遵义市播州区人民医院
People's Hospital Of Zunyi City Bo Zhou District

遵义市播州区人民医院
关于等保测评及网络安全运维服务采购项目的内部竞争性磋商公告

一、项目基本情况

项目编号：BYC-2024-ZX010

项目名称：等保测评及网络安全运维服务采购项目

采购方式：内部竞争性磋商

采购需求：

项目编号	产品名称	数量	单位
BYC-2024-ZX010	等保测评及网络安全运维服务	1	项

技术参数或服务要求

序号	产品名称	技术参数或服务要求	数量	单位
1	等保测评	等保三级系统测评服务，输出整改报告、测评报告、公安备案证书。	3	套
2	渗透测试服务	一、服务概述 在获得授权的情况下对指定的业务系统进行深层次的漏洞挖掘和利用，模拟黑客展开渗透测试攻击，获取到该业务系统的服务器权限以及最具价值的信息和资产。 二、服务内容 1.前期交互阶段 与用户进行沟通、确定渗透测试的时间、范围、深度、测试方式（黑盒 OR 白盒、现场 OR 远程）等问题，并拿到用户签署的渗透测试授权函； 2.情报搜集阶段 服务团队在拿到用户授权后开始情报搜集工作，搜集阶段是对目标用户的系统进行一系列踩点工作，包括：基础资产收集、互联网信息泄露搜集、指纹识别、业务系统功能收集、接口信息收集等； 3.威胁建模阶段 在搜集到充分的情报信息之后，服务工程师对获取的信息进行威胁建模与攻击规划；从大量的信息情报中理清思路，确定出最可行的攻击通道； 4.漏洞分析阶段 针对威胁建模阶段总结的测试方法进行一一验证，通过测试总结出可行的测试方法，排除不可行的测试方法； 5.渗透攻击阶段 对用户的业务系统进行攻击性测试；	1	套

		6. 报告输出阶段 渗透测试工作全部完成后输出报告，报告中阐明客户系统中存在的安全隐患以及专业的漏洞风险处置建议； 7. 汇报阶段 ★向用户汇报本次渗透测试的成果，并现场对用户提出的疑问进行现场答疑； 8. 漏洞复测阶段 当用户业务系统的漏洞修补完成后可申请一次免费的漏洞复测服务，用于验证业务系统的漏洞修补情况，并向用户提交复测报告。 三、服务交付物 《渗透测试报告》、《渗透测试复测报告》		
3	风险评估	一、服务概述 通过运用丰富的技术经验和专用工具对组织信息资产面临的威胁、存在的脆弱性、现有防护措施及综合作用而带来风险的发生可能性进行评估，最终提供完整的风险评估报告及修复建议。 二、服务内容 1. 资产识别 ★使用专用工具对包括：业务系统、服务器、安全设备、网络设备等进行自动化扫描发现、识别、评估，可覆盖所有的资产，根据业务对资产的实际依赖程度区分重要资产，脆弱性识别、威胁识别、风险分析等后期工作将针对重要资产进行识别； 2. 脆弱性评估 漏洞扫描：使用专用工具的漏洞扫描功能，快速从内网和外网两个角度来查找网络结构、网络设备、服务器主机、数据和用户账号/口令等安全对象目标存在的安全漏洞，并给出关于安全隐患的详细信息； 基线配置核查：使用专用工具的基线配置核查功能识别信息系统的安全配置情况； 3. 威胁评估 ★分析用户信息系统存在的威胁种类，确定威胁分类的标准；综合威胁来源、种类和其他因素后得出威胁列表；针对每项需要保护的信息资产，尽可能全面的发现资产所面临的威胁； 4. 防护能力评估 ★识别已有的安全控制措施，分析安全措施的有效性，确定威胁利用弱点的实际可能性，指出当前安全措施的不足； 5. 风险分析 综合考虑资产本身的价值、威胁发生几率、脆弱性的破坏力、现有防护能力等因素分析资产可能存在的安全风险，结合风险对业务战略的影响程度区别明确风险处置计划； 6. 风险评估报告 根据资产识别、脆弱性评估、威胁评估、防护能力评估的输出结果进行风险分析之后，输出风险评估报告，风险评估报告中为用户提供符合业务需求的安全整改建议； 7. 风险整改验证 在用户根据风险评估报告完成对应风险项整改后，可以免费申请一次整改项结果验证。 三、服务交付物	4	套

		《风险评估报告》		
4	漏洞扫描	一、服务概述 使用漏洞扫描工具对业务系统进行扫描，通过扫描工具准确识别出注入缺陷、跨站脚本攻击、非法链接跳转、信息泄露、异常处理等安全漏洞，全面检测并发现业务应用安全隐患。 二、服务内容 1.准备阶段 对目标用户的服务范围内资产进行搜集，获取域名、IP、网络拓扑等相关信息，作为后续的扫描资产范围； 签署漏洞扫描委托授权函，获得用户的授权，约定漏洞扫描的时间和漏洞扫描工具；确认漏洞扫描设备接入点；与用户协商进行相关目标资产文件与数据的备份； 2.扫描实施阶段 ★实施扫描阶段开始现场检查网络连通性情况，根据情况分配合理 IP，确保扫描工具能探测到扫描范围内的所有主机，且无防火墙等安全设备进行阻拦，之后开展漏洞扫描；扫描过程中，如果目标系统出现无响应、中断等情况，扫描人员会立即中止漏洞扫描，并配合客户进行问题排查，在确认问题以及完成系统修复之后，根据分析结果调整扫描方式，经客户再次授权同意的前提下才会继续进行其余的扫描； 三、服务交付物 《漏洞扫描报告》	4	次
5	应急演练服务	一、服务概述 据相关国家标准或国际标准，提供对应的应急演练场景专项应急预案模板，以指导应急响应团队应对与处置安全事件； 制定应急演练方案及脚本并协助开展应急演练，模拟安全事件发生及处置的全过程，提高应对安全事件的处置能力，预防和减少安全事件造成的危害和损失。 二、服务内容 ★应急演练服务主要通过模拟各种突发事件场景进行，根据突发网络安全事件的性质，应急演练场景可分为：有害程序事件演练、网络攻击事件演练、信息破坏事件演练、设备设施故障演练； 有害程序事件：内网传播型病毒应急演练、勒索病毒应急演练、挖矿病毒应急演练等； 网络攻击事件：漏洞攻击应急演练、后门攻击应急演练等； 信息破坏事件：网站篡改应急演练、网页挂马应急演练等； 设备设施故障事件：网络设备故障应急演练、服务器故障应急演练等； 三、服务交付物 《应急演练方案》、《应急演练总结报告》、《专项应急预案模板》	2	次
6	基线核查	一、服务概述 对重要服务器、操作系统、网络设备、安全设备、中间件、数据库等基于信息安全风险的角度进行配置核查，检测网络设备的安全策略弱点和部分主机的安全配置错误等安全隐患。提出整改建议，指导运维人员优化配置策略，从而达到相应的安全防护要求。 二、服务内容	1	次

		1.主机操作系统检查内容 主机操作系统安全配置检查包含但不限于以下内容：帐号和口令管理、异常启动项、认证合授权策略、访问控制、通信协议、日志审核策略、文件系统权限、帐号和口令管理、防 ddos 攻击、剩余信息保护、其它安全配置； 2.数据库检查内容 ★数据库安全配置检查包含但不限于以下内容：帐号和口令管理认证、认证和授权策略、访问控制、通讯协议、日志审核功能、其他安全配置； 3.中间件检查内容 ★中间件及常见网络服务安全配置检查包含但不限于以下内容：帐号和口令管理认证、授权策略、通讯协议、日志审核功能、其他安全配置； 4.网络设备及安全设备检查内容 网络及安全设备安全配置检查包含但不限于以下内容：OS 安全、异常启动项、帐号和口令管理、认证和授权策略、网络与服务、访问控制策略、通讯协议、路由协议、日志审核策略、加密管理、设备其他安全配置。 三、服务交付物 《基线核查安全评估报告》		
7	安全设备巡检服务	一、服务概述 提供安全巡检服务，每月一次例行安全设备巡检，巡检内容为分为硬件状态检查、安全性检查和稳定性检查， 二、服务内容 1、硬件状态检查包含：设备电源指示灯，网口指示灯，设备 ALARM 灯，CPU，内存等使用情况； 2、安全性检查包含：配置备份，规则库更新，软件升级，预警补丁更新情况； ★3、稳定性检查包含：设备流量负载情况分析，系统运行日志分析，及时发现潜在风险。 三、服务交付物 《安全设备巡检报告》	1	年
8	应急响应服务	一、服务概述 提供安全事件应急响应服务，一旦客户发生网络安全事件，一般事件半小时内远程响应技术指导，重要事件 2 小时内现场响应处置，防止网络瘫痪、系统中断等对客户业务带来影响。 二、服务内容 ★1、应针对突发的安全事件，及时进行评估风险，按需协助客户对高危对象进行紧急安全策略加固； ★2、应针对突发的安全事件，对病毒或恶意代码进行安全扫描与紧急查杀，并采取其他措施消除安全风险； 3、在安全事件报告和响应处理过程中，应按流程进行汇报，分析和鉴定。 三、服务交付物 《应急响应报告》	1	年
9	重大节日	一、服务概述 提供重要时期安全值守保障服务，安排指定的安全专家在重要保障时期	1	年

	网络安全保障服务	提供每日的日志分析和研判服务，确保重要时期客户业务的安全稳定运行。 二、服务内容 1、在重大会议、节假日等特殊时期内，指派安全攻防经验丰富的安全专家，对客户目标系统进行远程安全值守和保障，对业务系统的安全状况进行安全监控和日志分析。 ★2、在重大节日期间，当目标遭受黑客入侵攻击时，值守人员应立即对入侵事件进行分析、检测、抑制、处理，查找入侵来源并恢复系统正常运行，完成后给出应急响应报告，报告中将还原入侵过程，同时给出对应的解决建议。 三、服务交付物 《重大节日保障方案》 《重大节日值守日报》 《重大节日值守总结报告》		
10	安全策略优化服务	一、服务概述 提供对网络和安全设备的安全策略优化服务，对客户当前部署的网络和安全设备进行等保合规性配置检查，并根据等保合规要求调整优化安全配置。 二、服务内容 1、帐号和口令管理：对网络设备的管理员进行分级管理，权限更高的管理员的帐号和口令的管理要求必须保证是最严格等级，同时对其他管理员的帐号和口令的复杂度进行优化； ★2、认证和授权策略调整：对网络设备的登录帐号进行加固，使其满足一定强度的认证要求，并对不同级别的授权策略进行优化； ★3、网络与服务加固：网络安全设备的服务配置方面，必须遵循最小化服务原则，关闭网络安全设备不必要的所有服务，修复网络服务或网络协议自身存在的安全漏洞以降低网络的安全风险； 4、访问控制策略增强：针对网络安全设备管理设置访问安全限制策略，只允许特定主机访问网络设备； 5、日志审核策略增强：根据安全级别要求，开启网络设备必需的监控日志记录，并支持一定周期的日志本地存储或外置存储； 6、安全设备价值实现：未使用安全设备上线使用，安全设备功能和策略优化启用等。 三、服务交付物 《安全策略优化报告》	1	年
11	网络安全培训	一、服务概述 网络安全培训旨在提升企业内部员工安全认知，让员工认识到信息安全意识不足对组织可能造成的危害，传导应正确恪守的行为方式；通过全员安全意识的理论培训和案例分析，让信息安全“人防“保障有效支撑业务高效稳定运行。 二、服务内容 1、针对全体员工进行一次网络安全培训服务，提升员工网络安全意识、规范安全用网； 2、针对信息科进行一次网络安全运维培训，提升信息科技术人员网络安全运维能力。 三、服务交付物	1	项

		《全院网络安全意识培训》 《安全岗位技能培训》		

商务要求
1、本项目服务期限为 12 个月：合同签订后按时间节点完成招标范围内项目。 2、合同签订之日起一个月内付款 50%，测评完成后付款 50%。

★本项目不接受联合体投标。

其它要求：详见《采购文件》

二、合格供应商应当具备的资格条件

（一）一般条件要求：

符合《中华人民共和国政府采购法》第二十二条规定。

1、在中华人民共和国境内注册取得有效的营业执照（三证合一），具有独立法人资格或其他组织机构及法人委托文件（附法定代表人及授权委托人身份证正反两面复印件）；分公司投标的，必须由具有法人资格的总公司授权；

2. 须提供具备履行合同所必需的设备和专业技术能力的证明材料（自行承诺）；

3. 须提供经合法审计机构出具的 2022 或 2023 年度财务审计报告，或投标截止时间前 3 个月的资产负债表）【新注册企业提供当年内】；

4. 提供供应商 2023 年 9 月至今任意 3 月的依法缴纳税收及缴纳社会保障金的凭据或证明材料【新注册企业提供当年内或者依法不用纳税及缴纳社保的，须提供有效的证明文件】；

5. 提供供应商 1 年以上无违法不良记录的证明材料【新注册企业提供当年内】【供应商自行承诺】；

6. 其它特别指明要求提供的材料、证明等；项目属特种行业的提供相应证明材料。

（二）诚信资格要求：

提供购买标书当日至谈判前一天任一时间，在“信用中国”网站[www.creditchina.gov.cn，包括行业失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信名单]、中国政府采购网[政府采购严重违法失信行为记录名单 http://www.ccgp.gov.cn/cr/list]的查询记录截图[完整清晰]。

三、报名与采购文件获取

（一）报名与采购文件获取时间：

2024 年 5 月 8 日-2024 年 5 月 14 日[8:00-11:30;14:00-17:30][周末、节假日除外]，供应商须在规定的时间内到指定地点获取本采购文件，并登记备案，如在规定时间内未获取采购文件并登记备案的供应商均无资格参加。

（二）报名方式：

电子邮件报名；

（三）报名邮箱：

zysbzqrmyy2024@163.com ；

（四）相关提示及报名资料

参与本项目报名的投标人请在电子邮件主题：注明公司名称、竞标的项目名称。

正文注明公司名称、授权委托人姓名和联系方式、竞标的项目名称，另扫描以下资料作为该邮件附件发送至报名邮箱：

1）三证合一的营业执照副本（复印件加盖公章）；

2）法定代表人授权委托书附法定代表人及授权委托人身份证正反两面复印件（复印件加盖公章）；

3）诚信资格证明材料、无违法不良记录证明（复印件加盖公章）；

4）《遵义市播州区人民医院采购项目供应商报名表》；

5）《投标廉洁承诺书》。

四、响应文件递交须知

（一）截止时间：

2024 年 5 月 15 日 14：30（星期三）上班时间，逾期送达的文件拒不接收。

（二）投响应文件密封方式

档案袋密封。

五、开标时间和地点

（一）开标时间

2024 年 5 月 15 日 14 时 30 分（星期三）[北京时间]。

（二）开标地点

遵义市播州区人民医院远程医疗中心二楼开标室。

六、信息公开媒介

遵义市播州区人民医院[官网]:http://www.zysbzqrmyy.cn 。

七、保证金

供应商递交响应文件前，应提交人民币 0 元的保证金。望供应商以法律规范、行业标准自律谈判行为，不恶意扰乱投标规则和采购秩序，一经发现则列入黑名单并进行公示。

八、评标办法摘要

（一）合格供应商须提供规范有效的响应文件[1 正、1 副]对项目要求、技术参数、配置要求进行实质性响应。

（二）评标方法：

综合评标法。

（三）开标条件：

响应报价≥3 家。

九、联系方式

（一）主管科室：

信息科　联系人及电话：　李先生　18076239198

（二）办理科室：

总务科　联系人及电话：　罗女士　0851-27221960

（三）联系地址：

遵义市播州区人民医院远程医疗中心二楼开标室

（四）投诉与举报电话

纪委综合办　　联系电话：　0851-27252009

遵义市播州区人民医院总务科

2024 年 5 月 8 日