中山市小榄人民医院

2025-2026年度网络与数据安全服务项目

招标采购需求书

1 总则

1.1 响应供应商报价应包括服务项目相关的全部费用，如咨询规划、方案设计、需求调研、系统集成、数据处理、测试评估、设备维护费用、税费、人员差旅费、保险费、培训和质保等。在项目实施过程中出现报价内容的任何遗漏，均由成交供应商负责相关费用，采购人将不再支付任何费用。

1.2 响应供应商须对第 4 节《2025-2026 年度网络与数据安全服务清单》逐行进行单项报价。

1.3 采购文件中凡有“★”标识的内容条款为关键条款，响应供应商必须对此作出回答并完全满足这些要求，不可以出现任何负偏离，对这些关键条款的任何负偏离将视为无效响应。加注“▲”的内容为重点评标项目，响应供应商必须对该

标识项目按照要求进行真实应答描述。

★1.4 本项目不接受联合体投标，成交供应商不得以任何方式转包本项目。**（提供承诺函）**

★2.供应商资格要求：

响应供应商必须具备下列规定的条件，并提供相应的证明材料：

2.1 必须是具有独立承担民事责任能力的在中华人民共和国境内注册的企业法人或其他组织，具备相应的经营范围。分公司报名的，还需提供投标人及其总公司营业执照，若投标人及其总公司之间存在多级授权的，则一并提供中间授权公司营业执照。**（提供承诺函）**

2.2 单位负责人为同一人或者存在直接控股、关联关系的不同投标人，不得参加同一项目下的招标活动。**（提供承诺函）**

2.3 有良好的信誉、健全的财务会计制度。**（提供承诺函）**

2.4 无重大违法记录或失信记录。**（提供承诺函）**

2.5 依法缴纳税收和社会保障资金。**（提供承诺函）**

2 采购内容

序号	名称	数量	限价
1	中山市小榄人民医院 2025-2026 年度网络与数据安全服务项目	1	70 万元

3 项目概述

3.1 项目名称

中山市小榄人民医院2025-2026年度网络与数据安全服务项目

3.2 项目背景

依据国家网络安全等级保护相关规范与标准的要求，中山市小榄人民医院必须对院内重要信息系统进行定级备案、测评分析、整改建设、验收测评。同时，为满足中山市卫健局发布的《中山市医疗卫生机构网络数据安全绩效考核指标明细表（100分）》的具体要求，医院需要建立一个完整的、动态的、可靠的网络与数据安全保障体系。

3.3 项目目标

通过采购人网信安全现状的全面排查与隐患整改，为采购人建立一个完整的、动态的、可靠的网络与数据安全保障体系，有效保障其系统业务的正常开展，保护敏感数据信息的安全，保证信息系统的安全防护能力达到《信息安全技术信息系统安全等级保护基本要求》中的相关技术和管理要求，满足《中山市医疗卫生机构网络数据安全绩效考核指标明细表（100分）》的绩效要求。

3.4 项目依据及标准

3.4.1政策/法律法规

- 《中华人民共和国网络安全法》
- 《中华人民共和国数据安全法》
- 《中华人民共和国计算机信息系统安全保护条例》（国务院147号令）
- 《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）

- 《中共中央办公厅国务院办公厅转发<国家信息化领导小组关于加强信息处理安全保障工作的意见>的通知》（中办发[2003]27 号）
- 《关于印发<关于信息安全等级保护工作的实施意见>的通知》（公通字[2004]66 号文）
- 《关于印发<信息安全等级保护管理办法>的通知》（公通字[2007]43 号文）
- 《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安[2007]861 号文）
- 《国家网络与信息安全协调小组关于开展信息安全风险评估工作的意见》（国信办[2006]5 号）

3.4.2技术标准

- 《信息安全技术 网络安全等级保护定级指南》（GB/T22240-2020）
- 《信息安全技术 网络安全等级保护基本要求》（GB/T22239-2019）
- 《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019）
- 《信息安全技术 网络安全等级保护实施指南》（GB/T25058-2019
- 《信息安全技术 网络安全等级保护测评过程指南》（GB/T28449-2018）
- 《计算机信息系统安全保护等级划分准则》（GB17859-1999）
- 《信息安全技术 信息系统通用安全技术要求》（GB/T20271-2006）
- 《信息安全技术 网络基础安全技术要求》（GB/T20270-2006）
- 《信息安全技术 操作系统安全技术要求》（GB/T20272-2006）
- 《信息安全技术 数据库管理系统安全技术要求》（GB/T20273-2006）
- 《信息安全技术 服务器技术要求》（GB/T21028-2007）

- 《信息安全技术 终端计算机系统安全等级技术要求》（GA/T671-2006）
- 《数据安全技术 数据分类分级规则》（GB/T 43697-2024）
- 《信息技术 数据加密保护要求》（GB/T 39786-2021）
- 《信息技术 数据备份与恢复》（GB/T 30285-2023）
- 《信息技术 数据处理 安全要求》（GB/T 35273-2022）
- 《信息技术 安全技术 远程办公 数据保护指南》（GB/T 35416-2021）

除上述规范以外，还遵循国家现行的相关标准和规范要求。

4 2025-2026年度网络与数据安全服务清单

序号	类别	工作内容	服务频次	交付成果
1	等级保护测评服务	1、等保测评：依据国家网络安全法最新的要求，对采购人的医院信息系统、PACS影像系统、LIS检验系统、门户系统四个系统按照等级三级的最新标准进行等级保护测评，进行差距分析、验收测评，并出具符合公安机关要求的测评报告。 2、测评支撑服务：供应商严格按照最新国家等级保护标准要求，提供等级保护测评现场支撑服务，包含但不限定测评前期沟通协调、新上线系统定级备案、专家评审、现场实施对接、整改加固支撑、验收及公安报备等工作。 3、公安报备：协助向公安监管部门提交测评报告，取得回执。	服务期内	《差距分析报告》 《等保测评报告》 《整改实施方案》 《管理制度集》 《整改实施过程清单》

2	资产梳理及安全巡检服务	1、需采用专业手段对采购人的全部互联网资产进行周期性探测与梳理，范围涵盖主机、网站、业务系统、服务器、网络设备以及小程序、微信公众号、APP 应用等。必须发现未知资产并跟踪变更趋势，对资产进行精确分类，并最终形成一套可动态维护的资产台账。台账需关联记录资产指纹、安全风险状态、所属资产组、责任部门及联系人等关键信息。 2、须指派经验丰富且经过专业培训的安全服务人员，定期赴现场开展工作。服务内容应包括：对信息系统进行工具扫描与专家人工检测；对防火墙、防病毒、数据备份等安全设备的策略有效性、配置安全性进行审计；对系统及设备日志进行深度分析（须包含不少于 180 天的日志巡检），以排查可疑安全事件。基于巡检结果，供应商需提供清晰的安全策略调整优化建议，并提交详尽的安全分析报告。 3、以攻击方视角，对医院敏感信息泄露情况的分析，探测范围覆盖互联网的各类公开应用，如搜索引擎、代码托管平台、网盘、暗网情报、Telegram 情报等。 4、对全院防病毒日志进行分析，处置高危病毒	年度 4 次	《资产台账表》 《敏感信息泄露分析报告》 《安全巡检报告》 《全网病毒巡检分析报告》

		源头，避免病毒在医院网络内持续传播扩散。		
3	漏洞扫描及整改服务	1、需提供持续性的自动化扫描与专家式管理相结合的综合解决方案。供应商须对采购人的全部网络资产进行定期、全面的漏洞扫描，范围必须包括但不限于：系统漏洞、Web 应用漏洞、数据库漏洞及弱口令检测。服务应遵循 “风险导向”原则，对扫描出的漏洞按其风险级别进行排序和归类，并为每一个漏洞提供详尽的修复方案或加固建议。 2、为确保服务不影响业务连续性，所有扫描操作必须在每日非业务高峰期开展。供应商不仅需提供扫描报告，更需协助采购方对漏洞进行全生命周期的跟踪与闭环管控，确保漏洞被发现、评估、修复、验证的完整流程得以落实，切实提升整体安全防护水平。	年度 4 次	《漏洞扫描报告》
4	暴露面监测服务	根据采购人需求，定期开展医院互联网资产暴露面的监测梳理工作，协助采购人收敛医院不必要对外开放的服务及端口，并开展互联网暴露面的风险识别工作。服务核心内容如下： 1、资产风险监测：主动监测并验证采购人互联网资产（如网站、系统等）是否存在可利用的安全漏洞、弱口令等高风险问题。	年度 4 次	《互联网暴露面资产梳理报告》 《互联网侧漏洞扫描报告》

		2、敏感信息泄露监测：持续在互联网空间进行巡查,监测是否存在因泄露而产生的采购人敏感信息，包括但不限于邮箱账号、代码片段、内部文档等。 3、专业的收敛建议：不仅限于发现风险，供应商必须对发现的所有暴露面风险提供具体、可操作的收敛和整改建议，并协助采购人评估 4、整改效果，最终形成监测、发现、预警、整改、验证的管理闭环。		
5	渗透测试服务	供应商在确保客户信息系统稳定运行的前提下，遵循非破坏性原则,模拟真实黑客的攻击思路与技术，对指定的信息系统（如 Web 应用、APP、业务系统等）进行授权范围内的入侵测试。服务应通过远程及本地等多种方式,深入检测并发现信息系统中的应用层漏洞、逻辑缺陷及深层安全风险。供应商需帮助客户准确理解其应用系统的真实安全状况，定位系统复杂架构中最脆弱环节，并针对发现的安全隐患提供具体、可操作、有效的解决方案与修复建议,最终提交详尽的渗透测试报告,切实为信息系统的安全加固提供决策依据，提升整体安全防护水平。	年度 2 次	《渗透测试报告》
6	安全加	供应商基于漏洞扫描、渗透测试、定期巡检及上	按需	《安全加固

	固服务	级检查等结果,对发现的安全隐患与薄弱环节提供系统性、闭环式的加固解决方案并为每一个漏洞提供人工编制的可操作修复方案或加固建议（非漏洞扫描工具自动导出），服务内容必须包括： 1、全面风险评估与方案设计：对发现的安全问题进行分析，制定详尽的加固方案。 2、系统性加固实施：依据方案，对操作系统、网络设备、数据库、中间件及应用系统等进行安全配置优化、漏洞修补、补丁更新和权限收紧等操作。 3、加固效果验证与复测：加固完成后，须进行严格的效果验证与复测,确保安全隐患已被彻底消除。 4、交付物要求：提供完整的加固过程报告，确保所有操作可审计、可追溯。 整个加固过程必须流程规范、操作可审计，并首要保证业务的连续性与系统的稳定性,严禁因加固操作引发新的系统故障。通过本服务，须有效修复安全漏洞，建立安全加固的闭环管理机制，显著提升信息系统的整体防护能力与安全基线。		服务报告》
7	应急响	1、应急响应:针对采购人出现的网络安全事件，	一年	《安全事件

	应及演练服务	提供安全应急响应支撑服务,协助对包括勒索病毒、网络攻击等安全事件，进行事件分析、攻击溯源、系统恢复等应急处置工作。 2、应急演练:按照应急演练的要求，结合采购人的需求，在服务期内提供两次安全应急演练服务，当发生安全事件时提供应急响应服务，且针对采购人实际情况提供应急预案材料。		应急响应处置报告》 《应急演练预案》 《应急演练计划方案》 《应急演练报告》 《应急过程材料等》
8	7*24 小时安全运营服务	1、以 7*24 小时持续在线守护为主线、以“资产、脆弱性、威胁、事件"四个核心安全风险要素为抓手，提供常态化 7*24 小时的远程监测分析服务，及时排查高危的漏洞和存在的安全隐患。 2、对内外网威胁封堵：精准研判外网威胁告警，封堵外网攻击 IP 地址及内网病毒传播、跳板攻击。	一年	《监测服务日报》 《监测服务月报》 《监测服务年报》 《实时预警通报》
9	安全培训服务	通过培训使技术员工了解信息安全基础知识和防护技能,使技术人员了解信息安全风险评估和信息安全等级保护的有关国家政策和技术发展趋势，以及常见的攻击手段及防范方法。培训内	年度一次	《安全培训课件》

		容参考《网络安全法讲解》、《等级保护讲解》、《网络安全意识》、《网络安全攻防基础》、《个人信息保护》、《数据安全》等课题。		
10	主机威胁检测防护与管理系统	采购人规格要求至少等于或高于以下功能要求：标准机架式设备，冗余电源，采用国产化平台和国产操作系统，内存≥32G，硬盘≥4T+32G mSATA；至少提供2个千兆电口、8个扩展槽、1个RJ45串口、2个USB口；提供资产管理、运维管理、病毒查杀、外设管理、非法外联监控、网络管理、终端响应、日志管理等功能；可扩展脆弱性检测、合规检查、安全审计、身份鉴别（含准入认证、Ukey认证）、入侵检测、主机微隔离、数据防泄漏等功能模块；最大可支持终端数量≥3000，本次配置不少于300个Windows服务器端授权、20个linux和信创服务器终端授权，3年硬件质保及病毒特征库升级服务许可。	一台	《实施方案》 《试运行报告》 《设备拓扑》 《培训记录》 《验收报告》 《使用手册》
备注：主要内容及要求详见附件《项目需求内容及要求》				

5 采购项目需求内容及要求

5.1.1 等级保护测评服务

在项目服务期内，依据国家网络安全法最新的要求，组织具等级测评资质的机构对采购人医院信息系统、PACS 影像系统、LIS 检验系统、门户系统四个系统按照最新标准进行等级保护测评，出具符合公安机关要求的测评报告。

5.1.1.1 系统定级备案服务要求

成交供应商需协助采购人完成采购人系统的定级备案工作,包括定级备案过程中的资产梳理、文档整理、材料编制及递交工作等事项，保证后续等级保护测评工作的顺利开展。

5.1.1.2 等级保护测评服务要求

成交供应商需委托具有资质的测评机构,根据《网络安全等级保护基本要求》等标准开展信息系统等级保护符合性测评,衡量采购人信息系统的安全保护管理措施和技术措施是否符合等级保护三级的相关要求,是否具备相应的安全保护能力。差距测评完成后，测评机构出具《差距问题清单》，罗列采购人系统存在的不符合问题项。

协助采购人根据《差距问题清单》完成相应整改后，测评机构针对采购人系统进行验收测试,验收测评完成后,测评机构出具《网络安全等级保护测评报告》,评估确认采购人系统是否满足等级保护三级相关要求。

5.1.1.3 管理制度修订要求

成交供应商需按照最新法律法规及《差距问题清单》要求对采购人的管理制度更新及修订，对应急预案进行修订优化，提供满足法律法规及相关规范要求的管理制度，包括安全管理制度、安全管理机构、安全管理人员、安全建设管理、

安全运维管理等，所提供的网络安全管理制度需满足等级保护三级相关要求。

5.1.1.4整改加固要求

成交供应商需提供技术支持协助采购人开展整改加固工作，对《差距问题清单》中存在的不符合问题项逐一进行整改加固，使其满足等保三级相关要求，整改范围包括主机、数据库、应用系统、网络设备、安全设备等。整改完成后，成交供应商需提交相应的整改证明材料提交给测评机构做审核。当医院官网系统存在高危漏洞无法整改时，为医院官网系统网站提供高危漏洞屏蔽服务，具体服务要求如下：

1）为医院提供1个互联网应用1年的漏洞屏蔽服务，通过将地址栏的URL动态加密，隐藏网站所有源代码、JS、API、漏洞、组件信息等敏感信息，能够防御各种针对协议头、交互内容的抓包重放攻击，屏蔽一切漏洞利用、病毒植入、Webshell执行、网页篡改等恶意攻击。

2）漏洞屏蔽服务能完全隐藏受保护网站的所有真实WEB漏洞（包含网站自有程序、所用第三方Web框架和Web中间件软件的漏洞），无论网站本身有多少WEB漏洞，都能使攻击者无法探测到网站任何可被利用的WEB漏洞。

3）▲漏洞屏蔽服务能完全隐藏受保护网站的完整源代码，并使网站所有页面对外呈现的源代码都一样，使攻击者无法分析网站源代码漏洞。**（需提供产品功能截图证明和具备CMA或CNAS标识的第三方检测报告）**

4）▲漏洞屏蔽服务能完全隐藏受保护网站的活动脚本、API，使攻击者完全无法探测到以上信息。**（需提供产品功能截图证明和具备CMA或CNAS标识的第三方检测报告）**

5）漏洞屏蔽服务能使访问者的终端上的浏览器无法获取受保护网站的原始

COOKIE，完全屏蔽窃取 COOKIE 发起的 CSRF 攻击。

6）▲漏洞屏蔽服务能使受保护的网站应用不对外展示目录结构和文件名，使攻击者无法对应用进行任何注入语句和 WEBSHELL 调用，URL 的加密结果应能是固定不变的或动态变化的，该功能应能通过管理界面的按钮控制开关。**（需提供产品功能截图证明和具备 CMA 或 CNAS 标识的第三方检测报告）**

5.1.1.5 安全保密要求

成交供应商应当提供与采购人的保密协议草拟本，并在中标后与采购人签署保密协议，对于安全服务所获取的相关信息进行严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据、信息进行任何侵害采购人信息系统的行为。

5.1.1.6 服务人员要求

现场测评开展时，成交供应商必须安排中级或以上的安全工程师（有 CISP 或 CISSP 证书）到现场协助采购人完成测评工作，以及后续的整改实施，根据系统遗留隐患和不符合项的整改工作量，成交供应商安排的安全工程师在医院现场开展安全整改工作。投标人应提供项目组成员姓名、学历、相关资质、在本项目中的职责及以前参与过的项目情况说明等。

成交供应商须保证队伍稳定，并由采购人项目负责人审核，审核通过后才能参与实施工作；经确认的技术团队，未经采购人项目负责人同意，不得更换技术人员；成交供应商必须遵守采购人内部各项规章制度和内部操作规程，履行保密义务，签署保密协议，未经批准不得以任何理由泄露任何保密信息和内部资料；技术团队应具备有利于开展实施工作的工具（包括软件和硬件）。

5.1.1.7 服务技术要求

成交供应商需提供详细的整体服务方案，包括技术方案和实施方案。技术方

案包括整体流程、技术方法和服务方案设计等；实施方案包括人员组织、时间安排、阶段性文档提交、验收标准、质量保证和风险规避措施等。

服务实施过程中所使用到的其他各种工具软件由成交供应商自行提供，漏洞扫描检测至少使用一款商用扫描系统。成交供应商须承诺所使用的所有工具和软件不具有所有权和知识产权纠纷，并保证工具和软件可用性和可靠性。由此产生的一切责任由成交供应商负完全责任。

5.1.1.8 服务成果物要求

本项服务的交付成果包含但不限于以下文档：

- 《中山市小榄人民医院 XX 系统差距分析报告》
- 《中山市小榄人民医院 XX 系统等级保护测评报告》
- 《中山市小榄人民医院 XX 系统整改实施方案》
- 《中山市小榄人民医院管理制度集》
- 《整改实施过程清单》

5.1.2 资产梳理及安全巡检服务

服务期内，成交供应商需定期对采购人院内资产进行梳理及系统、设备等做安全巡检，包括：

1）需采用专业手段对采购人的全部互联网资产进行周期性探测与梳理，范围涵盖主机、网站、业务系统、服务器、网络设备、物联网设备（如摄像头）以及小程序、微信公众号、APP 应用等。必须发现未知资产并跟踪变更趋势，对资产进行精确分类，并最终形成一套可动态维护的资产台账。台账需关联记录资产指纹、安全风险状态、所属资产组、责任部门及联系人等关键信息。通过部署一套资产探测工具，对相关系统的内、外网进行资产情报的搜集，梳理出资产的IP、端口信息、应用指纹信息等资产详情，提升资产管理能力。资产探测工具应具备以下能力：

1.可以发现暴露在互联网侧的域名资产及各种属性。包括：域名名称、主子域名关系、备案主体等。

2.可以发现暴露在互联网侧的 IP 资产及各种属性。包括：IP 地址、端口数量、关联域名、归属地、运营商、ASN 等。

3.可以支持全端口扫描探测及各种属性的识别。包括：端口、协议、服务、组件、版本等信息。

4.可以基于系统返回结果，深度识别站点详情。包括：网站截图、网站标题、访问地址、状态码、渲染标题、网站所属业务类型等信息。**（提供功能截图并加盖投标人公章）**

5.可以基于网站目录及相关信息，深度识别网站资产的指纹特征。包括：产品名称、组件、版本。指纹类型覆盖主流 web 应用、中间件、开发语言和框架、

内容应用（cms 等）、开源组件、第三方组件等。**（提供功能截图并加盖投标人公章）**

6.采用开放架构设计，支持灵活导入、卸载或删除第三方插件，用户可通过插件自由扩展 web 指纹识别、资产测绘、子域名接管检测、url 爬取、敏感信息泄露检测、页面监控等 30+功能模块，可根据业务需求组合个性化解决方案，实现资产识别与梳理工作效率倍增。**（提供功能截图并加盖投标人公章）**

2）▲以攻击方视角，对医院敏感信息泄露情况的分析，探测范围覆盖互联网的各类公开应用，如搜索引擎、代码托管平台、网盘、暗网情报、Telegram 情报等。其中搜索的暗网通道覆盖中文及英文，数量不少于 20 个。**（提供暗网渠道功能截图及以往发现敏感情报泄露的样本截图作为证明并加盖投标人公章）**

3）须指派经验丰富且经过专业培训的安全服务人员，定期赴现场开展工作。服务内容应包括：对信息系统进行工具扫描与专家人工检测；对防火墙、防病毒、数据备份等安全设备的策略有效性、配置安全性进行审计；对系统及设备日志进行深度分析（须包含不少于 180 天的日志巡检），以排查可疑安全事件。基于巡检结果，供应商需提供清晰的安全策略调整优化建议，并提交详尽的安全分析报告。

4）提供防病毒系统巡检、病毒查杀服务、防病毒管理软件的安装管理和协助安装服务。旨在保障防病毒软件的全面覆盖，持续提升防病毒系统的使用效果，实现防病毒安全预警，提升病毒安全事件应对能力。通过防病毒智能数据分析服务工具，结合人工研判，通过人机共治方式，对周期性病毒数据进行自动化分析，保障病毒巡检报告的准确性与可靠性。每次巡检服务导入服务期内的病毒日志，自动生成全网病毒分析报告。智能数据分析服务工具要求如下：

1.▲服务期间自备智能数据分析系统且具备合法使用权，导入全院终端防病毒日志数据后，可自动生成病毒分析报告；**（提供病毒分析报告证明及智能数据分析系统的软件著作权证书或购买发票或合作协议等能证明具有该系统的合法使用权）**

2.▲智能数据分析系统可对病毒传播及感染方向分析，可展示数据包括本机内横向扩散病毒数、通过移动存储感染病毒数、通过互联网感染病毒数、引导区病毒数、局域网横向传播病毒数，辅助安全管理人员直观判断病毒传播渠道风险；**（需提供产品功能截图证明和具备 CMA 或 CNAS 标识的第三方检测报告）**

3.智能数据分析系统可对医院前十病毒全网扩散情况进行分析，可展示数据包括病毒扩散情况排名前十的病毒名称、被感染计算机数量与具体被感染的计算机名称；

4.▲智能数据分析系统可进行勒索病毒感染情况、挖矿病毒感染情况分析，可展示数据包括病毒名、受感染文件路径、感染计算机名称、感染计算机数量，帮助安全管理人员梳理勒索病毒、挖矿病毒感染情况，有效闭环病毒处置工作；**（需提供产品功能截图证明和具备 CMA 或 CNAS 标识的第三方检测报告）**

5.▲智能数据分析系统支持自定义防病毒运维考核 KPI 指标包括病毒码更新率、客户端部署率、病毒感染率、病毒接触率。通过防病毒日志分析周期内运维考核 KPI 指标完成情况，直观呈现出单位当前防病毒运维效率。**（需提供产品功能截图证明和具备 CMA 或 CNAS 标识的第三方检测报告）**

5.1.2.1 服务成果物要求

- 《安全巡检报告》
- 《资产台账表》

- 《敏感信息泄露分析报告》
- 《全网病毒巡检分析报告》

5.1.3 漏洞扫描及整改服务

项目服务期内，成交供应商需对采购人全部网络资产进行定期、全面的漏洞扫描，范围必须包括但不限于：系统漏洞、Web 应用漏洞、数据库漏洞及弱口令检测。服务应遵循 “风险导向” 原则，对扫描出的漏洞按其风险级别进行排序和归类，并为每一个漏洞提供详尽的修复方案或加固建议；

为确保服务不影响业务连续性，所有扫描操作必须在每日非业务高峰期开展。供应商不仅需提供扫描报告，更需协助采购方对漏洞进行全生命周期的跟踪与闭环管控，确保漏洞被发现、评估、修复、验证的完整流程得以落实，切实提升整体安全防护水平。

服务频率为每季度一次。

5.1.3.1 服务工具要求

为了保障服务质量，成交供应商需提供相应的漏洞扫描工具，服务工具要求如下：

1）支持对目标设备进行漏洞扫描、基线扫描、弱口令扫描，支持主流的 IT 设备与操作系统、中间件、数据库等。

2）内置扫描任务报表、基线检查报表、资产报表、漏洞报表、对比报表和自定义报表模板；自定义的维度包括且不限于资产（主机存活性、主机指纹、端口、web 指纹等）、漏洞（修复方案、CVSS 评分、漏洞细节、漏洞描述、漏洞危害、影响范围等）进行筛选。**（提供功能截图并加盖投标人公章）**

3）支持对漏洞进行单个或批量复测，且支持查看复测结果。**（提供功能截**

图并加盖投标人公章）

4）支持按需自定义漏洞 POC 检测插件，包括漏洞名称、漏洞类型、漏洞危害、CVSS 信息、检测脚本等，用于日常突发漏洞应急。**（提供功能截图并加盖投标人公章）**

5）支持突发漏洞检机制，针对 1day/nday 漏洞，可通过 poc 快速生成漏洞扫描策略，对指定的客户资产进行漏洞风险检测。**（提供功能截图并加盖投标人公章）**

6）提供漏洞扫描工具的软件著作权证书或购买发票或合作协议等能证明具有该系统的合法使用权。

5.1.3.2 服务成果物要求

本项服务的交付成果包含但不限于以下文档：

- 《漏洞扫描报告》

5.1.4 暴露面监测服务

成交供应商应根据采购人需求，定期开展采购人互联网资产暴露面的梳理工作，协助采购人收敛医院不必要对外开放的服务及端口，并开展互联网暴露面的风险识别工作。

本次采购的暴露面监测服务要求成交供应商提供常态化、自动化的互联网暴露面监测与风险验证服务。服务须涵盖以下核心内容：

1、资产风险监测：主动监测并验证采购人互联网资产（如网站、系统等）是否存在可利用的安全漏洞、弱口令等高风险问题。

2、敏感信息泄露监测：持续在互联网空间进行巡查，监测是否存在因泄露而产生的采购人敏感信息，包括但不限于邮箱账号、代码片段、内部文档等。

3、专业的收敛建议：不仅限于发现风险，供应商必须对发现的所有暴露面风险提供具体、可操作的收敛和整改建议，并协助采购人评估 4、整改效果，最终形成监测、发现、预警、整改、验证的管理闭环。

该服务旨在实现对互联网暴露风险的持续发现与主动管理，有效收敛攻击面，预防因信息泄露而导致的安全事件。服务频率为每季度一次。

5.1.4.1 服务成果物要求

- 《互联网暴露面资产梳理报告》
- 《互联网侧漏洞扫描报告》

5.1.5 渗透测评服务

项目服务期内，成交供应商需对采购人对指定的信息系统（如 Web 应用、APP、业务系统等）进行授权范围内的渗透测试，服务应通过远程及本地等多种方式，深入检测并发现信息系统中的应用层漏洞、逻辑缺陷及深层安全风险。供应商需

帮助客户准确理解其应用系统的真实安全状况，定位系统复杂架构中最脆弱环节，并针对发现的安全隐患提供具体、可操作、有效的解决方案与修复建议，最终提交详尽的渗透测试报告，切实为信息系统的安全加固提供决策依据，提升整体安全防护水平。服务频率为一年二次。

5.1.5.1 渗透测试要求

模拟黑客攻击手段对目标系统进行探测攻击，从而发现黑客入侵信息系统的潜在可能途径。

渗透测试方法包括：信息收集、端口扫描、远程溢出、口令猜测、本地溢出、客户端攻击、中间人攻击、web 脚本渗透、B/S 或 C/S 应用程序测试、社会工程等。

测试范围必须包括以下内容：

- Web 安全：Web 安全测试范围包括 SQL 注入、XSS、XXE、CSRF、RFI、上传漏洞、信息泄露、远程命令执行、反序列化漏洞等。
- 业务逻辑安全：业务逻辑安全测试范围包括用户或口令枚举、弱口令测试、平行/垂直越权、未授权访问、验证缺陷、业务逻辑限制缺陷等。
- 中间件安全：中间件安全测试范围包括配置缺陷、中间件弱口令、反序列化漏洞、代码执行漏洞等。
- 服务器安全：服务器安全测试范围包括域传送漏洞、弱口令漏洞、未授权访问漏洞、脚本密码检查、本地提权漏洞、应用防护软硬件缺陷等。

5.1.5.2 服务成果物要求

- 《XX 系统渗透测试报告》

5.1.6 安全加固服务

5.1.6.1 安全加固服务要求

服务期内，成交供应商针对漏洞扫描、渗透测试、定期巡检及上级检查等结果，对发现的安全隐患与薄弱环节提供系统性、闭环式的加固解决方案并为每一个漏洞提供人工编制的可操作修复方案或加固建议(非漏洞扫描工具自动导出)，服务内容必须包括：

1）全面风险评估与方案设计：对发现的安全问题进行分析，制定详尽的加固方案。

2）系统性加固实施：依据方案，对操作系统、网络设备、数据库、中间件及应用系统等进行安全配置优化、漏洞修补、补丁更新和权限收紧等操作。

3）加固效果验证与复测：加固完成后，须进行严格的效果验证与复测，确保安全隐患已被彻底消除。

4）整个加固过程必须流程规范、操作可审计，并首要保证业务的连续性与系统的稳定性，严禁因加固操作引发新的系统故障。通过本服务，须有效修复安全漏洞，建立安全加固的闭环管理机制，显著提升信息系统的整体防护能力与安全基线。

5.1.6.2 服务成果物要求

- 《安全加固报告》

5.1.7 应急响应及演练服务

服务期内，成交供应商需针对采购人出现的网络安全事件，提供安全应急响应支撑服务，协助对包括勒索病毒、网络攻击等安全事件，进行事件分析、攻击溯源、系统恢复等应急处置工作；此外，成交供应商需提供两次安全应急演练服

务，检验采购人应急响应流程的有效性和实用性。

5.1.7.1 应急响应要求

在项目服务期内，服务提供商提供信息安全事件应急响应救援服务。应急响应内容主要包括：病毒暴发、黑客攻击、网络大范围瘫痪、应用系统瘫痪及其他严重影响业务运行的事件。响应要求如下：

1. 对于病毒暴发和黑客攻击现象发生时、在十分钟内响应，提供远程诊断技术支持，远程无法解决的，2小时内赶到现场，解决故障恢复正常或提出可行的临时解决措施。

2. 出现网络大范围瘫痪、应用系统瘫痪及其他严重影响业务运行的事件时、应立即派具有相关应急经验的工程师2小时内上门协助处理，若指定时间内未能解决故障，应提供事件处理的临时解决方案。

3. 在应急响应结束3天内，需提供本次应急解决处理方案和安全防护建议，针对事件中的问题协助采购人进行安全加固。

5.1.7.2 应急演练要求

信息安全应急管理体系是指导及提升应急响应工作的重要支撑。由于信息安全的动态变化，成交供应商需根据安全态势的发展，协助采购人优化与完善应急响应体系。

成交供应商需协助采购人完成现有信息安全应急管理体系文件的年度修编，确保采购人网络安全应急总预案满足安全监控部门以及行业主管机构在信息安全及安全预案方面的整体性要求，同时确保采购人网络安全预案能够应对最新的安全攻击技术、最新出现的安全事件，具有较强的实时性。

成交供应商需协助采购人开展应急演练工作。通过应急演练，完善应急流程

与操作，提升采购人对重大安全事件的应急处置能力。

5.1.7.3 服务成果物要求

- 《中山市小榄人民医院安全事件应急响应处置报告》
- 《中山市小榄人民医院应急演练预案》
- 《中山市小榄人民医院应急演练计划方案》
- 《中山市小榄人民医院应急演练报告》
- 《中山市小榄人民医院应急过程材料等》

5.1.8 7*24 小时安全运营服务

以 7*24 小时持续在线守护为主线、以“资产、脆弱性、威胁、事件"四个核心安全风险要素为抓手，提供常态化 7*24 小时的远程监测分析服务的及时高危的漏洞和存在的安全隐患。同时对内外网威胁封堵：精准研判外网威胁告警，封堵外网攻击 IP 地址及内网病毒传播、跳板攻击。

成交供应商需提供 7*24 小时远程威胁检测与响应运营服务，实时监测和发现采购人网络中的安全威胁，以自动化+人工介入的形式分析和处置安全事件，开展实战化与常态化安全运营。

本项服务提供的具体服务项，包括但不限于以下内容：

1.项目须配备不少于 1 名专职服务经理及 3 名安全运营专家,不少于 200Mbps 流量提供全年 7*24 小时安全监测分析与事件响应服务。

2.托管服务内容应全面覆盖资产清点、脆弱性管理、威胁监测、事件应急响应、预警通告、互联网暴露面梳理服务。

3. 提供 SAAS 化远程托管安全运营与本地化远程托管安全运营两种服务模式的能力。

4.投标人承诺在服务期内，可根据采购人需求进行两种运营模式的平滑切换。**（提供加盖公章的承诺函）**

5.在“本地化远程托管安全运营”模式下，安全告警日志于内网平台存储，不出互联网；投标人运营人员通过采购人指定的VPN及堡垒机，并基于零信任构建的安全通道进行远程运营操作。

6.投标人运营平台在两种安全运营服务模式下支持对接不同安全厂商设备的告警日志,能基于多源异构日志进行有效的组合与关联分析,并通过威胁情报、模型分析等技术快速定位并研判安全威胁。

7.依据《网络安全事件分类分级指南》，对于重大及以上安全事件，须承诺15分钟内完成响应，1小时内提供初步处置方案，事件处置闭环率达到100%。**（提供SLA承诺函并加盖投标人公章）**

8. 提供独立的服务交付门户，采购人可实时查看日志总量、告警量、风险资产、脆弱性数量、待办工单数量，告警处置状态、攻击链阶段分布以及日志与告警等趋势性等数据。**（提供功能截图并加盖投标人公章）**

9.托管安全运营服务应当支持与采购人现有流量采集探针、EDR的对接，支持实时接收安全设备信息日志数据、联动抑制威胁、联动封锁处置工作。

10. 投标人提供的远程安全托管运营必须是一套功能完备的一体化解决方案，应自带集成其核心服务组件，包括但不限于：网络流量采集与分析探针。组件间需协同工作，共同构成一套独立的、标准化的安全运营体系。同时，平台必须具备良好的兼容性，支持接收并解析通过Syslog、API等标准方式的第三方日志。

5.1.8.1 服务成果物要求

- 《监测服务日报》

- 《监测服务月报》
- 《监测服务年报》
- 《实时预警通报》

5.1.9 安全培训服务服务

通过培训使技术员工了解信息安全基础知识和防护技能,使技术人员了解信息安全风险评估和信息安全等级保护的有关国家政策和技术发展趋势,以及常见的攻击手段及防范方法。培训内容参考《网络安全法讲解》、《等级保护讲解》、《网络安全意识》、《网络安全攻防基础》、《个人信息保护》、《数据安全》等课题。安全培训讲师需具备丰富的教培经验,从事网络安全相关工作5年以上,提供一年一次的现场培训。

5.1.9.1 服务成果物要求

- 《安全培训课件》

5.2 安全设备类

5.2.1 主机威胁检测防护与管理系统

实现医院重要主机及终端的深度威胁检测与防御，具体要求如下：

序号	指标项	技术指标
1	基本要求	★标准机架式设备，冗余电源，采用国产化平台和国产操作系统，内存≥32G，硬盘≥4T+32G mSATA；至少提供2个千兆电口、2个USB口；本次配置不少于300个Windows服务器端授权、20个linux和信创服务器终端授权，3年硬件质保及病毒特征库升级服务许可。**（提供承诺函并加盖章投标人公章）**
2		▲提供资产管理、运维管理、病毒查杀、外设管理、非法外联监控、网络管理、终端响应、日志管理等功能；可扩展脆弱性检测、合规检查、安全审计、身份鉴别（含准入认证、Ukey认证）、入侵检测、主机微隔离、数据防泄漏等功能模块；最大可支持终端数量≥3000(提供承诺函并加盖章投标人公章)
3	部署环境	服务端支持在欧拉系统、银河麒麟操作系统中部署，客户端支持在常见Windows、Linux系统以及主流的国产化系统中部署；支持同一个服务端对安装在不同类型操作系统的客户端进行统一管理；
4	安全态势	▲具备多维度的态势大屏，包括资产态势大屏、运维态势大屏、威胁态势大屏、数据安全态势大屏。展示内容至少包括威胁告警统计、攻击阶段统计、威胁等级统计、漏洞信Top5、终端威胁告警Top5、敏感信息Top5、敏感终端Top5、最新告警事件、威胁态势评分等信息，提供功能截图及具备多维度网络态势感知的能力，提供第三方

		机构（中国信息安全测评中心、中国信息安全认证中心、公安部检验/检测中心、中国网络安全审查技术与认证中心、国家知识产权局、商用密码检测认证中心和国家版权局中的任一单位）出具的多维度网络态势感知方法的技术检验报告或认证材料；
5	资产管理	支持全网终端资产统一管理和资产画像，基于 DeepSeek 的智能分析实现单个终端与全网终端的风险解读，直观展示终端资产的综合健康状态，并为用户提供合理的优化策略与处置建议；**（提供加盖制造商公章的功能截图证明）**
6		支持全网终端资产发现和统一管理，可对终端资产进行关闭、重启、锁屏、结束进程、断开网络、远程协助等操作；可通过 ARP、PING、NMAP 等多种方式对非法接入的终端资产进行探测，发现未安装客户端的终端资产；**（提供加盖制造商公章的功能截图证明）**
7		▲支持全网终端资产一键体检，可一键完成漏洞风险、合规检查、弱密码检查、病毒查杀、Webshell 检测、内存马检测、反弹 shell 等体检项目。同时，产品应具备风险评估中心，能够根据终端威胁风险情况进行失陷终端分析、勒索风险评估、全网威胁统计、泄露防护统计等；**（提供功能截图及第三方技术检验报告或认证材料）**
8		支持全网终端资产清点，至少包括数据库、中间件、环境变量、内核模块、共享目录、Web 应用、Web 站点、安装包、证书等资产信息；
9	风险管理	支持终端风险管理，至少包括漏洞检查、弱密码检查、暴露面管理能力；检测的漏洞类型至少包括系统漏洞、应用漏洞、中间件漏洞、

		数据库漏洞等；**（提供第三方技术检验报告或认证材料）**
10		支持弱密码检查，包含系统弱密码和应用弱密码，支持弱密码分类，类别应至少包括密码长度小于 8、字符种类小于 3、空密码、账号密码相同、可疑高权限等；
11	基线合规	具备全网终端安全基线检查，能够对资产进行即时和定时基线检查，能够直观展示未通过项、检查项通过率、未通过主机数、主机通过率等检测信息；
12	病毒查杀	支持病毒查杀，可自行选择查杀效率、查杀位置、查杀引擎、处置方式等，直观展示已处理和未处理的病毒数量，展示内容应包括已处理/未处理的全病毒数量、已处理/未处理的勒索病毒数量、已处理/未处理的挖矿病毒数量、已处理/未处理的蠕虫病毒数量等；
13		病毒检出率≥99%，病毒检测误报率＜1%；**（提供第三方技术检验报告或认证材料）**
14		支持勒索病毒专项防护，包括勒索诱捕、文件保险箱、数据备份等，实时检测勒索病毒，防止勒索病毒入侵；**（提供加盖制造商公章的功能截图证明）**
15	威胁检测	支持威胁行为检测，包括端口扫描、暴力破解、反弹 shell（linux）、系统命令篡改、异常行为等，提供第三方技术检验报告或认证材料；
16		支持敏感行为检测，包括文件篡改、敏感文件访问、系统日志文件删除、自启动项添加、敏感命令执行等，全面的判断终端安全性；
17		支持行为基线检测，对进程行为、网络连接行为、端口监听行为、DNS 访问行为、登录行为进行建模，形成行为基线进行异常判断；

18	微隔离	支持主机微隔离，能可视化的展示全网资产的网络访问关系，形成安全访问控制，缩小网络暴露面；**（提供第三方技术检验报告或认证材料）**
19	数据安全	支持基于关键字、正则表达式、文件指纹等方式检测终端敏感文件，并形成本地密级标识；
20		支持监测并阻止敏感文件的外发行为，包括文件拷贝、打印刻录、邮件、HTTP、FTP 等，防止敏感信息通过 U 盘、网络等途径泄露敏感信息；
21		▲支持屏幕水印，包括文字、图片、点阵水印，防止通过录屏、截屏等方式进行数据窃取；**（提供第三方技术检验报告或认证材料）**
22	安全加固	支持对 Windows 系统的账户策略、密码策略、本地策略、环境策略、注册表等项目进行安全加固，并具备抗拒绝攻击专项防护能力，保证 Windows 系统的安全；
23		具备对移动存储介质的认证和加密功能，可实现对 U 盘的授权认证管理、专用目录加密认证管理以及全盘加密认证管理；具备外设管控能力，支持对 U 盘、光驱、软盘、手机平板、打印机、摄像头等外设进行使用控制；
24		具备剧本式的全网自动响应能力，可根据告警事件类型编排响应动作、响应时间等，支持与防火墙设备深度联动实现应用准入控制，仅允许安装客户端且合规的终端访问受保护资源，对未装客户端用户提供浏览器友好引导自助安装，并对不合规终端实施访问阻断；**（提供加盖制造商公章的功能截图证明）**

25	分析溯源	内置多种场景分析能力，包括勒索软件、WEB 服务器异常、失陷主机、挖矿软件、横向渗透等多种场景，应对复杂的安全威胁场景；**（提供第三方技术检验报告或认证材料）**
26		支持终端安全审计，包括软/硬件变更审计、资源使用审计、账号变更审计、文件操审计作、注册表行为审计、命令行审计、打印行为审计、刻录行为审计、FTP 访问行为审计、网站访问行为审计等，便于审计人员溯源违规行为；**（提供功能截图及第三方技术检验报告或认证材料）**
27	告警管理	▲支持自定义告警规则，可通过日志事件类型的发生次数开启邮箱告警。当日志事件发生数超过设定阈值，可触发邮箱告警机制，提供第三方机构（中国信息安全测评中心、中国信息安全认证中心、公安部检验/检测中心、中国网络安全审查技术与认证中心、国家知识产权局、商用密码检测认证中心和国家版权局中的任一单位）出具的基于消息队列的报警信号处理方法的技术检验报告或认证材料；
28	运维管理	▲产品自带运维平台，支持监控应用系统的 url 访问是否正常；支持监控应用系统的开放端口是否正常；支持监控应用系统在操作系统资源使用状态；**（提供加盖制造商公章的功能截图证明）**
29		产品自带运维平台，可以通过配置发送邮件通知给指定的收件人，通过集成短信网关来发送短信通知给指定的手机号码，通过 HTTP 请求发送通知给指定的 URL 地址；**（提供加盖制造商公章的功能截图证明）**

30		▲产品自带运维平台，支持提供监控应用系统、中间件、数据库、操作系统、服务器、网络设备等资源授权不低于300个。**（提供承诺函并加盖章投标人公章）**

5.2.1.1 成果物要求

- 《主机威胁检测防护与管理系统实施方案》
- 《主机威胁检测防护与管理系统试运行报告》
- 《主机威胁检测防护与管理系统设备拓扑》
- 《主机威胁检测防护与管理系统培训记录》
- 《主机威胁检测防护与管理系统验收报告》
- 《主机威胁检测防护与管理系统使用手册》

6 项目服务要求

6.1 技术服务团队要求

1) 成交供应商应为本项目提供专业服务团队，该团队包括项目经理和至少四名技术人员。团队所有人员均具有不少于三年网络或信息安全从事经验（**成交供应商应提供项目组成员姓名、学历、相关资质、在本项目中的职责及以前参与过的项目情况说明等。）**，同时，技术人员对采购人现有的安全设备型号具有一定的维护和实施经验，如：熟悉防火墙、堡垒机参数配置、性能优化调整等。

2) 成交供应商须保证队伍稳定，并由采购人审核，审核通过后才能参与实施工作；经确认的技术团队，未经采购人同意，不得更换技术人员；成交供应商必须遵守采购人内部各项规章制度和内部操作规程，履行保密义务，签署保密协议，未经批准不得以任何理由泄露任何保密信息和内部资料；技术团队应具备有利于开展实施工作的工具（包括软件和硬件）。

6.2 安全服务技术要求

成交供应商需提供详细的整体服务方案，包括技术方案和实施方案。技术方案包括整体流程、技术方法和服务方案设计等；实施方案包括人员组织、时间安排、阶段性文档提交、验收标准、质量保证和风险规避措施等。

服务实施过程中所使用到的其他各种工具软件由成交供应商推荐，系统安全维护的定期漏洞扫描服务至少使用一款商用扫描系统。成交供应商须承诺所使用的所有工具和软件不具有所有权和知识产权纠纷，并保证工具和软件可用性和可靠性。由此产生的一切责任由成交供应商负完全责任。

6.3 文档管理要求

成交供应商须按照项目阶段，提供符合采购人文件管理及版本控制要求的项

目文档，要求如下：

（1） 记录专门的档案；

（2） 详细记录系统环境、运行状况评估、故障问题报告等信息；

（3） 现场档案与资料的管理，后方档案与资料的管理；

（4） 档案报告交流。

6.4 项目管理要求

成交供应商须根据实际维护服务项目的状况，定期组织汇报与技术交流、紧急情况工作会议，要求如下：

双方技术人员定期（1 次/月）开会，就过去遇到问题情况作总结汇报和交流，确定下一步工作方案，以提高和改善服务质量，并根据需求对服务方案不断进行完善；发现潜在和细小问题，防患于未然；最新产品介绍与业界动态信息；其它用户的经验介绍及分享；举办年度研讨会，对一年的工作作出总结，并为下一年度的工作作出规划。

对于任何紧急情况，如有必要，应协调相关部门负责人、技术人员，无论何时，根据需要召开紧急会议，重点处理紧急问题，以保证重大故障得到及时解决。

6.5 项目服务周期

项目服务周期，自合同签订之日起一年。自签订合同之日起30天内完成主机威胁检测防护与管理系统的安装调试服务。其他服务内容按第二章第2点《2025-2026年度网络与数据安全服务清单》的要求在自签订合同之日起一年内完成。

6.6 项目售后要求

1) 成交供应商应提供切实可行的售后服务方案

2) ★成交供应商应提供 7×24 小时运维响应服务，在 10 分钟内响应，30 分钟内派出有能力的技术人员赴现场处理，同时提供远程和现场两类方式的安全支撑服务，**（需要提供投标人盖章的承诺函）**。

3) ▲成交供应商应承诺，如中标后，在服务期内，成交供应商应安排至少一名同时具备以下资质和经验的项目经理：持有软考类的信息系统项目管理师、软考类的网络工程师、中国信息安全测评中心认证的注册信息安全管理人员（CISO）认证；**投标时提供该项目经理资质证书及其在投标单位近半年任意一个月的社保缴纳记录**。

4) ▲为保障渗透测试服务效果，成交供应商渗透测试技术服务人员需具备国内原创漏洞报送证书。投标时提供渗透测试人员资质证书及其在投标单位近半年任意一个月的社保缴纳记录。

6.7 项目验收要求

1、按照国家相关标准及规范进行验收。相关服务无国家标准时按地方相关标准或行业规范进行验收。

2、在符合国家相关标准及规范的前提下，服务期满结束后，由成交供应商提起验收申请，15 个工作日内，经招标人同意并签字盖章确认后完成验收。

7 付款方式

（一）货物款项，付款方式如下：

合同签订后 15 个工作日内，成交供应商向采购人开具货物（主机威胁检测

防护与管理系统）款项金额30%的普通发票，采购人在收到发票后15个工作日内向成交供应商支付对应款项。

货物（主机威胁检测防护与管理系统）完成验收后，成交供应商向采购人开具货物款项金额70%的普通发票，采购人在收到发票及货物验收报告后15个工作日内向成交供应商支付对应款项。

（二）服务款项，付款方式如下：

合同签订后，成交供应商向甲方开具服务款项金额的30%的普通发票，采购人在收到发票后15个工作日内向成交供应商支付对应款项。

成交供应商完成HIS、PACS、LIS、医院官网四个系统等级保护测评获得备案证明后，成交供应商向采购人开具等级保护测评相应款项的普通发票及备案证明，采购人在收到发票后15个工作日内向成交供应商支付对应款项。

在所有服务项目均完成并通过最终验收后，成交供应商向采购人开具合同金额剩余款项的普通发票，采购人在收到发票后15个工作日内向成交供应商支付剩余款项。