数字江门网络建设有限公司信息系统安全运维服务（2025-2026）项目采购公告

本项目已由数字江门网络建设有限公司批准，资金自筹，项目资金已落实。数字江门网络建设有限公司对该项目进行采购。现公开进行采购，采购项目相关要求如下：

1、项目背景、概况

1.1 项目背景：随着当前信息系统规模的扩大和应用的复杂化，相关的信息安全风险也随之而来，比如病毒、蠕虫、垃圾邮件、间谍软件、流氓软件、数据截获、嗅探、监听、肆意泛滥，内部机密数据泄漏、办公系统受到影响等等，因此为了保证业务正常运营，不因各种安全威胁的破坏而中断，信息安全建设不可或缺，信息安全建设必然应该和当前的信息化建设进行统一全局考虑，应该在相关的重要信息化建设中进行安全前置的考虑和规划，避免安全防护措施的遗漏，安全防护的滞后造成的重大安全事件的发生。

1.2 项目主要内容：

序号	服务类别	服务内容	数量	备注
1	安全评估	采用专业的扫描工具对信息系统、开放端口、数据库进行扫描，通过扫描发现系统在配置和管理上潜在的安全问题和可能面临的安全威胁。并提供《安全评估报告》，安全评估报告内容主要包括以下几个方面： 1.系统补丁修补； 2.弱口令扫描； 3.系统账号权限； 4.文件系统权限； 5.网络端口及系统服务运作； 6.系统安全配置文件； 7.文件或文件夹共享； 8.提出整改建议。	2次/年	输出《安全评估服务报告》
2	安全加固	对甲方指定机房网络中的主机系统、网络设备、安全设备，以及相关的数据库系统实施安全加固，包括： 1.服务器加固：主要包括对Windows服务器和Linux服务器的评估加固，其中还包括对服务器操作系统层面的评估和数据库层面的评估加固； 2.应用系统加固：主要包括协助开发商完成整改后的漏洞验证； 3.网络设备加固：主要包括防火墙，IPS，WAF，交换机的评估	2次/年	输出《安全加固服务报告》

		加固； 4.安全加固服务主要以人工服务的方式实现；		
3	安全渗透测试服务	安排专业工程师进行重点网络及关键系统安全渗透测试，对用户的信息系统进行模拟攻击或入侵，识别测试系统的未知漏洞及安全隐患，及时防范及安全加固，并提供测试报告及整改建议方案。	1次/年	输出《安全渗透测试报告》
4	安全应急演练服务	提供一次关键网络安全应急演练服务：模拟关键网络发生故障，通过分析故障原因提供对应的解决方案，从而恢复关键网络通信；通过提前制定应急演练预案，并协助单位开展预案演练，提高应对网络与信息安全事件的处置能力，预防和减少网络与信息安全事件造成的危害和损失。	1次/年	输出《网络应急演练预案》、《网络应急演练服务报告》
5	PC终端巡检规范	对甲方指定的PC终端系统优化、病毒查杀、系统修复、重要系统补丁更新。	1次/年	输出《PC终端巡检服务报告》
6	机房定期巡检	定期对机房的设备提供安全巡检服务，主要包括： 1. 系统进程检测：采用相关工具进行检测，并记录所有当前检测到的正在运行进程，并生成报告； 2.端口连接情况检测：打开专用工具，列出当前所有进程；对当前窗口列出已经连接或是正在监听的所有端口进行确认，并追查文件位置、文件属性；如果有不能确认的连接，立即进行关闭处置；生成进程运行报告； 3.系统账户检测：采用相关账户检测工具检查系统的账户，检查所有账户，确认所有账户为合法账户，出现不明账户必须记录并删除。 4.协助用户对机房机柜、设备、网线端对端的整理及标签加贴标识。	2次/年	输出《机房定期巡检服务报告》
7	机房设备上架及标签整理	1. 协助用户上架机房设备； 2. 设备标签整理。	按实际工作情况开展	
8	防火墙运维服务	1.防火墙策略优化：根据业务系统的具体需求，提交防火墙优化方案，并得到用户确认和授权后，优化调整策略，包括对规则的梳理、合并、删除和新增，以确保策略的有效性和可读性，提升防火墙的拦截能力； 2.性能监控与调优：可以实时监测防火墙的运行状态、警指示灯是否告警、流量情况、连接数等关键指标，发现性能瓶颈并进行调优。根据用户需求进行维护和配置，提供每年不少于4次现场巡检服务，日常运维若发现异常事件故障记录，立即向用户提交异常报告情况及解决方案； 3.定期更新和维护：防火墙软件和硬件需要定期更新和维护，以确保其功能和性能的稳定性和可靠性；	2次/年	输出解决方案和巡检服务报告

		4.备份和恢复：为了应对可能出现的意外情况，需要对防火墙的配置和数据进行备份和恢复。		
9	日志管理及溯源支撑	攻防演练期间，系统遭受攻击后，协助用户对服务器和防火墙的日志管理，协助用户开展溯源工作，了解攻击方式、攻击路径以及攻击者身份等关键信息，并协助应用系统支撑单位完成系统加固和完善溯源整改报告。	2 次/年	输出《溯源整改报告》
10	重大活动期间和攻防演练网络安全保障	重大活动、会议、工作检查、护网行动等特殊时期按采购方要求执行 7*24 小时特别巡视、维护和保障。在上级部门或相关主管部门通知开展攻防演练期间，须按要求派遣技术人员前往市政务数据局信息中心指定地点进行现场驻场，实施重点安全保障。	按实际工作情况开展	
11	安全培训服务	提供 1 次信息安全现场培训服务。	1 次/年	培训文档
12	完善规章制度和各类台账建立	协助修订和完善相关网络安全方面的管理制度，协助终端、设备接入网络系统日常运维、介质清单等台账的建立。	1 项	输出制度、台账模板
13	应急响应	1.当出现网络安全事件突发情况，服务单位派出不少于 4 名本地技术人员进行应急响应。 2.在网络安全部门向用户发出网络安全警示等相关信息后，要及时协助排查和处置。	1 项	网络或系统出现安全事故，提供响应。

1.3 服务期限为自合同签订之日起一年（12 个月）。

1.4 本项目采购预算最高限价为人民币 4.26 万元整（含税）。

2、供应商资格要求：

2.1 供应商应当具备《中华人民共和国政府采购法》第二十二条规定的条件。

2.2 供应商应当是具有合法经营资格的法人或者其他组织，具有良好的信誉。

2.3 供应商须具备本项目履约能力的在中华人民共和国境内工商局登记注册、根据中华人民共和国有关法律合法成立并存续的独立于采购人和采购机构的独立法人或其他组织，提供合法有效的营业执照，并提供商事法律关系主体信息最新查询结果（显示经营范围、注册资本等信息）的截屏打印件（加盖公章）。

2.4 供应商未被列入“信用中国”网站(www.creditchina.gov.cn)“记录失信被执行人或重大税收违法案件当事人名单或政府采购严重违法失信行为”记录名单；不处于中国政府采购网(www.ccgp.gov. cn)“政府采购严重违法失信行为信息记录”中的禁止参加政府采购活动期间。（提供截屏打印件并加盖公章）。

2.5 单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的政府采购活动。

2.6 本项目不接受联合体参与应答。

3、采购文件获取

3.1 请供应商于 2025 年 12 月 29 日 8 时 30 分至 2025 年 12 月 31 日 17 时 30 分（北京时间，下同），通过江门市采购行业协会（请前往“江门市采购行业协会”，网址：http://www.jmcgxh.org.cn），提取《采购需求文件》中的《采购需求文件领取登记表》后需打印并加盖公章，将扫描件发送至数字江门网络建设有限公司邮箱（shuzijiangmen2018@szjmltd.com），并致电通知确认，联系人：岑小姐；联系方式：0750-3081185。完成上述要求报名，本项目的报名方可成功。

3.2 参与报价的供应商需在递交现场将《采购需求文件领取登记表》盖章原件交予数字江门网络建设有限公司采购实施部门。

4、资料提交方式

本次比选会议将于递交响应文件截止的同一时间在进行，法定代表人/负责人或其委托的代理人应随身携带身份证及法人代表授权委托书准时参加。

4.1 响应文件递交时间（截止时间）：2025 年 12 月 31 日 17 时 30 分（北京时间，下同），在此时间后送达的响应文件将不再接受。

4.2 响应文件递交地址：江门市蓬江区建设路 42 号二至五层（自编），联系人：岑小姐/0750-3081185(工作时间:工作日 8:30-12:00，14:30-17:30)。

4.3 响应文件，需用信封密封，在密封袋上标明项目编号、供应项目名称、供应人名称，密封袋两头封口处均需贴封条。

4.4 响应文件可以现场递交，邮寄、快递方式需要在响应文件截止时间前，确保采购方签收。

5、联系方式

采 购 人：数字江门网络建设有限公司

地　　址：江门市蓬江区建设路 42 号二至五层（自编）

联系人：岑小姐

联系人电话：0750-3081185(工作时间:工作日 8:30-12:00，14:30-17:30)

采购人：数字江门网络建设有限公司

2025 年 12 月 29 日