导。对上线安全检测、常规安全漏洞检测、应用系统安全基线核查、渗透测试等工作中发现的问题提出加固意见，指导责任单位及时整改。

（6）安全顾问咨询。从安全管理、安全合规、安全运营等方面提供咨询服务，包括但不限于制度修编、技术论证和方案咨询等。

（7）安全策略巡查。根据实际监测的风险隐患及福田区各机关单位业务申请，优化网络安全策略，做好配置和安全策略的变更记录，并定期做好安全设备配置备份。

（8）制度修编。根据国家、省、市相关法律法规，结合福田区政务网络安全体系建设情况，协助完善网络安全制度和流程管理文件。

（9）安全服务报告。每个月对福田区政务网络和主机系统的安全情况及服务工作进行总结，并向采购人提交书面的安全服务报告。

2.信息安全等级保护服务

根据国务院信息化工作办公室颁布的《电子政务信息安全等级保护实施指南（试行）》，按照国家《信息安全等级保护管理办法》和《信息安全技术网络安全等级保护定级指南》（GB-T 22240-2020 ），协助进行相应的等级保护合规和监管工作。做好迎接市信息安全主管部门对福田区信息系统安全等级保护检查的准备工作。

3.渗透测试服务

针对福田区机关事业单位不少于150个信息系统、网站进行渗透测试，找出存在的安全漏洞及风险，出具渗透报告，并督促责任单位完成漏洞整改。主要内容包括：（1）每3个月对机关单位的互联网系统开展至少一次渗透测试；（2）每6个月对医院、学校、国企等行业单位互联网系统开展至少一次渗透测试；（3）每6个月对机关单位的政务网系统开展至少一次渗透测试。

4.应急保障服务

（1）应急预案修编。协助修订、完善福田区数字政府网络安全和数据安全事件应急预案。

（2）应急响应。提供应急技术支撑服务，以满足网络安全突发事件处置工作的相关要求。需提供7×24小时安全应急服务，当福田区政务网络及其主机系统发现有安全问题时，应立即组织查明发生问题的原因，采取有效的措施尽快恢复网络和主机的正常运行。

（3）应急演练。全年至少开展一次网络安全事件应急演练，根据需要开展视频拍摄和视频剪辑等工作。

5.专项安全服务

（1）风险评估。根据国家、省、市相关标准，对福田区政务网络指定信息系统进行网络安全风险评估、供应链安全风险评估，出具风险评估报告。

（2）防范网络钓鱼。及时通报最近网上流行的安全陷阱类型（如通过邮件、聊天软件、网络下载等途径进行网络钓鱼，传播病毒、安装木马程序等）及其识别和防范方法，每年至少组织开展1次网络钓鱼测试，提升个人安全意识水平。

（3）供应链安全治理。针对福田区信息系统情况，协助开展福田区软件供应链安全在组织管理、制度建设、人员管理、供应商管理等方面的工作。

（4）宣教培训。组织开展网络安全宣传和教育工作，每年至少开展 1 次全区工作人员年度网络安全培训工作。

（5）网络安全联合检查及迎检。根据深圳市党政机关信息安全绩效评估和联合检查指标要求开展自查自纠，协助整理佐证材料。协助开展全区党政机关网络安全现场检查。

6.设备维保服务

（1）设备巡检。每季度安排专业技术人员，对福田区政务网络安全应用软件、安全设备等进行现场巡检对发现的问题及时进行处理，及时发现问题、处理故障，形成巡检报告。

（2）故障修复。发生故障后立即组织技术人员分析故障原因，并协调安全设备厂商做好故障修复工作。

（3）升级更新。组织对网络安全设备开展漏洞库升级更新等工作,确保设备可用性。

7.SSL 域名证书使用服务

服务期内提供 SSL 域名证书使用服务，包括通配符 OV 型一套、国密一套，通过加密传输（如 TLS/SSL 协议）保护用户数据（如密码、支付信息）不被窃取或篡改，保障甲方所监管的信息系统、网站安全。

8.其他服务要求

（1）乙方负责提供并保管其安全技术服务人员的工作电脑；服务期间若发生的交通费、误餐费等均由乙方承担。

（2）乙方负责其安全技术服务人员的工资、奖金、福利待遇及其他一切费用，必须为其安全服务人员购买劳动保险，对其安全服务人员做好安全生产教育。如乙方的安全技术服务人员在工作现场发生工作事故或工伤事故的，由乙方负全责。

（3）若乙方指派到现场服务的安全技术服务人员的工作表现不能符合要求，且经过教育后仍不能改正的，可要求乙方更换相关技术安全服务人员。

（三）服务范围

本项目的服务范围为福田区电子政务外网所有重要信息化资产，包括安全系统、业务系统、服务器、计算机终端等。

（四）项目管理要求

中标方应提交如下常规工作记录：1.每周提交周工作总结和下周工作计划，

2.每季度提供服务报告，包含但不限于以下内容：安全设备策略维护情况、系统上线检测情况、漏洞扫描及复扫情况、安全设备可用性巡检情况、重点工作完成情况。

第三条、付款方式

对本合同第一条的合同总金额，双方约定按照服务进度进行付款，具体付款步骤如下：

1、本合同签字生效后，在甲方收到乙方提供的等额合法有效的税务发票后，甲方办理相关付款资料，审批流程完成且财政资金到账后 15 个自然日内，甲方向乙方支付合同总金额的 30%服务费，**即人民币（大写）人民币捌拾柒万柒仟捌佰元整（877,800.00 元）**。

2、乙方完成 6 个月的驻场技术服务工作，乙方按合同履行服务工作任务并通过双方组织的验收合格后，在甲方收到乙方提供的等额合法有效的税务发票后，甲方办理相关付款资料，审批流程完成且财政资金到账后 15 个自然日内，甲方向乙方支付合同总金额的 20%服务费，**即人民币（大写）伍拾捌万伍仟贰佰元整（585,200.00 元）**。

3、合同服务期满，乙方按合同履行服务工作任务并通过双方组织的验收合格，在甲方收到乙方提供的等额合法有效的税务发票后，甲方办理相关付款资料，审批流程完成且财政资金到账后 15 个自然日内，甲方向乙方支付合同剩余的 50%服务费，**即人民币（大写）壹佰肆拾陆万叁仟元整（1,463,000.00 元）**。

第四条、双方的责任

（一）甲方责任：

1、应按合同第三条的约定按时向乙方支付合同款。

2、在本合同执行过程中，甲方应为乙方提供方便并积极配合。

3、在乙方的协助下，制定和不断完善计算机网络安全管理制度，强化网络安全管理。

4、有义务保守乙方与本合同执行有关的所有技术和商业机密，不向第三方泄漏。

（二）乙方责任：

1、乙方应投入投标承诺的足够的技术力量，以确保按期完成本合同第二条规定的服务内容。在安全服务期间，未经甲方同意，乙方不得随意抽调或更换乙方承诺的驻场服务人员，如果甲方认为乙方的驻场服务人员的技术能力或管理能

力不能胜任本合同的服务要求，甲方可以要求乙方更换有关人员。乙方不得拒绝甲方要求，如乙方拒绝甲方要求，即构成违约，造成后果由乙方自负并应向甲方支付本合同总金额3%的违约金。

2、承诺向甲方提供及时、准确、高效、优质的安全服务，以保证甲方的网络和主机系统具有高安全性。

3、遵守福田区政府及甲方在网络及信息安全方面的要求，承诺将保守甲方网络和主机系统所有参数和系统资源的秘密，不向第三方泄漏。

4、承诺需精通电子政务网络及信息安全体系，对相关安全重点具有敏锐洞察力。

5、承诺有较强的信息安全技术服务力量和服务团队。

6、承诺具有安全等级保护定级、安全域规划实施和访问控制的实际工作经验。

7、承诺掌握信息安全防护的最新技术，了解电子政务网络和安全体系的弱点，有一定的先知先觉的预判能力。

8、承诺具有网络攻防经验，可以应对任何复杂的信息安全问题，在信息安全领域有较强的研发能力。

9、若乙方指派的安全服务人员的工作表现不能符合甲方的要求，且经过教育后仍不能改正时，乙方须按甲方的要求更换服务人员。

10、安全服务人员的工作电脑由乙方提供并负责保管，服务期间发生的交通费、误餐费等由乙方承担。

11、承诺所有参与本合同的乙方人员，在安全服务前须与甲方、乙方签订保密协议（详见附件）。在安全维护和安全服务期间及安全维护期满后的5年内，不得将服务中涉及的我区网络、主机系统和业务应用系统的网络结构、设备配置等所有安全信息（含文档、资料等），提供给其它第三方的单位或个人查看或使用。

12、乙方负责安全服务人员的工资、奖金、福利待遇及其他一切费用，乙方必须为其安全服务人员购买劳动保险，并对进入甲方工作现场的工作人员加强安全生产教育，为现场工作人员购买安全保险。若出现安全事故造成乙方工作人员伤亡的情况完全由乙方承担责任，甲方对此不负任何责任。

13、乙方有义务加强对本单位工程实施人员的安全保密教育，遵守福田区政府及甲方在网络及信息安全方面的要求。

第五条 人员及投入设施要求

人员要求：

根据本项目的招标要求，乙方应派驻不少于 8 人常驻甲方办公场所，其中 1 人为项目经理。驻场服务人员需按照甲方的作息时间和甲方的工作安排开展工作，非驻场服务人员的安全服务工作根据需要由甲、乙双方具体商定。需常备 1 名机动安全专家，以便于在紧急情况或工作量较大时，可随时抽调熟悉相关环境的工程师进行补充。未经过甲方同意，不得随意更换驻场技术服务人员；甲方可对拟安排的驻场服务人员进行提前面试，如面试未通过，乙方须提供与投标文件同等资质的其他人员进行替换。

项目经理权利和责任如下：

1、项目联络；

2、组织和协调项目进展；

3、代表委派方签署合同变更的文件（包括但不限于项目相关文件的签字确认权）。

乙方如需更换项目经理，需经甲方同意后进行更换，更换的项目经理具有至少五年与本项目类似的安全服务工作经验，并按甲方招标文件的要求和乙方投标文件的承诺，**具有不低于乙方投标文件所承诺的资格要求**。

技术服务人员素质要求：

乙方应按照投标文件指定的驻场服务人员到甲方现场进行驻场服务。乙方如需更换，需经甲方同意后进行更换，更换的现场服务的人员须具有同类安全服务项目至少三年的工作经验，并按甲方招标文件的要求和乙方投标文件的承诺，**具有不低于乙方投标文件所承诺的资格要求**，能够独立、按时完成现场服务工作，遵守甲方的工作作息时间。

投入设施要求：

（1）用于信息安全服务的检测设备由乙方负责提供。

（2）提供漏洞扫描检测工具。具备开展业务信息系统服务器漏洞扫描、网络层扫描、移动安全漏洞扫描及对外服务网站应用层扫描所使用的专业检测工具。

成果要求：

服务过程产生的所有过程文档、原始数据、扫描报告、正式报告等必须进行电子或纸质归档，在项目结束后一并移交给甲方。

技术资料：

1、安全运维服务过程产生的所有过程文档、原始数据、扫描报告、正式报告等必须进行电子归档，在项目结束后一并移交给甲方。

2、信息安全风险评估报告须符合深圳市信息安全主管部门的要求。

3、协助进行相应的等级保护合规和监管工作，整理汇总系统等级保护备案证明、测评结果通知书等资料。

4、信息系统应急预案必须以信息系统真实业务流程为基础，真实科学准确。演练工作每年至少开展 1 次。

第六条、违约责任

1、如甲方未在规定的时间内向乙方支付合同款，甲方应按超过的天数每天向乙方支付本合同第三条中到期应付而未付金额的**千分之三**作为违约金，但每次违约金支付不得超过当次到期应付而未付金额的 **5%**。

2、如乙方未按每三个月一次对甲方的网络及主机系统进行安全评估和审计或者未在该三个月内提交安全审计报告，每少一次，甲方将全额扣除该三个月内乙方的服务费，同时乙方应向甲方支付三个月的服务费金额的 **10%**作为违约金，但由于甲方自身原因造成的除外。因此导致甲方聘请第三方提供服务产生的费用等一切损失均由乙方承担，此项支出费用甲方可在乙方的安全服务费中扣除，不足部分甲方可向乙方继续追偿。

3、如乙方未对福田区政务网络中的所有主机服务器进行安全检测、漏洞修补、安全巡检、安全审计等服务，甲方将按月扣除乙方的维护费用。

4、如乙方在一个月内（当月一日至当月最后一天）未每天派乙方承诺的至少 8 名维护服务工程师驻场检查网络和主机系统的安全状况、安全补丁程序，甲方将扣除乙方当月的维护费外，同时乙方须向甲方支付该月维护服务费的 **10%** 作为违约金，甲方可在支付给乙方的服务费中扣减该违约金（由于甲方自身原因造成的除外）。因此导致甲方聘请第三方提供服务产生的费用等一切损失均由乙方承担，此项支出费用甲方可在乙方的安全服务费中扣除，不足部分甲方可向乙方继续追偿。

5、如果乙方每月向甲方发送安全通报少于 2 次（在当月上半月或下半月发送超过 1 次的按 1 次计算），少于 2 次的月份，每少一次，乙方须向甲方支付该月维护费的 **10%**作为违约金，甲方可在支付给乙方的服务费中扣减该违约金。因此导致甲方聘请第三方提供服务产生的费用等一切损失均由乙方承担，此项支

出费用甲方可在乙方的安全服务费中扣除，不足部分甲方可向乙方继续追偿。

6、如发现乙方工作人员泄漏甲方的网络和主机系统的参数，甲方认为可能导致甲方利益受损，本合同自动终止；若合同终止履行，甲方向乙方支付服务款的期间为本合同生效之日起至发现乙方人员泄密时止，同时乙方须向甲方支付本合同总金额的**20%**作为违约金，甲方可在支付给乙方的服务费中扣减该违约金。问题严重的，甲方保留向公安部门检举，追究乙方管理责任和相关责任人的泄密刑事责任的权利。因此导致甲方的一切损失均由乙方承担，此项支出费用甲方可在乙方的安全服务费中扣除，不足部分甲方可向乙方继续追偿。

7、如因乙方未及时给甲方的主机系统安装补丁，未向甲方建议关闭系统（网络和主机）中不必要的服务或端口，或经双方确认关闭但乙方未关闭的原因导致甲方服务器的 Web 页面被非法篡改，或者造成甲方的网络系统瘫痪，经权威的独立的第三方（如深圳市公安局网监分局）检测鉴定为乙方责任的，乙方须向甲方支付人民币**贰万元**作为违约金。甲方可在支付给乙方的服务费中扣减该违约金。同时甲方保留解除本合同的权利。因此导致甲方聘请第三方提供服务产生的费用等一切损失均由乙方承担，此项支出费用甲方可在乙方的安全服务费中扣除，不足部分甲方可向乙方继续追偿。

8、为保障甲方业务应用系统和网络系统的正常运行，避免事故发生，乙方可根据信息安全体系的实际需要向甲方提供安全系统建议方案或调整方案。如因甲方未采纳乙方建议而导致的安全事故，经权威的独立的第三方（如深圳市公安局网监分局）检测鉴定后，确系前述原因造成损失的，可完全免除或部分免除乙方的赔偿责任，免责比例由甲乙双方协商确定。

9、在安全服务期间，若出现由于乙方人员泄露福田区政府网络和信息系统参数的情况，造成甲方网络系统、信息系统损失和产生不良政治后果的，甲方保留对其本人和乙方采取法律诉讼的权利。因此导致甲方的一切损失均由乙方承担，此项支出费用甲方可在乙方的安全服务费中扣除，不足部分甲方可向乙方继续追偿。

10、在合同服务期内，出现以下情况的视为安全技术服务质量没有达到要求，将追究乙方的违约责任，违约金额从服务费中核减：

（1）因乙方原因导致信息安全工作被采购人上级点名批评的，每次扣除合同金额 1 万元。

（2）因乙方工作不力，未能及时发现安全隐患，以致信息系统（网站）被上级部门渗透成功，且造成较大影响时，按每个系统（网站）扣除合同金额 1 万元。

（3）发现乙方技术服务人员在工作时间从事其他与信息安全工作无关的，第 1 次警告，从第 2 次起，每次扣除合同金额 1000 元。

（4）因乙方工作不到位，导致发生信息安全事件被上级部门通报，或导致采购人在市信息安全主管部门检查中扣分的，扣除合同总金额的 20%。

第七条、资料及保密

1、对于一方向另一方提供或使用的资料和秘密信息，另一方负有安全保护和保密的责任，不得向任何第三方透露、不得随意丢弃而造成泄密；对于本合同项目的最终成果及阶段性成果，双方均负有保密义务。

2、未经双方授权代表签字认可，任何一方不得向第三方透露本合同内容。

3、本条款不因本合同或其下项目的变更、解除或终止而失效。

4、乙方人员通过本项目的实施接触到福田区电子政务网络、应用系统的资料、配置或业务数据，以及个人隐私、甲方的工作信息等，乙方均有义务和责任对甲方上述网络、网站、服务器系统和业务应用系统的信息资料或数据进行保密。若乙方及其工作人员未履行好保密职责，发生信息泄漏等行为，乙方需无条件承担甲方的一切损失，挽回对甲方造成的不利影响，并承担相应的法律责任。

5、承担安全服务的技术人员必须与采购人签定安全保密协议。

第八条、本合同的修改

对本合同的条款的任何修改，必须经甲乙双方协商同意后，以本合同的补充协议方式，以书面的形式订立，该补充协议与本合同具有同等法律效力。

第九条、其他事宜

1、本合同的适用法律：本合同的甲、乙双方应遵守《中华人民共和国民法典》及其他相关的法令和条例。因本合同或与本合同有关的争议，双方应通过协商解决；协商解决不成，向甲方所在地法院提起诉讼，诉讼裁判对双方均具约束力。

2、不可抗拒力：由于不可抗力的事故或自然灾害导致一方或双方违约，由甲、乙双方协商解决。但双方均有义务采取一切必要的措施减少损失。有义务采取措施而不采取造成严重后果，由有义务采取措施一方承担相应责任，并向另一方支付总金额 3%的违约金。

3、乙方就本同项目的“投标文件”与本合同具有同等的法律效力。投标文件中与本合同条款有差异的部分，按照本合同条款的规定执行。在本合同中未涉及但在乙方的“投标文件”中涉及的，按“投标文件”中的条款执行。

4、本合同服务期自 2025 年 4 月 24 日至 2026 年 4 月 23 日，共计 12 个月（本项目为长期服务政府采购项目，服务期限最长为三十六个月，合同一年一签，合同期满前一个月，甲方对履约情况进行考核，考核合格的，可按原合同条款续签合同；如甲方对履约考核情况不满意，甲方不再续约）。

5、本合同未尽事宜，双方可协商解决，并可签订补充协议，该补充协议与本合同具同等法律效力。

6、本合同附件与本合同具有同等的法律效力。若附件与本合同有冲突的地方，以本合同为准。

7、本合同自甲、乙双方授权代表签字并加盖双方主体印章之日起生效。本合同壹式陆份，甲方执肆份，乙方执贰份，均具同等法律效力。

8、如果后续年度经人大审议通过的部门预算中，该采购项目预算金额较提前采购计划金额发生变化的，双方可根据相关规定签订补充协议或终止协议执行。

（以下为签署页，无正文）

甲方：深圳市福田区民意速办和智慧城市建设中心（盖章）

授权代表（签字）：[redacted]

日 期：2025 年月日 2025年4月24日

乙方：北京启明星辰信息安全技术有限公司（盖章）

授权代表（签字）：[redacted]

日 期：2025 年月日 2025年4月24日

安全保密协议

甲方：深圳市福田区民意速办和智慧城市建设中心

乙方：北京启明星辰信息安全技术有限公司

乙方在甲方网络安全服务过程中，为确保甲方计算机网络相关信息的保密性，依照《中华人民共和国计算机信息安全保护条例》、《中华人民共和国著作权法》、《计算机软件保护条例》和《中华人民共和国网络安全法》及有关部门商业信息法规，达成此保密协议。

一、签订对象

参与甲方的安全服务项目的乙方技术人员，在进行安全服务前必须在本协议第六条的表格中签署本人名字，查验身份证，留存本人身份证复印件及工作简历。凡未在第六条的表格中签名备案的乙方人员，不能参与本合同的安全服务工作。

二、保密的内容和范围

乙方（含乙方参与安全服务的技术人员）在执行本合同的安全服务期间，掌握的或所接触到甲方的计算机网络系统和业务应用系统的一切技术秘密、网络设备信息、网络结构、IP 地址资源、安全设备信息、业务系统的资料和数据等，均属于保密范围。

三、协议双方的权利和义务

1、甲方有权拥有乙方在安全服务中所有技术资料及相关文档。

2、甲方拥有对安全服务中的所有知情权、询问权及掌握项目进度的权力。

3、乙方必须管理好自己的安全服务人员，乙方（含乙方参与施工的技术人员）不得将第 2 条所及的保密内容非法披露给外单位、转让给第三者或自行使用。

四、保密协议的期限

本协议自签订之日起，有效期为**伍年**。

五、违约责任

若乙方（含乙方参与安全服务的技术人员）泄密，需无条件向甲方赔偿因泄密所造成的相关损失，并承担相应的法律责任。

六、乙方在甲方进行安全服务的技术人员名单

说明：乙方的安全服务技术人员在执行安全服务前，必须在上表的“签字”栏内签字确认后，才能在甲方工作现场进行安全服务。

七、其他

本协议自甲、乙双方授权代表签字盖章之日起生效。本协议壹式叁份，甲方执贰份，乙方执壹份。

（以下为签署页，无正文）

甲方：深圳市福田区民意速办和智慧城市建设中心（盖章）

授权代表（签字）：[redacted]

日　　期：2025 年 4 月 24 日

乙方：北京启明星辰信息安全技术有限公司（盖章）

授权代表（签字）：[redacted]

日　　期：2025 年 4 月 24 日