政府采购项目采购需求

采购单位：眉山市生态环境局

所属年度：2024年

编制单位：眉山市生态环境局

编制时间：2024年01月17日

一、项目总体情况

（一）项目名称： 环境信息化系统等级保护测评和密保测评采购项目

（二）项目所属年度： 2024年

（三）项目所属分类： 服务

（四）预算金额（元）：540,000.00元，大写（人民币）：伍拾肆万元整

（五）项目概况：

依据《中华人民共和国网络安全法》《中华人民共和国计算机信息系统安全保护条例》(国务院令147号)《信息安全等级保护管理办法》、《中华人民共和国密码法》、《信息系统密码应用测评要求》GM/T 0115-2021等文件规定，对采购人信息系统开展网络安全等级保护测评服务、商用密码应用安全性评估和商用密码应用方案评估工作。

（六）本项目是否有为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商：否

二、项目需求调查情况

依据《政府采购需求管理办法》的规定，本项目不需要需求调查，具体情况如下：

（一）需求调查方式

（二）需求调查对象

（三）需求调查结果

1.相关产业发展情况

2.市场供给情况

3.同类采购项目历史成交信息情况

4.可能涉及的运行维护、升级更新、备品备件、耗材等后续采购情况

5.其他相关情况

三、项目采购实施计划

（一）采购组织形式：分散采购

（二）采购方式：竞争性磋商

（三）本项目是否单位自行组织采购：否

（四）采购包划分：不分包采购

（五）执行政府采购促进中小企业发展的相关政策

本项目专门面向中小企业采购。面向中小企业采购金额为540000.00元，总体预留比例为100.00%，其中，面向小微企业采购金额为0.00元，占0%。

（六）是否采购环境标识产品：否

（七）是否采购节能产品：否

（八）项目的采购标的是否包含进口产品：否

（九）采购标的是否属于政府购买服务：否

（十）是否属于政务信息系统项目：是

（十一）是否属于高校、科研院所的科研仪器设备采购：否

（十二）是否属于PPP项目：否

（十三）是否属于一签多年项目：是

一签多年服务期限：三年

四、项目需求及分包情况、采购标的

（一）分包名称：合同包一

1、执行政府采购促进中小企业发展的相关政策

1) 专门面向中小企业采购

2)面向的企业规模： 中小企业

3)预留形式： 设置专门采购包

4)预留比例： 100%

2、预算金额（元）：540,000.00，大写（人民币）： 伍拾肆万元整

最高限价（元）： 540,000.00，大写（人民币）： 伍拾肆万元整

3、评审方法：综合评分法

4、定价方式：固定单价

5、是否支持联合体投标：否

6、是否允许合同分包选项：否

7、拟采购标的的技术要求

1	**采购品目**	测试评估认证服务	**标的名称**	环境信息化系统等级保护测评和密保测评采购项目
	数量	1.00	**单位**	项
	合计金额（元）	540,000.00	**单价（元）**	540,000.00
	是否采购节能产品	否	**未采购节能产品原因**	无
	是否采购环保产品	否	**未采购环保产品原因**	无
	是否采购进口产品	否	**标的物所属行业**	软件和信息技术服务业

标的名称：环境信息化系统等级保护测评和密保测评采购项目

参数性质	序号	技术参数与性能指标
		项目概况： 依据《中华人民共和国网络安全法》《中华人民共和国计算机信息系统安全保护条例》(国务院令147号)《信息安全等级保护管理办法》、《中华人民共和国密码法》、《信息系统密码应用测评要求》GM/T 0115-2021等文件规定，对采购人信息系统开展网络安全等级保护测评服务、商用密码应

用安全性评估和商用密码应用方案评估工作。

网络安全等级保护测评服务			
序号	系统名称	等级	服务周期
1	电子政务综合管理平台	三级	合同有效期内每年1次（共3年）
2	眉山视频中心系统	三级	合同有效期内每年1次（共3年）
3	数据共享交换平台	三级	合同有效期内每年1次（共3年）
4	国控重点污染源自动监控系统	二级	合同有效期内每年1次（共3年）
5	数智指挥调度平台	二级	合同有效期内每年1次（共3年）
6	执法监管调度平台	二级	合同有效期内每年1次（共3年）
商用密码应用安全性评估			
序号	系统名称	等级	服务周期
1	电子政务综合管理平台	三级	合同有效期内每年1次（共3年）
2	眉山视频中心系统	三级	合同有效期内每年1次（共3年）
3	数据共享交换平台	三级	合同有效期内每年1次（共3年）
4	国控重点污染源自动监控系统	二级	合同有效期内每年1次（共3年）
5	数智指挥调度平台	二级	合同有效期内每年1次（共3年）
6	执法监管调度平台	二级	合同有效期内每年1次（共3年）
为采购人提供网络安全、密码应用咨询、业务培训服务，每月提供 1次渗透测试服务并提供 1 份信息化网络的漏洞扫描报告和病毒扫描报告等。			

3.2.2服务要求

采购包1：

标的名称：环境信息化系统等级保护测评和密保测评

测评服务需求。

根据等级保护测评的工作要求，测评范围覆盖安全管理中心、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、安全运维管理十个层面，以及云计算安全、移动互联安全、物联网安全、工业控制系统安全、大数据安全等扩展方面的要求。

具体服务内容包括：

1.协助采购人进行信息系统的信息安全等级定级和备案工作。

2.差距测评，至少包括：

安全技术测评。包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心五个方面的安全测评。

安全管理测评。包括安全管理制度、安全管理机构、安全管理人员、安全系统建设和安全系统运维五个方面的安全测评。

形成问题汇总及整改意见报告。依据测评结果，对等级测评结果进行汇总统计（测评项符合情况及比例、单元测评结果符合情况比例以及整体测评结果）；通过对信息系统基本安全保护状态的分析给出初步测评结论。根据测评结果制定《系统等级保护测评问题汇总及整改意见报告》，列出被测信息系统中存在的主要问题及整改意见。

3.协助完成整改工作。依据整改方案，为安全整改的各项工作提供技术咨询服务。

4.等级保护测评，至少包括：

按照等级保护相关标准对系统从安全技术、安全管理等方面进行等级测评工作。

编制测评报告，制定并提交《网络安全等级保护测评报告》，报告需提交公安机关有关部门备案，且能满足合规性要求。

按照信息系统等级保护测评依据开展测评工作（包括但不限于以下项目）。

2.2 测评服务内容指标。

2.2.1 物理安全检查。主要是了解信息系统的物理安全保障情况。涉及对象为机房。在内容上，物理安全层面测评实施过程涉及的工作单元，具体如下表：

表1 安全物理测评内容：

序号	工作单元名称	工作单元描述
1	物理位置的选择	检查机房，测评机房物理场所在位置上是否具有防震、防风和防雨等多方面的安全防范能力。
2	物理访问控制	检查机房出入口等过程，测评信息系统在物理访问控制方面的安全防范能力。
3	防盗窃和防破坏	检查机房内的主要设备、介质和防盗报警设施等过程，测评信息系统是否采取必要的措施预防设备、介质等丢失和被破坏。
4	防雷击	检查机房设计/验收文档，测评信息系统是否采取相应的措施预防雷击。
5	防火	检查机房防火方面的安全管理制度，检查机房防火设备等过程，测评信息系统是否采取必要的措施防止火灾的发生。
6	防水和防潮	检查机房及其除潮设备等过程，测评信息系统是否采取必要措施来防止水灾和机房潮湿。
7	防静电	检查机房等过程，测评信息系统是否采取必要措施防止静电的产生。
8	温湿度控制	检查机房的温湿度自动调节系统，测评信息系统是否采取必要措施对机房内的温湿度进行控制。
9	电力供应	检查机房供电线路、设备等过程，测评是否具备为信息系统提供一定电力供应的能力。

10	电磁防护	检查主要设备等过程，测评信息系统是否具备一定的电磁防护能力。

2.2.2 安全通信网络

安全通信网络检查主要是了解系统的网络架构和通信传输等，涉及对象为防火墙、核心路由器、核心交换机等设备和网络架构。在内容上，安全通信网络层面测评过程涉及的工作单元，具体如下表：

表2 安全通信网络测评内容

序号	工作单元名称	工作单元描述
1	网络架构	检查核心设备的CPU和内存使用率，整个网络带宽是否满足现状，VLAN划分是否合理，网络架构是否做到设备冗余、链路。
2	通信传输	检查数据在传输过程中的的完整性和保密性措施。
3	可信计算	检查设备是否进行可信验证。

2.2.3 安全区域边界

安全区域边界检查主要是了解系统在网络边界的防护措施，涉及对象为防火墙、入侵检测、安全审计等安全设备。在内容上，安全区域边界层面测评实施过程涉及的工作单元，具体如下表：

表3 安全区域边界测评内容

序号	工作单元名称	工作单元描述
1	边界防护	检查网络边界是否有访问控制设备，访问控制策略是否合理，是否关闭了闲置端口等。
2	访问控制	检查网络中的访问控制策略是否合理、有效。
3	入侵防范	检查网络中是否采用了入侵防范措施，验证该措施是否有效。
4	恶意代码和垃圾邮件防范	检查网络中是否有恶意代码和垃圾邮件防范措施。
5	安全审计	检查网络中是否有综合安全审计措施。
6	可信验证	检查设备是否进行可信验证。

2.2.4 安全计算环境

安全计算环境检查主要是了解系统的运行环境是否采取了相关安全措施，涉及对象为网络设备、安全设备、操作系统、数据库、中间件等。内容上，安全计算环境层面测评实施过程涉及的工作单元，具体如下表：

表4 安全计算环境测评内容

序号	工作单元名称	工作单元描述
1	身份鉴别	检查所有设备的登录用户是否有身份鉴别措施，是否有复杂度、唯一性等检查。
2	访问控制	检查用户的权限分配情况，默认用户和默认口令使用情况等。
3	安全审计	检查是否开启安全审计功能，是否能审计到每个用户，审计记录是否有保护措施。
4	入侵防范	检查设备在运行过程中的入侵防范措施，如关闭不需要的端口和服务、最小化安装、部署入侵防范产品等。
5	恶意代码防范	检查设备的恶意代码防范情况。
6	可信验证	检查设备是否进行可信验证。

7	数据完整性	检查系统数据的传输完整性和存储完整性措施。
8	数据保密性	检查系统数据的传输保密性和存储保密性措施。
9	数据备份恢复	检查系统的安全备份情况，如重要信息的备份、硬件和线路的冗余等。
10	剩余信息保护	检查系统的剩余信息保护情况，如将用户鉴别信息以及文件、目录和数据库记录等资源所在的存储空间再分配时的处理情况。
11	个人信息保护	检查系统对个人信息的采集和使用情况。

2.2.5 安全管理中心

安全管理中心检查主要是了解系统在管理、审计等集中管理的情况，涉及对象为综合管理类设备、综合审计类设备等。在内容上，安全管理中心实施过程涉及的工作单元，具体如下表：

表5 安全管理中心测评内容

序号	工作单元名称	工作单元描述
1	系统管理	检查是否对系统管理员进行统一的身份鉴别，操作审计等。
2	审计管理	检查是否对审计管理员进行统一的身份鉴别，操作审计等。
3	安全管理	检查是否对安全管理员进行统一的身份鉴别，操作审计等。
4	集中管控	检查是否划分独立的安全管理区域，是否对网络中运行的设备进行状态监测、日志审计、安全审计等，是否对补丁、恶意代代码进行统一管理。

2.2.6 安全管理制度

安全管理制度测评是为了了解评测安全管理制度的制定、发布、评审和修订等情况。主要涉及安全主管人员、安全管理人员、各类其它人员、各类管理制度、各类操作规程文件等对象。在内容上，安全管理制度测评实施过程涉及的工作单元，具体如下表：

表6 安全管理制度测评内容

序号	工作单元名称	工作单元描述
1	安全策略	核查网络安全工作的总体方针和安全策略文件是否明确机构安全工作的总体目标、范围、原则和各类安全策略
2	管理制度	检查有关管理制度文档和重要操作规程等过程，测评信息系统管理制度在内容覆盖上是否全面、完善。
3	制定和发布	检查有关制度制定要求文档等过程，测评信息系统管理制度的制定和发布过程是否遵循一定的流程。
4	评审和修订	检查管理制度评审记录等过程，测评信息系统管理制度定期评审和修订情况。

2.2.7 安全管理机构

安全管理机构测评是为了了解评测安全管理机构的组成情况和机构工作组织情况。主要涉及安全主管人员、安全管理人员、相关的文件资料和工作记录等对象。在内容上，安全管理机构测评实施过程涉及的工作单元，具体如下表：

表7 安全管理机构测评内容

序号	工作单元名称	工作单元描述
1	岗位设置	检查部门/岗位职责文件，测评信息系统安全主管部门设置情况以及各岗位设置和岗位职责情况。
2	人员配备	检查人员名单等文档，测评信息系统各个岗位人员配备情况。

3	授权和审批	检查相关文档，测评信息系统对关键活动的授权和审批情况。
4	沟通与合作	检查相关文档，测评信息系统内部部门间、与外部单位间的沟通与合作情况。
5	审核与检查	检查记录文档等过程，测评信息系统安全工作的审核和检查情况。

2.2.8 安全管理人员

安全管理人员测评是为了了解单位人员安全方面的情况，主要涉及安全主管人员、人事管理人员、相关管理制度、相关工作记录等对象。在内容上，安全管理人员测评实施过程涉及的工作单元，具体如下表：

表8 安全管理人员测评内容

序号	工作单元名称	工作单元描述
1	人员录用	检查人员录用文档等过程，测评信息系统录用人员时是否对人员提出要求以及是否对其进行各种审查和考核。
2	人员离岗	检查人员离岗安全处理记录等过程，测评信息系统人员离岗时是否按照一定的手续办理。
3	安全意识教育和培训	检查培训计划和执行记录等文档，测评是否对人员进行安全方面的教育和培训。
4	外部人员访问管理	检查有关文档等过程，测评对第三方人员访问（物理、逻辑）系统是否采取必要控制措施。

2.2.9 安全建设管理

安全建设管理测评是为了了解评测系统建设管理过程中的安全控制情况，主要涉及安全主管人员、系统建设负责人、各类管理制度、操作规程文件、执行过程记录等对象。在内容上，安全建设管理测评实施过程涉及的工作单元，具体如下表：

表9 安全建设管理测评内容

序号	工作单元名称	工作单元描述
1	定级和备案	检查系统定级相关文档等过程，测评是否按照一定要求确定系统的安全等级。
2	安全方案设计	检查系统安全建设方案等文档，测评系统整体的安全规划设计是否按照一定流程进行。
3	产品采购和使用	测评是否按照一定的要求进行系统的产品采购。
4	自行软件开发	检查相关软件开发文档等，测评自行开发的软件是否采取必要的措施保证开发过程的安全性。
5	外包软件开发	检查相关文档，测评外包开发的软件是否采取必要的措施保证开发过程的安全性和日后的维护工作能够正常开展。
6	工程实施	检查相关文档，测评系统建设的实施过程是否采取必要的措施使其在机构可控的范围内进行。
7	测试验收	检查测试验收等相关文档，测评系统运行前是否对其进行测试验收工作。
8	系统交付	检查系统交付清单等过程，测评是否采取必要的措施对系统交付过程进行有效控制。
9	等级测评	检查系统之前等级测评的情况，以及之前测评机构的资质等。
10	服务供应商选择	测评是否选择符合国家有关规定的安全服务单位进行相关的安全服务工作。

2.2.10 安全运维管理

★ 1

安全运维管理测评是为了了解系统运维管理过程中的安全控制情况，主要涉及安全主管人员、安全管理人员、各类运维人员、各类管理制度、操作规程文件、执行过程记录等对象。在内容上，安全运维管理测评实施过程涉及的工作单元，具体如下表：

表10 安全运维管理测评内容

序号	工作单元名称	工作单元描述
1	环境管理	检查机房安全管理制度，机房和办公环境等过程，测评是否采取必要的措施对机房的出入控制以及办公环境的人员行为等方面进行安全管理。
2	资产管理	检查资产清单，检查系统、网络设备等过程，测评是否采取必要的措施对系统的资产进行分类标识管理。
3	介质管理	检查介质管理记录和各类介质等过程，测评是否采取必要的措施对介质存放环境、使用、维护和销毁等方面进行管理。
4	设备维护管理	检查设备使用管理文档和设备操作规程等过程，测评是否采取必要的措施确保设备在使用、维护和销毁等过程安全。
5	漏洞和风险管理	检查系统对于漏洞和安全隐患风险的管理，是否有报告、记录等文档，是否定期开展安全测评等。
6	网络和系统安全管理	检查系统和网络的安全管理文档，是否明确了角色划分、权限划分，是否覆盖安全策略、账户管理、配置文件的生成及备份、变更审批等内容；检查运维操作日志是否覆盖网络和系统的日常巡检、运行维护、参数的设置和修改等内容；核查是否具有对日志、监测和报警数据等进行分析统计的报告；核查开通远程运维的审批记录，核查针对远程运维的审计日志是否不可以更改等。
7	恶意代码防范管理	检查恶意代码防范管理文档和恶意代码检测记录等过程，测评是否采取必要的措施对恶意代码进行有效管理，确保系统具有恶意代码防范能力。
8	配置管理	检查是否对基本配置信息进行记录和保存，基本配置信息改变后是否及时更新基本配置信息库等。
9	密码管理	测评是否能够确保信息系统中密码算法和密钥的使用符合国家密码管理规定。
10	变更管理	检查变更方案和变更管理制度等过程，测评是否采取必要的措施对系统发生的变更进行有效管理。
11	备份与恢复管理	检查系统备份管理文档和记录等过程，测评是否采取必要的措施对重要业务信息，系统数据和系统软件进行备份，并确保必要时能够对这些数据有效地恢复。
12	资产管理	检查是否有资产清单，清单是否包括资产类别、资产责任部门、重要程度和所处位置等内容；是否依据资产的重要程度对资产进行标识，不同类别的资产在管理措施的选取上是否不同；核查资产管理制度是否明确资产的标识方法以及不同资产的管理措施要求。
13	应急预案管理	检查应急响应预案文档等过程，测评是否针对不同安全事件制定相应的应急预案，是否对应急预案展开培训、演练和审查等。
14	外包运维管理	检查外包运维服务情况，单位是否符合国家有关规定，协议是否明确约定外包运维的范围和工作内容等。

2.3 技术标准和规范

1.《中华人民共和国计算机信息系统安全保护条例》(国务院令147号)

2.《信息安全等级保护管理办法》

3.《计算机信息系统安全保护等级划分准则》（GB17859-1999）

4.《信息安全技术网络安全等级保护定级指南》（GB/T22240-2020）

5.《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）

6.《信息安全技术网络安全等级保护测评要求》（GB/T28448-2019）

7.《信息安全技术网络安全等级保护测评过程指南》（GB/T28449-2018）

8.《信息安全风险评估规范》（GB/T20984-2007）

注：以上涉及的相关标准及规范，若国家有最新出台的标准和规定，则按最新标准和规定执行。

2.4 其他要求

★1.保密：对测评的过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据进行任何侵害采购方的行为，否则采购方有权追究供应商的责任。（实质性要求，单独提供承诺函）

2.标准性：测评方案的设计与实施应依据国家等级保护的相关标准进行。

3.规范性：供应商的工作中的过程和文档，具有很好的规范性，可以便于项目的跟踪和控制，测评出具的报告须符合公安部颁布的《网络安全等级测评报告模板》的相关要求。

4.可控性：等保测评服务的进度要按照采购文件的要求，保证采购方对于测评工作的可控性。

5.整体性：等保测评服务的范围和内容应当整体全面，包括国家等级保护相关要求测评要求涉及的各个层面。

6.安全性：等保测评服务工作应不得影响系统和网络的正常运行；测评工作不得对现有信息系统的正常运行、业务的正常开展产生任何影响。

7.人员要求：测评期间需遵守被测单位相关管理规定，禁止利用测评工作从事危害被测单位利益、安全的活动。

★2.5 成果要求（实质性要求）

在测评完成后，供应商须提供以下文档资料：

1.《信息系统安全问题汇总及整改建议》

2.《网络安全等级保护等级测评报告》及过程资料

（三）商用密码应用安全性评估。

3.1 服务需求

供应商对系统按密码应用要求开展密码测评工作,依据GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》从密码应用技术要求、密码应用管理要求两个角度出发，围绕信息系统的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、管理制度、人员管理、建设运行、应急处置八个方面开展密码测评工作，通过现场测评逐项比较信息系统与其相应安全等级要求之间的差距，进行逐项分析、整体分析、量化评估、风险分析，为信息系统的密码应用建设提供工作建议，保障信息系统密码合规、正确、有效地应用。供应商需提供符合相关要求的商用密码应用安全性评估报告，并协助在当地密码管理局备案。

3.2 服务内容

开展密码测评工作，并依据相关文件模板，对对测评的系统出具符合国家密码管理局和当地密码管理部门要求的密评报告。

根据测评结果，给出整改意见，指导软件承建单位对被测系统暴露出的密码应用安全问题进行整改。

根据国家密码管理局关于规范商用密码应用安全性评估结果备案工作的通知，协助采购人准备备案资料并完成密评备案工作。

对采购人安全技术和密码管理人员开展相关培训。

协助采购人完成与密评相关的其他工作。

3.3 服务要求

测评准备。供应商通过查阅被测系统已有资料并使用调查表格的方式，了解整个系统的构成和密码保护情况，为编写密评方案和开展现场测评工作奠定基础。测评项目组成员在进行现场测评之前，熟悉与被测信息系统相关的各种组件、调试测评工具、准备各种表单等。

方案编制。根据已经了解到的被测信息系统情况，分析整个被测系统及其涉及的业务应用系统，以及与此相关的密码应用情况，确定出本次测评的测评对象；根据已经了解到的被测系统定级结果，确定出本次测评的测评指标；确认测评过程中需要现场检查的关键安全点，并且充分考虑到检查的可行性和风险，最大限度的避免对被测系统，尤其是在线运行业务系统的影响；确定现场测评的具体实施内容；最终完成测评方案的编制。

现场测评。现场测评准备：召开测评现场首次会，供应商介绍测评工作，交流测评信息，进一步明确测评计划和测评方案中的内容，说明测评过程中具体的实施工作内容，测评时间安排，测评过程中可能存在的安全风险等，以便于后面的测评工作开展。供应商和采购方确认现场测评需要的各种资源，包括采购方的配合人员和需要提供的测评条件等，确认被测信息系统已备份过系统及数据。采购方签署现场测评授权书。密评人员根据会议沟通结果，对测评结果记录表单和测评程序进行必要的更新。

测评项目组根据密评方案以及现场测评准备的结果，安排密评人员在现场完成测评工作，汇总现场测评的测评记录；召开测评现场结束会，供应商和采购方对测评过程中发现的问题进行现场确认；密评机构归还测评过程中借阅的所有文档资料，并由采购方文档资料提供者签字确认。

分析与报告编制活动。

在现场测评工作结束后，供应商对现场测评获得的测评结果进行汇总分析，形成评估结论，并编制评估报告。

密评人员在初步判定各测评单元涉及的各个测评对象的测评结果后，还需进行单元测评、整体测评、量化评估和风险分析。经过整体测评后，有的测评对象的测评结果可能会有所变化，需进一步修订测评结果，而后进行量化评估和风险分析，最后形成评估结论。

3.4 技术要求

依据GB/T 39786—2021《信息安全技术信息系统密码应用基本要求》、GM/T 0115-2021《信息系统密码应用测评要求》、GM/T 0116-2021《信息系统密码应用测评过程指南》、《信息系统密码应用高风险判定指引》等标准和系统自身的安全需求等，对被测系统进行密评工作，密码应用安全性评估的技术服务包括但不限于以下内容:

3.4.1 通用测评要求

核查信息系统中使用的密码算法、密码技术、密码产品和密码服务是否满足国家密码管理的相关标准或规范要求。

3.4.2 密码应用技术要求测评

具体包括但不限于:物理和环境安全测评、网络和通信安全测评、设备和计算安全测评、应用和数据安全测评，制定安全验证性测评工作方案，验证不同安全等级信息系统的密码应用是否达到相应安全等级的安全保护能力、是否满足相应安全等级的保护要求。

3.4.3 物理和环境安全测评

物理和环境安全主要实现对测评的系统所在机房等重要区域的物理防护，物理机房的进出必须严格符合相关规范，并对相关人员进出信息实时记录，防止非法人员采用非法手段进出，如果出现人为物理破坏将造成不可逆的重大损失。

针对“身份鉴别”、“电子门禁记录数据存储完整性”、“视频监控记录数据存储完整性”等物理和环境安全方面采取的密码保障措施进行各项测评，详细记录现场测评情况（如访谈记录、配置截图、抓包分析截图、产品照片等），完成单项及单元测评结果判定。测评结果应由采购方配合人员确认。

标准要求内容：

采用密码技术进行物理访问身份鉴别,保证重要区域进入人员身份的真实性。

采用密码技术保证电子门禁系统进出记录数据的存储完整性。

采用密码技术保证视频监控音像记录数据的存储完整性。

3.4.4 网络和通信安全测评

网络和通信安全主要实现对信息系统与经由外部网络连接的实体进行网络通信时的安全防护，密码应用要求主要涉及通信过程中实体身份真实性、数据机密性和数据完整性，以及网络边界访问控制和设备接入控制。

针对“身份鉴别”、“通信数据完整性”、“通信过程中重要数据的机密性”、“网络边界访问控制信息的完整性”、“安全接入认证”等网络和通信安全方面采取的密码保障措施进行各项测评，详细记录现场测评情况(如访谈记录、配置截图、抓包分析截图、产品照片等)，完成单项及单元测评结果判定。测评结果应由采购方配合人员确认。

标准要求内容：

采用密码技术对通信实体进行身份鉴别,保证通信实体身份的真实性。

宜采用密码技术保证通信过程中数据的完整性。

采用密码技术保证通信过程中重要数据的机密性。

采用密码技术保证网络边界访问控制信息的完整性。

采用密码技术对从外部连接到内部网络的设备进行接入认证,确保接入设备身份的真实性。

3.4.5 设备和计算安全测评

设备和计算安全主要实现对对测评的系统中各类设备和计算环境的安全防护,密码应用要求主要涉及对登录设备用户的身份鉴别、远程管理通道的建立、重要可执行程序来源真实性，以及系统资源访问控制信息、设备的重要信息资源安全标记、重要可执行程序、日志记录的完整性。

针对“身份鉴别”、“远程管理通道安全”、“系统资源访问控制信息完整性”、“重要信息资源安全标记完整性”、“日志记录完整性”、“重要可执行程序完整性、重要可执行程序来源真实性”等设备和计算安全方面采取的密码保障措施进行各项测评，详细记录现场测评情况(如访谈记录、配置截图、抓包分析截图、产品照片等)，完成单项及单元测评结果判定。测评结果应由采购方配合人员确认。

标准要求内容：

采用密码技术对登录设备的用户进行身份鉴别,保证用户身份的真实性。

远程管理设备时,采用密码技术建立安全的信息传输通道。

采用密码技术保证系统资源访问控制信息的完整性。

采用密码技术保证设备中的重要信息资源安全标记的完整性。

采用密码技术保证日志记录的完整性。

采用密码技术对重要可执行程序进行完整性保护,并对其来源进行真实性验证。

3.4.6 应用和数据安全

实现对信息系统中应用及其数据的安全防护,密码应用主要涉及应用的用户身份鉴别、访问控制，以及应用相关重要数据的存储安全、传输安全和相关行为的不可否认性。其中，重要数据包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

针对“身份鉴别”、“访问控制信息完整性”、“重要信息资源安全标记完整性”、“重要数据传输机密性”、“重要数据存储机密性”、“重要数据传输完整性”、“重要数据存储完整性”、“不可否认性”等应用和数据安全方面采取的密码保障措施进行各项测评，详细记录现场测评情况(如访谈记录、配置截图、抓包分析截图、产品照片等)，完成单项及单元测评结果判定。测评结果应由采购方配合人员确认。

标准要求内容：

采用密码技术对登录用户进行身份鉴别,保证应用系统用户身份的真实性。

采用密码技术保证信息系统应用的访问控制信息的完整性。

采用密码技术保证信息系统应用的重要信息资源安全标记的完整性。

采用密码技术保证信息系统应用的重要数据在传输过程中的机密性。

采用密码技术保证信息系统应用的重要数据在存储过程中的机密性。

采用密码技术保证信息系统应用的重要数据在传输过程中的完整性。

采用密码技术保证信息系统应用的重要数据在存储过程中的完整性。

在可能涉及法律责任认定的应用中,采用密码技术提供数据原发证据和数据接收证据,实现数据原发行为的不可否认性和数据接收行为的不可否认性。

3.5 密码应用管理要求

3.5.1 管理制度

针对“具备密码应用安全管理制度”“密钥管理规则”“建立操作规程”“定期修订安全管理制度”“明确管理制度发布流程”“制度执行过程记录留存”等制度方面采取的管理措施进行各项测评,详细记录现场测评情况，完成单项及单元测评果判定。测评结果应由采购方人员确认。

标准要求内容：

应具备密码应用安全管理制度,包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度。

应根据密码应用方案建立相应密钥管理规则。

应对管理人员或操作人员执行的日常管理操作建立操作规程。

应定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定,是否对存在不足或需要改进之处进行修订。

应明确相关密码应用安全管理制度和操作规程的发布流程并进行版本控制。

应具有密码应用操作规程的相关执行记录并妥善保存。

3.5.2 建设运行

针对“制定密码应用方案”、“制定密钥安全管理策略”、“制定实施方案”、“投入运行前进行密码应用安全性评估”、“定期开展密码应用安全性评估及攻防对抗演习”等建设方面采取的管理措施进行各项测评，详细记录现场测评情况，完成单项及单元测评结果判定。测评结果应由采购方配合人员确认。

标准要求内容：

应依据密码相关标准和密码应用需求,制定密码应用方案。

应根据密码应用方案,确定系统涉及的密钥种类、体系及其生存周期环节,各环节密钥管理要求照GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》附录B。

应按照应用方案实施建设。

投入运行前应进行密码应用安全性评估,评估通过后系统方可正式运行。

在运行过程中,应严格执行既定的密码应用安全管理制度,是否定期开展密码应用安全性评估及攻防对抗演习,并根据评估结果进行整改。

3.5.3 应急处置

针对“应急策略”、“事件处置”、“向有关主管部门上报处置情况”等应急方面采取的管理措施进行各项测评，详细记录现场测评情况，完成单项及单元测评结果判定。

测评结果应由采购方配合人员确认。

标准要求内容：

应制定密码应用应急策略,做好应急资源准备,当密码应用安全事件发生时,应立即启动应急处置措施,结合实际情况及时处置。

事件发生后,应及时向信息系统主管部门进行报告。

事件处置完成后,应及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况。

3.6 技术标准和规范

《中华人民共和国网络安全法》

《中华人民共和国密码法》

《信息安全技术计算机信息系统安全保护等级划分准则》GB 17859-1999

《信息安全技术信息系统密码应用基本要求》GB/T 39786-2021

《信息系统密码应用测评要求》GM/T 0115-2021

《信息系统密码应用测评过程指南》GM/T 0116-2021

《信息系统密码应用高风险判定指引》

《商用密码应用安全性评估量化评估规则》

注：以上涉及的相关标准及规范，若国家有最新出台的标准和规定，则按最新标准和规定执行。

★3.7 成果要求（实质性要求）

在项目完成后，供应商须提供以下文档资料：

《商用密码应用安全性评估基本情况调查表》

《商用密码应用安全性评估测评方案》

《商用密码应用安全性评估报告》

★三、商务要求

（一）服务时间和地点。

1.服务时间：网络安全等级保护测评服务：自合同签订后满足进场条件之日起3个月内出具《网络安全等级保护测评报告》；商用密码应用安全性评估服务：自合同签订后满足进场条件之日起3个月内出具《商用密码应用安全性评估报告》。

2.服务地点：采购人指定地点。

3.本项目合同期限：一招三年，合同一年一签。

（二）履约验收。

1.验收主体：采购人。

2.验收时间：服务项目达到验收标准并在成交供应商申请开展履约验收后15个工作日内进行验收。

3.验收组织方式：采购人自行组织。

4.验收程序：一次性验收。

5.内容和验收标准：严格按照《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》（财库〔2016〕205号）及政府采购相关法律法规的要求进行验收。存在国家强制规定或行业标准的遵照相关规定执行。

（三）其他要求。

1.供应商应保证本项目所提供的所有服务、成果不涉及侵犯任何第三方的专利权、商标权或著作权等。

2.供应商若成为成交供应商，须提供保密承诺书，承诺对项目实施过程中的数据保密，且制定针对本项目的保密制度，加强对实施人员的管理和培训。

（四）付款方式。

合同签订后15个工作日内，供应商向采购人出具合法有效完整的发票及凭证资料后，采购人支付合同总金额的50%；

		供应商完成密码应用和等级保护测评，出具正式测评报告，完成项目验收，供应商向采购人出具合法有效完整的发票及凭证资料后15个工作日内支付合同总金额的50%。

8、供应商一般资格要求

序号	资格要求名称	资格要求详细说明
1	具有独立承担民事责任的能力。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。
2	具有良好的商业信誉	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。
3	具有健全的财务会计制度。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。{如需提供其他材料，需代理机构手动填写具体要求并关联相应格式要求，以下是样例：供应商财务状况证明材料包括采购代理机构在采购文件中明确需要供应商提供的财务状况证明材料。如XXXX或XXXX年度经审计的财务报告（包含审计报告和审计报告中所涉及的财务报表和报表附注）；XXXX或XXXX年度供应商完整的全套财务报表（应当包括资产负债表、利润表、现金流量表、所有者权益变动表、附注）；截至采购文件（资格预审申请文件）提交截止之日前一年内银行出具的资信证明；供应商注册时间截至采购文件（资格预审申请文件）提交截止之日前不足一年的，也可提供在相关主管部门备案的公司章程等证明材料。供应商需在项目电子化交易系统中按要求上传相应证明文件并进行电子签章。}
4	具有履行合同所必需的设备和专业技术能力。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。
5	有依法缴纳税收和社会保障资金的良好记录。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。
6	参加政府采购活动前三年内，在经营活动中没有重大违法记录。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。
7	不存在与单位负责人为同一人或者存在直接控股、管理关系的其他供应商参与同一合同项下的政府采购活动的行为。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。

序号	资格要求名称	资格要求详细说明
8	不属于为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。

9、供应商特殊资格要求

序号	资格要求名称	资格要求详细说明
1	（1）供应商具备有效的《网络安全等级测评与检测评估机构服务认证证书》。（2）供应商应是国家密码管理局公告（第42号）《商用密码应用安全性评估试点机构目录》中的单位。	（1）供应商具备有效的《网络安全等级测评与检测评估机构服务认证证书》。（2）供应商应是国家密码管理局公告（第42号）《商用密码应用安全性评估试点机构目录》中的单位。

10、分包的评审条款

评审项编号	一级评审项	二级评审项	详细要求	分值	客观评审项
1	详细评审	技术方案	1、供应商方案完全响应项目需求（包括测评指标、被测系统网络拓扑及资产清单、被测系统密码应用现状分析、风险告知及规避对策、人员安排及时间进度安排等五个方面）。方案齐全且无缺陷得10分，每项中每有一处缺陷扣1分，每缺少一项内容扣2分，扣完为止。 2、针对本项目提供的安全技术测评方案（包括安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心等五个方面）。方案齐全且无缺陷得10分，每项中每有一处缺陷扣1分，每缺少一项内容扣2分，扣完为止。 3、针对本项目提供的安全管理测评方案（包括安全管理制度、安全管理机构、安全管理人员、安全系统建设和安全系统运维管理等五个方面）。方案齐全且无缺陷得10分，每项中每有一处缺陷扣1分，每缺少一项内容扣2分，扣完为止。 注： 缺陷指：方案内容与项目实际情况不符或相对应评分标准不符、套用其他项目方案或存在明显与本项目无关的文字内容、内容前后矛盾或存在逻辑错误或表述错误或科学原理错误或涉及的规范及标准错误、存在不可能实现的情形等任意一种情形。	30.00	是
2	详细评审	实施能力	1、供应商具有密码算法验证工具系统软件著作权得2.5分； 2、供应商具有网络安全等保测评信息管理系统软件著作权得2.5分； 3、供应商具有网络安全密码测评数据分析系统软件著作权得2.5分。 4、供应商拥有网络安全漏洞扫描安全系统软件著作权得2.5分。 注：软件著作权提供中华人民共和国国家版权局颁发的著作权登记证书复印件并加盖公章。	10.00	是
3	详细评审	报价	满足招标文件要求且最终报价最低的报价为评审基准价，其价格分为满分。其他申请人的价格分统一按照下列公式计算： 报价得分=（评审基准价/最终报价）×10。	10.00	是

评审项编号	一级评审项	二级评审项	详细要求	分值	客观评审项
4	详细评审	质量体系	1. 供应商通过质量体系认证证书，且认证范围包括“信息安全等级保护测试评估服务、商用密码应用安全性评估”得2分； 2. 供应商通过信息安全管理系统认证证书，且认证范围包括“信息安全等级保护测试评估服务、商用密码应用安全性评估”得2分； 3. 供应商通过环境管理体系认证证书且认证范围包括“信息安全等级保护测试评估服务、商用密码应用安全性评估”得2分； 4. 供应商通过职业健康安全管理系统认证证书，且认证范围包括“信息安全等级保护测试评估服务、商用密码应用安全性评估”得2分； 5、供应商具有信息安全服务资质认证证书信息安全应急处理得2分。 注：资质或资格证书复印件加盖投标人公章	10.00	是
5	详细评审	履约经验	供应商自2021年1月1日至今每有一个密码测评相关案例2分，每增加一个加2分，最多得6分。 供应商自2021年1月1日至今每有一个等保测评相关案例2分，每增加一个加2分，最多得6分。 注：提供相关合同复印件或授权书加盖投标人公章。	12.00	是
6	详细评审	项目总测评师	项目总测评师同时具有网络安全等级测评师（高级）证书和商用密码应用安全性评估人员能力合格证书的情况下，具有以下证书： 1.互联网安全评估师高级证书（CIISA）得1分； 2.计算机技术与软件专业资格信息安全工程师（软考类）得1分； 3.注册数据安全治理工程师（高级）得1分 4.系统架构师（高级）得1分； 5.注册渗透测试工程师（CISP-PTE）得1分 6.网络安全管理（I级）得1分； 此项最多6分，每少提供一个证书扣1分。 注： (1)、提供相关人员证书复印件加盖供应商鲜章。 (2)、提供任职供应商单位的有效的在职证明材料（如社保缴纳证明或工资流水或劳动合同等任意一种。）	6.00	是
7	详细评审	项目经理	项目经理同时具有网络安全等级测评师证书和商用密码应用安全性评估人员能力优秀证书的情况下，具有以下证书： 1.网络安全技术（I级）证书得1分； 2.具有市级人力资源和社会保障局颁发的网络安全服务高级工程师职称证书得1分； 3.网络信息安全工程师得1分； 4.电子技术工程师职称证书得1分； 5.信息安全保障人员认证证书，认证范围：风险管理（专业级）得1分； 6、计算机技术与软件专业资格信息系统项目管理师证书得1分； 全部满足6分，缺少一项扣1分。 注： (1)、提供相关人员证书复印件加盖供应商鲜章。 (2)、提供任职供应商单位的有效的在职证明材料（如社保缴纳证明或工资流水或劳动合同等任意一种。） (3)、拟派项目总测评师与项目经理不得兼任； (4)、其余测评人员，同一人拥有多个证书的以最高单项计分，不累加得分。	6.00	是
8	详细评审	测评人员	其余测评人员具有： 1.互联网安全评估师证书（CIISA）得2分； 2.商用密码应用安全性评估人员能力合格证书得2分； 3.注册渗透测试专家（CISP-PTS）得2分； 4.中华人民共和国人力资源和社会保障部及工业和信息化部颁发的系统集成项目管理工程师证书得2分； 5.注册信息安全专业人员证书（CISP）得2分； 6.注册渗透测试工程师（CISP-PTE）得2分； 7.具有市级人力资源和社会保障局颁发的网络安全服务高级工程师职称证书得2分； 8.数据安全官（DSO）得2分； 全部提供得16分，每少提供一个证书扣2分。 注： (1)、提供相关人员证书复印件加盖供应商鲜章。 (2)、提供任职供应商单位的有效的在职证明材料（如社保缴纳证明或工资流水或劳动合同等任意一种。）	16.00	是

11、合同管理安排

1）合同类型：买卖合同

2）合同定价方式：固定单价

3）合同履行期限：365

4）合同履约地点：采购人指定地点

5）支付方式：分期付款

6）履约保证金及缴纳形式：

中标/成交供应商是否需要缴纳履约保证金：否

7）质量保证金及缴纳形式：

中标/成交供应商是否需要缴纳质量保证金：否

8）合同支付约定：

1、 付款条件说明： 供应商向采购人出具合法有效完整的发票及凭证资料后 ， 达到付款条件起 15 日内，支付合同总金额的 50.00%。

2、 付款条件说明： 供应商完成密码应用和等级保护测评，出具正式测评报告，完成项目验收，供应商向采购人出具合法有效完整的发票及凭证资料后 ， 达到付款条件起 15 日内，支付合同总金额的 50.00%。

9）验收交付标准和方法：严格按照《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》（财库〔2016〕205号）及政府采购相关法律法规的要求进行验收。存在国家强制规定或行业标准的遵照相关规定执行。

10）质量保修范围和保修期：合同约定

11）知识产权归属和处理方式：合同约定

12）成本补偿和风险分担约定：合同约定

13）违约责任与解决争议的方法：合同约定

14）合同其他条款：无

12、履约验收方案

1）验收组织方式：自行验收

2）是否邀请本项目的其他供应商：否

3）是否邀请专家：否

4）是否邀请服务对象：否

5）是否邀请第三方检测机构：否

6）履约验收程序：一次性验收

7）履约验收时间：

供应商提出验收申请之日起15日内组织验收

8）验收组织的其他事项：合同约定

9）技术履约验收内容：合同约定

10）商务履约验收内容：合同约定

11）履约验收标准：合同约定

12）履约验收其他事项：合同约定

五、风险控制措施和替代方案

该采购项目按照《政府采购需求管理办法》第二十五条规定，本项目是否需要组织风险判断、提出处置措施和替代方案：否