系统（平台）网络安全等级保护测评和密码应用安全性评估服务采购需求

一、采购清单（154 万元）

标段一：系统（平台）网络安全等级保护测评服务（70 万元）

序号	系统名称	服务内容	数量	单价（元）
1	智慧社会项目管理系统	等级保护测评	1	100000.00
2	华为云平台	等级保护测评	1	100000.00
3	上郡生活 APP	等级保护测评	1	100000.00
4	市时空信息云平台	等级保护测评	1	100000.00
5	市电子政务外网	等级保护测评	1	100000.00
6	华三云平台	等级保护测评	1	100000.00
7	数据共享交换平台	等级保护测评	1	100000.00
合计			700000	

标段二：系统（平台）密码应用安全性评估服务（84 万元）

序号	系统名称	服务内容	数量	单价（元）
1	智慧社会项目管理系统	商用密码应用安全性评估	1	120000.00
2	华为云平台	商用密码应用安全性评估	1	120000.00
3	上郡生活 APP	商用密码应用安全性评估	1	120000.00
4	市时空信息云平台	商用密码应用安全性评估	1	120000.00

5	市电子政务外网	商用密码应用安全性评估	1	120000.00
6	华三云平台	商用密码应用安全性评估	1	120000.00
7	数据共享交换平台	商用密码应用安全性评估	1	120000.00
合计			840000	

二、采购需求

标段一：系统（平台）网络安全等级保护测评服务

1.协助定级及备案

在单位自行定级的基础上。根据国家关于重要信息系统安全等级保护的相关标准和规范要求，测评机构协助单位填写《信息系统安全等级保护备案表》，指导到属地公安机关完成备案工作。

2.系统调研：

在单位相关部门人员的协助下，对重要信息系统进行调研和梳理，了解单位当前重要信息系统资产现状。

3.编制测评方案：

根据对单位的资产调研结果、网络架构及系统现状分别制定编制《测评方案》，《测评方案》通过单位相关项目负责人或技术人员审核通过后，严格按照方案进行现场测评工作。

4.进行现场测评和渗透测试：

在测评机构在测评过程中依据国标和相关行业标准，通过公安部测评机构认证的专业等级测评师开始进入现场进行现场测评工作，对承载信息系统的网络及信息系统所涉及的系统的安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全

管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理共10个层面进行安全等级保护测评。

在单位授权的前提下，针对三级以上信息系统由测评机构专业渗透团队采取模拟黑客攻击的方式，按照外网风险信息收集、外网渗透测试、内网横向渗透测试、测试结论整理汇报流程，开展渗透测试工作，协助单位完成漏洞检测、漏洞分类跟踪管理、漏洞预警及协助整改工作。

5.制定整改方案及协助进行整改：

完成现场测评后，依据《信息安全技术网络安全等级保护测评要求》（GB/T28448-2019）中相应级别重要信息系统的要求分别对单元测评结果、层面测评结果、整体测评结果进行分析，找出单位的重要信息系统中存在的安全问题或安全隐患，评估安全问题或安全隐患将导致的安全威胁，形成差距分析报告，为整改工作提供依据。针对单位的重要信息系统中存在的安全问题或安全隐患制定相应的整改方案。根据测评报告与国家相关规定测评机构协助单位运维人员对调度系统进行建设整改，包括系统安全、账户口令、规章制度、防火墙策略等。协助单位对重要信息系统进行整改，使系统达到《信息安全技术网路安全等级保护测评要求》（GB/T28448-2019）中相应级别信息系统的安全防护能力。

6.安全加固：

对重要信息系统安全整改建议进行确认，并依照建议，协助单位进行漏洞修复，补丁升级等非硬件层面的安全加固，指定可执行的安全整改方案和计划，然后协助单位分步实施安全整改工

作。

7. 进行现场复测：

在单位的重要信息系统的安全建设整改工作完成后，进行现场复测评工作，对安全建设整改工作进行验证。

8. 编制测评报告、渗透测试报告：

在完成测评和渗透测试后，对单位重要信息系统的各单元测评、层面测评、整体测评结构进行汇总分析，编制《测评报告》、《渗透测试报告》。整理项目过程中所有相关的过程文档，做到科学、详尽、统一，符合行业相关规范提交单位相关人员，由单位组织项目验收。

9. 信息系统风险评估服务

根据系统安全防护评估相关标准，在系统等级保护测评的基础上，增加如下评估项：资产评估、威胁评估、通用应用评估、基础设施安全评估、体系结构安全评估、系统本体安全评估、全面安全管理评估、安全应急能力评估、现有安全措施有效性评估等。

10. 安全咨询服务

服务方在测评项目结束后，要提供至少一年的安全咨询服务，包括但不限于安全技术咨询、安全整改建设咨询、管理制度及国家法规等，服务方需提供咨询建议和方案建议。

标段二：系统（平台）密码应用安全性评估服务

1. 系统密评：需针对评估对象，编制密码应用安全性评估报告，报告按照国家密码管理局要求包含的内容编制或参

考模版编制，查找漏洞，找出差距，提出有针对性的加强完善密码安全管理和防护建议。

2. 系统备案：对系统进行密评备案工作，取得商用密码应用安全性评估报告后，按照国家有关规定报送国家密码管理部门所在地省、自治区、直辖市密码管理部门备案，并协助系统责任主体单位获得相应密评备案证明。

3. 安全培训：在项目实施过程中或在项目实施结束后，通过安全培训使有关人员加深对密码安全工作的掌握程度，并对行业内的最佳实践案例进行分享，从而达到将密码安全工作与信息系统、安全设备的安全运维工作相结合的状态。

4. 配合检查服务：提供协助响应密码管理局、单位内部以及第三方机构针对商用密码应用安全性评估工作的检查工作。服务内容包括协助系统责任主体单位进行系统资料准备、完善各类资料文档，配合检查过程中的答疑及技术支持及其他现场检查的响应。

5. 安全咨询服务：提供一年技术咨询服务，包括新建信息系统密码安全建设方案咨询服务以及其他相关安全咨询服务，技术服务工程师在接到系统责任主体单位服务请求后应立即响应，帮助客户解决信息安全相关技术问题，全面配合系统责任主体单位做好业务系统安全保障工作。

榆林市大数据中心

2024 年 3 月 12 日