陕西省医疗保障信息平台运维服务项目网络安全等级保护测评服务及商用密码应用安全性评估服务采购需求

采购包1：陕西省医疗保障信息平台运维服务项目网络安全等级保护测评服务

服务范围：陕西省医疗保障信息平台采用国家医疗保障局统一的技术架构和应用框架进行建设，整体采取分布式+云平台的技术路线，通过租赁数据中心机房并自建医保云的方式进行建设，实现了全省医保信息系统的省级集中。

本项目根据国家《中华人民共和国网络安全法》《信息安全等级保护管理办法》（公通字〔2007〕43号）《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安〔2010〕303号）《陕西省信息安全等级保护安全建设整改工作指导意见》（陕等保办〔2011〕2号）等相关文件要求，对陕西省医疗保障信息平台核心经办业务管理子系统等8个信息系统开展等级保护测评，系统清单见下表：

序号	系统名称	等级保护级别
1	核心经办业务管理子系统	三级
2	公共服务子系统	三级
3	药品和医用耗材招采管理子系统	三级
4	应用支撑子系统	三级
5	宏观决策管理子系统	三级
6	智能监管子系统	三级
7	陕西省医疗保障信息平台云平台（核心业务区）	三级
8	陕西省医疗保障信息平台云平台（公共服务区）	三级

服务内容：1.本次测评工作主要针对陕西省医疗保障信息平台的8个定级对象完成等级保护测评。要求具有相关资质的机构在服务周期内提供评估测评服务，并出具测评报告、协助用户单位进行整改，直到8个定级对象全部完成等级保护测评工作，并出具测评通过报告。

2. 鉴于医保信息系统的复杂性，要求供应商针对本次测评工作的信息系统按照采购人实际需要进行至少1次的安全复测，并出具检测报告。针对陕西省医疗保障信息平台本次服务周期内新上线的信息系统提供安全服务等工作，并出具相关报告。

3. 重保及节假日期间，供应商应协助采购人做好信息安全检查及防护工作，包括但不限于漏扫、渗透等。

4. 协助采购人组织开展应急演练等工作，包括但不限于出具演练方案、应急预案等。

5. 整理及汇编本项目文档资料并协助采购人完善平台安全相关制度。

具体内容详见3.2.2服务要求

2.采购包2：陕西省医疗保障信息平台运维服务项目商用密码应用安全性评估服务

服务范围：陕西省医疗保障信息平台采用国家医疗保障局统一的技术架构和应用框架进行建设，整体采取分布式+云平台的技术路线，通过租赁数据中心机房并自建医保云的方式进行建设，实现了全省医保信息系统的省级集中。

本项目是对医保信息平台开展商用密码应用安全性评估服务，本项目商用密码应用安全性评估对象主要包含：

序号	系统名称
1	核心经办业务管理子系统
2	公共服务子系统
3	药品和医用耗材招采管理子系统
4	应用支撑子系统
5	宏观决策管理子系统
6	智能监管子系统
7	陕西省医疗保障信息平台云平台（核心业务区）
8	陕西省医疗保障信息平台云平台（公共服务区）

服务内容：

1. 本次测评工作主要针对陕西省医疗保障信息平台的8个定级对象完成商用密码应用安全性评估。要求具有相关资质的机构在服务周期内提供评估测评服务，并出具测评报告、协助用户单位进行整改，直到8个定级对象全部完成商用密码应用安全性评估测评工作，并出具测评通过报告。

2. 供应商应针对本次测评工作的信息系统根据采购人实际需求进行至少1次的安全复测，并出具检测报告。供应商应针对陕西省医疗保障局本次服务周期内新上线的信息系统不定期协同系统建设单位修订密码应用方案。

3. 协助采购人组织开展应急演练等工作，包括但不限于出具演练方案、应急预案等。

4. 整理及汇编本项目文档资料并协助采购人完善平台安全相关制度。

1 等级保护测评方案

1.1等级测评工作目的

等级测评是测评机构依据国家信息安全等级保护制度规定，按照有关管理规范和技术标准，对非涉及国家秘密信息系统安全等级保护状况进行检测评估的活动。是信息安全等级保护工作的重要环节。

通过开展等级测评，一是掌握信息系统安全状况、排查系统安全隐患和薄弱环节、明确信息系统安全建设整改需求；二是能够衡量出信息系统安全保护措施是否符合等级保护基本要求，是否具备了相应等级的安全保护能力。等级测评结果也是公安机关等安全监管部门进行监督、检查、指导的参照。

1.2开展等级测评的时机

（一）安全建设整改前

在开展信息系统安全建设整改前，信息系统运行使用单位可以通过等级测评（此时称为安全现状测评）分析判断目前信息系统所采取的安全措施与等级保护标准要求之间的差距，分析安全方面存在的问题，查找信息系统安全保护建设整改需要解决的问题，形成安全建设整改的安全需求。

（二）安全建设整改后

信息系统安全建设整改完成后，信息系统运行使用单位应通过等级测评对信息系统的等级保护措施落实情况与《基本要求》的要求之间的符合程度进行评判，形成信息系统安全等级测评报告。如果发现问题将继续整改。

（三）定期开展等级测评

信息系统运行维护期间，应定期进行安全等级测评，及时发现和分析信息系统存在的安全问题。《管理办法》要求信息系统建设完成后，运营使用单位应当选择符合规定条件的测评机构，依据《测评要求》等技术标准，定期对信息系统安全等级状况开展等级测评。第三级以上信息系统应当每年至少进行一次等级测评，对于重要部门的第二级信息系统，可参照上述要求开展等级测评工作。

1.3测评依据

测评过程中主要依据的标准：

1、GB/T 22239-2019：《信息安全技术 网络安全等级保护基本要求》

2、GB/T 28448-2019：《信息安全技术 网络安全等级保护测评要求》

3、GB／T 28449-2018：《信息安全技术 网络安全等级保护测评过程指南》

1.4测评范围

等级测评的测评对象种类上基本覆盖、数量进行抽样，重点抽查主要的设备、设施、人员和文档等。等级测评的测评对象在抽样时主要考虑以下几个方面：

1)主机房（包括其环境、设备和设施等）和部分辅机房，应将放置了服务于定级对象的局部（包括整体）或对定级对象的局部（包括整体）安全性起重要作用的设备、设施的辅机房选取作为测评对象；存储被测定级对象重要数据的介质的存放环境；

2)办公场地；

3)整个系统的网络拓扑结构；

4)安全设备，包括防火墙、入侵检测设备和防病毒网关等；

5)边界网络设备（可能会包含安全设备），包括路由器、防火墙、认证网

6)和边界接入设备（如楼层交换机）等；

7)对整个定级对象或其局部的安全性起作用的网络互联设备，如核心交换机、汇聚层交换机、路由器等；

8)承载被测定级对象主要业务或数据的服务器（包括其操作系统和数据库）；

9)管理终端和主要业务应用系统终端；

10)能够完成被测定级对象不同业务使命的业务应用系统；

11)业务备份系统；

12)信息安全主管人员、各方面的负责人员、具体负责安全管理的当事人、业务负责人；

13)涉及到定级对象安全的所有管理制度和记录。

1.5测评方法

本次等级测评的主要方式有：访谈、核查和测试及综合风险分析。

（一）访谈

访谈是指测评人员通过引导信息系统相关人员进行有目的的（有针对性的）交流以帮助测评人员理解、澄清或取得证据的过程。使用访谈方法进行测试的目的是为了了解信息系统的全局性、方向/策略性和过程性信息，一般不涉及具体的实现细节和技术措施。访谈主要应用于安全管理类测评、评测中获取证据，在安全技术测评、评测方面访谈主要用于收集目标系统的信息以辅助后续的检查或者测试。

访谈对象：主要包括信息安全主管、信息系统安全管理员、系统管理员、网络管理员、资产管理员等。

工具：管理核查表（checklist）。

（二）核查

核查是指测评人员通过对测评对象进行观察、查验、分析等活动，获取证据以证明信息系统安全保护措施是否有效的一种方法。使用检查方法进行测评、评测的目的是确认信息系

统当前的、具体的安全机制以及运行的配置和实现情况是否符合要求。核查方法的应用范围覆盖了安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心等方面的安全技术测评以及安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理等方面的安全管理测评。

检查对象：主要包括设备及其配置机制、运行实现，文档，机房，存储介质等。

核查可细分为文档审查、实地察看和配置核查等几种具体方法。

1）文档审查

a)核查GB/T22239中规定的制度、策略、操作规程等文档是否齐备。

b)核查是否有完整的制度执行情况记录,如机房出入登记记录、电子记录、高等级系统的关键设备的使用登记记录等。

c)核查安全策略以及技术相关文档是否明确说明相关技术要求实现方式。

d)对上述文档进行审核与分析,核查他们的完整性和这些文件之间的内部一致性。

2）实地察看（现场查看）

根据被测定级对象的实际情况,测评人员到系统运行现场通过实地的观察人员行为、技术设施和物理环境状况判断人员的安全意识、业务操作、管理程序和系统物理环境等方面的安全情况,测评其是否符合相应等级的安全要求。

3）配置核查

a)根据测评结果记录表格内容,利用上机验证的方式核查应用系统、主机系统、数据库系统以及各设备的配置是否正确,是否与文档、相关设备和部件保持一致,对文档审核的内容进行核实(包括日志审计等)。

b)如果系统在输入无效命令时不能完成其功能,应测试其是否对无效命令进行错误处理。

c)针对网络连接,应对连接规则进行验证。

（三）测试

测试是指测评人员使用预定的方法/工具使测评对象产生特定行为，通过查看、分析这些行为的结果，获取证据以证明信息系统安全保护措施是否有效的一种方法。测试方法的目的是验证信息系统当前的、具体的安全机制及运行的配置和实现情况的有效性或安全强度。

测试主要包括手工验证、漏洞扫描、渗透测试。

漏洞扫描，主要用于识别网络、操作系统、数据库系统的脆弱性，发现软件和硬件中已知的弱点，如非法账号、弱口令、权限配置错误、系统补丁、文件目录及文件系统安全、不必要的端口和服务等，以决定系统是否易受到已知攻击的影响。

渗透测试主要用于对信息系统漏洞进行深度探测，从攻击者角度，发现系统及网关入口设备存在的安全隐患；发现逻辑性更强、更深层次的漏洞，并直观反映漏洞的潜在危害；检验当前安全控制措施的有效性；检测对外提供服务的业务系统的威胁防御能力。

1.6测评内容

按照《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）、《关于信息安全等级保护工作的实施意见》（公通字[2004]66 号）、《信息安全等级保护管理办法》（公通字[2007]43 号）、《信息安全技术 信息系统安全等级保护基本要求》、《计算机信息系统安全保护等级划分准则》、《信息系统安全等级保护基本要求》（GB/T 22239-2019）、《信息系统安全等级保护定级指南》（GB/T 22240-2020）、《信息系统安全等级保护实施指南》（GB/T 25058-2010）、《信息系统安全等级保护测评要求》（GB/T 28448-2019）、《信息系统安全等级保护测评过程指南》（GB/T 28449-2018）、《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）开展等级保护测评服务，三级系统测评项目不少于211项。

安全等级保护测评包括以下内容：

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、安全管理中心等五个方面的安全测评；

安全管理测评：包括安全管理机构、安全管理制度、安全管理人员、系统建设管理和系统运维管理等五个方面的安全测评。

1.6.1安全通用要求指标

安全要求类	层面	三级测试项
技术要求	安全物理环境	22
	安全通信网络	8
	安全区域边界	20
	安全计算环境	34
	安全管理中心	12
管理要求	安全管理制度	7
	安全管理机构	14
	安全管理人员	12
	安全建设管理	34
	安全运维管理	48
合　计	10	211

1.6.1.1安全通用要求三级系统测评项

安全通用要求-安全物理环境	
测评控制点名称	三级测评点
物理位置选择	2
物理访问控制	1
防盗窃和防破坏	3
防雷击	2
防火	3
防水和防潮	3
防静电	2
温湿度控制	1

安全通用要求-安全物理环境	
电力供应	3
电磁防护	2

安全通用要求-安全通信网络	
测评组件名称	三级测评点
网络架构	5
通信传输	2
可信验证	1

安全通用要求-安全区域边界	
测评组件名称	三级测评点
边界防护	4
访问控制	5
入侵防范	4
恶意代码和垃圾邮件防范	2
安全审计	4
可信验证	1

安全通用要求-安全计算环境	
测评组件名称	三级测评点
身份鉴别	4
访问控制	7
安全审计	4
入侵防范	6
恶意代码防范	1
可信验证	1
数据完整性	2
数据保密性	2
数据备份恢复	3
剩余信息保护	2
个人信息保护	2

安全通用要求-安全管理中心	
测评组件名称	三级测评点
系统管理	2
审计管理	2
安全管理	2
集中管控	6

安全通用要求-安全管理制度	
测评组件名称	三级测评点
安全策略	1
管理制度	3
制定和发布	2
评审和修订	1

安全通用要求-安全管理机构	
测评组件名称	三级测评点
岗位设置	3
人员配备	2
授权和审批	3
沟通和合作	3
审核和检查	3

安全通用要求-安全管理人员	
测评组件名称	三级测评点
人员录用	3
人员离岗	2
安全意识教育和培训	3
外部人员访问管理	4

安全通用要求-安全建设管理	
测评组件名称	三级测评点
定级和备案	4
安全方案设计	3
产品采购和使用	3
自行软件开发	7
外包软件开发	3
工程实施	3
测试验收	2
系统交付	3
等级测评	3
服务供应商选择	3

安全通用要求-安全运维管理	
测评组件名称	三级测评点
环境管理	3
资产管理	3
介质管理	2
设备维护管理	4
漏洞和风险管理	2
网络和系统安全管理	10
恶意代码防范管理	2
配置管理	2
密码管理	2
变更管理	3
备份与恢复管理	3
安全事件处置	4
应急预案管理	4
外包运维管理	4

1.6.1.2安全通用要求三级系统测评内容

（一）安全物理环境

安全物理环境测评实施过程涉及10个方面的安全保护能力，具体测评指标描述如下表所示：

表1安全物理环境测评指标描述

序号	安全子类	测评指标描述
1	物理位置选择	通过访谈物理安全负责人，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	通过访谈物理安全负责人，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	通过访谈物理安全负责人，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	通过访谈物理安全负责人，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	通过访谈物理安全负责人，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	通过访谈物理安全负责人，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	通过访谈物理安全负责人，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	通过访谈物理安全负责人，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	通过访谈物理安全负责人，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	通过访谈物理安全负责人，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。

（二）安全通信网络测评

安全通信网络测评实施过程涉及3个方面的安全保护能力，具体测评指标描述如下表所示：

表2安全通信网络测评指标描述

序号	安全子类	测评指标描述
1	网络架构	测评分析网络架构与网段划分、隔离等情况的合理性和有效性。
2	通信传输	测评通信过程中的完整性、保密性等。
3	可信验证	基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等 进行可信验证，并在应用程序的关键执行环节进行动态可信验证。

（三）安全区域边界测评

安全区域边界测评主要涉及边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证6个方面的安全保护能力，具体测评指标描述如下表所示：

表3安全区域边界测评指标描述

序号	安全子类	测评指标描述
1	边界防护	测评分析信息系统网络边界安全防护的状况。
2	访问控制	测评分析信息系统对网络区域边界相关的网络隔离与访问控制能力。
3	入侵防范	测评分析信息系统对攻击行为的识别和处理情况。
4	恶意代码和垃圾邮件防范	测评分析信息系统网络边界和核心网段对病毒等恶意代码及垃圾邮件的防护情况。
5	安全审计	测评分析信息系统审计配置和审计记录保护情况。
6	可信验证	基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等 进行可信验证，并在应用程序的关键执行环节进行动态可信验证。

（四）安全计算环境测评

安全计算环境测评主要涉及身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护11个方面的安全保护能力，具体测评指标描述如下表所示：

表4安全计算环境测评指标描述

序号	安全子类	测评指标描述
1	身份鉴别	检查服务器的身份标识与鉴别和用户登录的配置情况。
2	访问控制	检查服务器的访问控制设置情况，包括安全策略覆盖、控制粒度以及权限设置情况等。
3	安全审计	检查服务器的安全审计的配置情况，如覆盖范围、记录的项目和内容等；检查安全审计进程和记录的保护情况。
4	入侵防范	检查服务器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	检查服务器的恶意代码防范情况，如服务器是否安装统一管理的恶意代码防范软件，是否及时升级病毒库等。
6	可信验证	基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等 进行可信验证，并在应用程序的关键执行环节进行动态可信验证。
7	数据完整性	测评操作系统、数据库管理系统的管理数据、鉴别信息和用户数据在传输和保存过程中的完整性保护情况。
8	数据保密性	测评操作系统和数据库管理系统的管理数据、鉴别信息和用户数据在传输和保存过程中的保密性保护情况。
9	数据备份恢复	测评信息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	测评鉴别信息所在的存储空间被释放或重新分配前是否得到完全清除。
11	个人信息保护	测评是否仅采集和保存业务必需的用户个人信息；是否禁止未授权访问和使用用户个人信息。

（五）安全管理中心测评

安全管理中心测评主要涉及系统管理、审计管理、安全管理、集中管控4个方面的安全保护能力，具体测评指标描述如下表所示：

表5安全管理中心测评指标描述

序号	安全子类	测评指标描述
1	系统管理	测评信息系统的系统管理员对系统的管理情况。
2	审计管理	测评信息系统的安全审计员对系统的审计情况。
3	安全管理	测评信息系统的安全管理员对系统的安全策略的配置情况。
4	集中管控	测评网络链路、安全设备、网络设备和服务器等设备的运行状况的集中监测、分析、报警等。

（六）安全管理制度测评

安全管理制度测评主要涉及安全策略、管理制度、制定和发布、评审和修订4个方面的安全保护能力，具体测评指标描述如下表所示：

表6安全管理制度测评指标描述

序号	安全子类	测评指标描述
1	安全策略	测评信息安全工作的总体方针、安全策略，总体目标、范围、原则和安全框架等。
2	管理制度	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	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	测评信息系统管理制度定期评审和修订情况。

（七）安全管理机构测评

安全管理制度测评主要涉及岗位设置、人员配备、授权和审批、沟通和合作、审核和检查5个方面的安全保护能力，具体测评指标描述如下表所示：

表7安全管理机构测评指标描述

序号	安全子类	测评指标描述
1	岗位设置	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	测评信息系统各个岗位人员配备情况。
3	授权和审批	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	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	审核和检查	检查信息系统安全工作的审核和测评情况。

（八）安全管理人员测评

安全管理人员测评主要涉及人员录用、人员离岗、安全意识教育和培训、外部人员访问管理4个方面的安全保护能力，具体测评指标描述如下表所示：

表8安全管理人员测评指标描述

序号	安全子类	测评指标描述

序号	安全子类	测评指标描述
1	人员录用	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	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	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	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。

（九）安全建设管理测评

安全建设管理测评主要涉及定级和备案、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、等级测评、服务供应商选择10个方面的安全保护能力，具体测评指标描述如下表所示：

表9安全建设管理测评指标描述

序号	安全子类	测评指标描述
1	定级和备案	测评是否按照一定要求确定系统的安全等级并完成备案工作。
2	安全方案设计	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	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	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	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	测评系统运行前是否对其进行测试验收工作。
8	系统交付	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	测评是否依据国家要求完成等级测评和整改工作。
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。

（十）安全运维管理测评

安全管理人员测评主要涉及环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理、外包运维管理14个方面的安全保护能力，具体测评指标描述如下表所示：

表10安全运维管理测评指标描述

序号	安全子类	测评指标描述
1	环境管理	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。

序号	安全子类	测评指标描述
2	资产管理	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	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	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	测评是否采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补。测评是否定期开展安全测评。
6	网络和系统安全管理	测评是否采取必要的措施对网络和系统的安全配置、系统账户、漏洞扫描和审计日志等方面进行有效的管理。
7	恶意代码防范管理	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	测评是否记录和保存系统的基本配置信息
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	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	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	安全事件处置	测评是否采取必要的措施对安全事件进行等级划分和对安全事件的报告、处理过程进行有效的管理。
13	应急预案管理	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	测评外包运维服务商的选择是否符合国家的有关规定并签订相关协议。

1.6.2云计算安全扩展要求指标

安全要求类	层　面	三级测试项
技术要求	安全物理环境	1
	安全通信网络	5
	安全区域边界	8
	安全计算环境	19
	安全管理中心	4
管理要求	安全建设管理	8
	安全运维管理	1
合　计	7	46

1.6.2.1云计算安全扩展要求三级系统测评项

云计算安全扩展要求-安全物理环境

云计算安全扩展要求-安全物理环境	
测评组件名称	三级测评点
基础设施位置	1

云计算安全扩展要求-安全通信网络	
测评组件名称	三级测评点
网络架构	5

云计算安全扩展要求-安全区域边界	
测评组件名称	三级测评点
访问控制	2
入侵防范	4
安全审计	2

云计算安全扩展要求-安全计算环境	
测评组件名称	三级测评点
身份鉴别	1
访问控制	2
入侵防范	3
镜像和快照保护	3
数据完整性和保密性	4
数据备份恢复	4
剩余信息保护	2

云计算安全扩展要求-安全管理中心	
测评组件名称	三级测评点
集中管控	4

云计算安全扩展要求-安全建设管理	
测评组件名称	三级测评点
云服务商选择	5
供应链管理	3

云计算安全扩展要求-安全运维管理	
测评组件名称	三级测评点
云计算环境管理	1

1.6.2.2云计算安全扩展要求三级系统测评内容

（一）安全物理环境

安全物理环境测评主要关注基础设施位置,具体测评指标描述如下表所示:

表11安全物理环境测评指标描述

序号	安全子类	测评指标描述
1	基础设施位置	查看云计算基础设施是否处于中国境内。

（二）安全通信网络

安全通信网络测评主要关注网络架构,具体测评指标描述如下表所示:

表12安全通信网络测评指标描述

序号	安全子类	测评指标描述
1	网络架构	测评分析网络架构与隔离等情况的合理性和有效性，测评拓扑图与实际运行情况的一致性，网络结构是否具备灵活性。

（三）安全区域边界

安全区域边界测评主要关注访问控制、入侵防范、安全审计,具体测评指标描述如下表所示:

表13安全区域边界测评指标描述

序号	安全子类	测评指标描述
1	访问控制	测评分析云租户内部网络区域边界相关的网络隔离与访问控制能力。
2	入侵防范	测评分析对外攻击和有害信息发布的检测、告警能力。
3	安全审计	测评分析云租户与云服务商的职责划分，并依此测评审计信息的完整性和可用性。

（四）安全计算环境

安全计算环境测评主要关注身份鉴别、访问控制、入侵防范、镜像和快照保护、数据完整性和保密性、数据备份和恢复、剩余信息保护,具体测评指标描述如下表所示:

表14安全计算环境测评指标描述

序号	安全子类	测评指标描述
1	身份鉴别	测评虚拟机、数据系统、网络设备和安全设备的身份鉴别能力。包括口令安全策略、身份鉴别机制等。
2	访问控制	测评虚拟机、数据库系统、网络设备和安全设备的访问控制设置情况，包括安全策略、控制粒度以及权限设置情况等。
3	入侵防范	测评分析对虚拟机在运行过程中的隔离失效、异常访问的检测、告警能力，对虚拟机的迁移范围进行限制。

序号	安全子类	测评指标描述
4	镜像和快照保护	测评虚拟机镜像和快照完整性、保密性和安全性。
5	数据完整性和保密性	测评虚拟机迁移过程的鉴别信息和用户数据在传输过程中的完整性保护情况。
6	数据备份和恢复	测评云租户重要数据的本地备份、存储位置，应用系统的可移植性等。
7	剩余信息保护	测评虚拟机的存储空间，被释放或再分配给其他用户前得到完全清除。

（五）安全管理中心

安全管理中心测评主要关注集中管控,具体测评指标描述如下表所示:

表15安全管理中心测评指标描述

序号	安全子类	测评指标描述
1	集中管控	测评网络链路、安全设备、网络设备和服务器等设备的运行状况的集中监测、分析、报警等。

（六）安全建设管理

安全建设管理测评主要关注云服务商选择、供应链选择,具体测评指标描述如下表所示:

表16安全建设管理测评指标描述

序号	安全子类	测评指标描述
1	云服务商选择	测评是否选择符合有关规定的云服务商。
2	供应链选择	测评供应链安全事件信息、重要变更或威胁信息是否及时传达到云租户。

（七）安全运维管理

安全建设运维管理测评主要关注云计算环境管理,具体测评指标描述如下表所示:

表17安全运维管理测评指标描述

序号	安全子类	测评指标描述
1	云计算环境管理	云计算平台的运维地点位于中国境内,境外对境内云计算平台实施运维操作应遵循国家有关规定。

1.6.3渗透测试

渗透测试主要依据CVE（Common Vulnerabilities & Exposures公共漏洞和暴露）已经发现的安全漏洞，以及隐患漏洞，模拟黑客入侵者的攻击方法对服务器和网络设备进行非破坏性质的攻击性测试。了解当前系统的安全性、了解攻击者可能利用的途径。它能够直观的让管理人员知道当前网络存在的安全弱点以及可能造成的影响，以便采取必要的防范措施。渗透测试不只是要模拟外部黑客的入侵，同时，防止内部人员的有意识（无意识）攻击也是很有必要的。

渗透测试包括但不限于以下测试内容：

（1）SQL注入：就是通过把SQL命令插入到Web表单提交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的SQL命令。

（2）跨站脚本攻击：通过在留言板或者查询页面中插入XSS语句，来欺骗用户进行点击，从而将恶意代码执行到用户端或管理端。

（3）任意文件下载、上传、删除：通过控制系统的文件上传、下载、删除功能，来执行上传、下载、删除的功能，如果该功能过滤不严，可导致攻击者可以直接上传恶意文件、下载敏感信息、删除系统页面。

（4）文件包含：文件包含漏洞的产生原因是在通过文件的函数引入文件时，由于传入的文件名没有经过合理的校验，从而操作了预想之外的文件，就可能导致意外的文件泄露甚至恶意的代码注入。

（5）逻辑错误：是指程序员在编写代码时，代码顺序或编写不规范，导致的各种逻辑错误。

（6）命令执行：是指针对采用struts2框架的网站，2010年7月9日至2014年4月23日爆发的struts远程命令执行漏洞进行测试。

（7）越权访问：是指越过某个账户本身具有的权限，去访问管理员信息或者其他本权限不能访问的数据或内容。

（8）敏感信息泄露：是指通过漏洞或者其他逻辑错误，获取系统的数据库信息、人员、金额、地址、账户密码等信息。

1.6.4漏洞扫描

利用漏洞扫描测试工具，我们不仅可以直接获取到目标系统本身存在的系统、应用等方面的漏洞，同时，也可以通过在不同区域接入测试工具所得到的测试结果，判定不同区域间的访问控制情况。利用工具测试，结合其他核查手段，可以为测试结果的客观和准确提供保证。针对漏洞扫描发现的系统漏洞，需被测评单位及时修复，避免系统漏洞被非授权人员利用，对信息系统安全性产生影响。

1.7等级保护测评安全性评估要求

1.7.1处理机制要求

1.7.1.1等级保护测评服务处理机制要求

应按照国家相关要求，从“定级-备案-等级测评-安全建设整改-配合监督检查”5个环节配合采购单位做好等级保护工作。其中针对等级测评工作过程，依据《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）和《信息安全技术网络安全等级保护测评过程指南》（GB/T28449-2018）等国家关于信息系统安全等级保护的相关标准和规范要求，要求参选人严格按照下列流程开展工作：

测评准备阶段：是开展等级测评工作的前提和基础，是整个等级测评过程有效性的保证。测评准备工作是否充分直接关系到后续工作能否顺利开展。本活动的主要任务是掌握被测系统的详细情况，准备测试工具，为编制测评方案做好准备。

方案编制阶段：是开展等级测评工作的关键活动，为现场测评提供最基本的文档和指导方案。本活动的主要任务是确定与被测信息系统相适应的测评对象、测评指标及测评内容等，并根据需要重用或开发测评指导书，形成测评方案。

现场测评阶段：是开展等级测评工作的核心活动。本活动的主要任务是按照测评方案的总体要求，严格按照测评指导书执行，分步实施所有测评项目，以了解系统的真实保护情况，获取足够证据，发现系统存在的安全问题。

分析与报告编制阶段：是给出等级测评工作结果的活动，是总结被测系统整体安全保护能力的综合评价活动。本活动的主要任务是根据现场测评结果和《信息安全技术网络安全等级保护实施指南》的有关要求，通过单项测评结果判定、单元测评结果判定、整体测评和风险分析等方法，找出整个系统的安全保护现状与相应等级的保护要求之间的差距，并分析这些差距导致被测系统面临的风险，从而给出等级测评结论，形成《XXX系统网络安全等级保护测评报告》文本。

建设整改咨询阶段：建设整改咨询工作以等级测评发现的安全问题为工作重点，以及测评报告中安全建设整改建议；将信息系统的安全建设整改需求落实到可操作的安全技术和管理上，提出能够实现的技术参数或制度及其具体规范。并依据测评报告中安全建设整改建议开展建设整改工作时，服务商将提供建设整改过程中的与建设整改相关的咨询服务。

1.7.2人员配置要求

为保证本项目测评工作质量及进度要求，项目组要求至少配备5名测评人员。项目经理要求至少为高级测评师，具备丰富的项目实施经验和技术能力；项目组成员（不包含项目经理）至少1名高级测评师和3名中级及以上测评师。

1.7.3其他要求

供应商须完全满足业主对本项目的所有要求及技术参数。

采购包2：

供应商报价不允许超过标的金额

（招单价的）供应商报价不允许超过标的单价

标的名称：陕西省医疗保障信息平台运维服务项目商用密码应用安全性评估服务

2.商用密码安全性评估方案

2.1商用密码安全性评估工作目的

商用密码应用安全性评估的主要工作内容包括总体测评、密码技术应用测评、密钥管理测评、安全管理测评等。依据前述标准、要求、过程指南及作业指导书，对被测系统进行全

面系统评估，及时发现系统脆弱性，识别变化的风险，了解系统安全状况。根据被评估对象的实际情况、所属行业及系统使用的密码产品情况，选择并确定测评依据。在系统真实环境下进行测评，以评估密码保障是否安全有效，密码使用是否合规、正确、有效。并通过测评发现系统存在的安全隐患和风险，提出可行性完善建议。

2.2开展商用密码安全性评估的时机

网络安全等级保护条例中第四十七条非涉密网络密码保护规定，非涉密网络应当按照国家密码管理法律法规和标准的要求，使用密码技术、产品和服务。第三级以上网络应当采用密码保护，并使用国家密码管理部门认可的密码技术、产品和服务。第三级以上网络运营者应在网络规划、建设和运行阶段，按照密码应用安全性评估管理办法和相关标准，委托密码应用安全性测评机构开展密码应用安全性评估。网络通过评估后，方可上线运行，并在投入运行后，每年至少组织一次评估。密码应用安全性评估结果应当报受理备案的公安机关和所在地设区市的密码管理部门备案。

商用密码应用安全性评估管理办法（试行）中第八条，在重要领域网络与信息系统规划阶段，责任单位应当依据商用密码应用安全性有关标准，制定商用密码应用建设方案，组织专家或委托测评机构进行评估。评估结果作为项目规划立项的重要依据和申报使用财政性资金项目的必备材料。

第九条，重要领域网络与信息系统建设完成后，责任单位应当委托测评机构进行商用密码应用安全性评估，评估结果作为项目建设验收的必备材料。

第十条，重要领域网络与信息系统投入运行后，责任单位应当委托测评机构定期开展商用密码应用安全性评估，评估未通过，责任单位应当限期整改并重新组织评估。

关键信息基础设施、网络安全等级保护第三级及以上信息系统，每年至少评估一次，测评机构可将商用密码应用安全性评估与关键信息基础设施网络安全测评、网络安全等级保护测评同步进行。对其他信息系统定期开展检查和抽查。

2.3测评依据

1、《信息系统密码应用基本要求》GB/T 39786—2021

2、《信息系统密码测评要求》GM/T 0115—2021

3、《商用密码应用安全性评估测评过程指南》GM/T 0116—2021

2.4测评范围

指标要求			测评项数	应用要求
总体要求	密码算法		1	应
	密码技术		1	应
	密码产品		1	应
	密码服务		1	应
密码技术	物理和环境	身份鉴别	1	应

指标要求			测评项数	应用要求
应用	安全	电子门禁记录数据完整性	1	应
		视频记录数据完整性	1	应
		硬件密码模块实现	1	宜
	网络和通讯安全	身份鉴别	1	应
		访问控制信息完整性	1	应
		通信数据完整性	1	应
		通信数据机密性	1	应
		集中管理通道安全	1	应
		硬件密码模块实现	1	宜
	设备和计算安全	身份鉴别	1	应
		远程管理身份鉴别信息机密性	1	应
		访问控制信息完整性	1	应
		重要程序或文件完整性	1	应
		日志记录完整性	1	应
		硬件密码模块实现	1	宜
	应用和数据安全	身份鉴别	1	应
		访问控制	1	应
		数据传输安全	2	应
		数据存储安全	2	应
		日志记录完整性	1	应
		重要应用程序的加载和卸载	1	应
		硬件密码模块实现	1	宜
密钥管理	生成		1	应
	存储		1	应
	使用		1	应
	分发		1	应
	导入与导出		1	应
	备份与恢复		1	应
	归档		1	应
	销毁		1	应
安全管理	制度	制定密码安全管理制度	1	应
		定期修订安全管理制度	1	应
		明确管理制度发布流程	1	应
	人员	了解并遵守密码相关法律法规	1	应
		正确使用密码相关产品	1	应
		建立岗位责任及人员培训制度	2	应
		设置密码管理和技术岗位并定期考核	1	应
		建立关键岗位人员保密制度和调离制度	1	应
	实施	规划	2	应
		建设	2	应
		运行	2	应
	应急	应急预案	1	应
		事件处置	1	应
		向有关主管部门上报处置情况	1	应
测评项合计		55项		

4.1.2.1 测评方法

本次商用密码应用安全性评估使用的测评方法包括：

访谈：通过与被测单位的相关人员进行交谈和问询，了解被测信息系统技术和管理方面的一些基本信息，并对一些测评内容进行确认；

文档审查：审核被测单位提交的有关信息系统安全的各个方面的文档，如：被测系统总体描述文件，被测系统密码总体描述文件，安全管理制度文件，密钥管理制度，各种密码安全规章制度及相关过程管理记录、配置管理文档，被测单位的信息化建设与发展状况以及联络方式；密码应用方案及评审意见，安全保护等级定级报告，系统验收报告，安全需求分析报告，安全总体方案，自查或上次评估报告等等。通过对这些文档的审核与分析确认测评的相关内容是否达到安全保护等级的要求；

实地查看：现场查看测评对象所处的环境、外观等情况；

配置检查：查看测评对象的相关配置；

工具测试：根据被测信息系统的实际情况，密评人员使用适合的技术工具对其进行测试。

4.1.2.2 测评内容

参照GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》和《信息系统密码测评要求》，结合已选定的测评指标和测评对象，确定现场测评实施的工作内容如下。

（一）物理和环境安全测评

物理和环境安全测评将通过访谈、文档审查、实地查看、配置检查和工具测试的方式测评本系统的物理安全保障情况，主要涉及数据中心机房的电子门禁系统、视频监控系统。

在内容上，物理和环境安全层面测评实施过程涉及以下各测评单元。

表1物理和环境安全测评工作内容

序号	测评单元	测评指标	测评对象	测评方法
1	身份鉴别	宜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。	信息系统所在机房等重要区域及其电子门禁系统。	访谈物理安全负责人，并查看相关技术文档，了解机房电子门禁系统的身份鉴别措施； 核查电子门禁系统是否具有商用密码产品认证证书； 查看电子门禁系统后台配置，确认电子门禁系统是否采用密码技术来确保进入重要区域人员身份鉴别信息的真实性； 实地查看电子门禁系统，检测电子门禁系统身份鉴别机制的有效性。
2	电子门禁记录数据存储完整	宜采用密码技术保证电子门禁系统	信息系统所在机房等重要区域及其	访谈物理安全负责人，并查看相关技术文档，了解机房电子门禁系统进出记录的完整性保护措施；

序号	测评单元	测评指标	测评对象	测评方法
	性	进出记录数据的存储完整性。	电子门禁系统。	核查电子门禁系统是否具有商用密码产品认证证书； 查看电子门禁系统后台配置，确认电子门禁系统是否采用密码技术的完整性服务来确保电子门禁系统进出记录的完整性； 实地查看电子门禁系统，尝试篡改电子门禁系统进出记录，验证完整性保护功能是否有效。
3	视频监控记录数据存储完整性	宜采用密码技术保证视频监控音像记录数据的存储完整性。	信息系统所在机房等重要区域及其视频监控系统。	访谈物理安全负责人，并查看相关技术文档，了解机房视频监控系统视频监控音像记录数据存储的完整性保护技术及实现机制； 核查实现完整性保护操作的密码产品是否具有商用密码产品认证证书，密码算法、密码协议是否符合相关密码标准； 实地查看视频监控系统，尝试篡改视频监控音像记录数据，验证完整性保护功能是否有效。

（二）网络和通信安全测评

网络和通信安全测评将通过访谈、文档审查、实地查看、配置检查和工具测试的方式测评本系统的网络和通信安全保障及密码应用情况，主要涉及IPSec/SSL VPN综合安全网关、网络和安全设备、集中管理等。

在内容上，网络和通信安全层面测评实施过程涉及以下各测评单元。

表2网络和通信安全测评工作内容

序号	测评单元	测评指标	测评对象	测评方法
1	身份鉴别	应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。	信息系统与网络边界外建立的网络通信信道，以及提供通信保护功能的设备或组件、密码产品。	查看设计文档中通信保护功能的设备或组件与其客户端之间身份认证采用的密码技术及实现机制； 查看身份鉴别机制密码算法、密码协议是否符合《信息技术 安全技术实体鉴别》（GB/T 15843）、《SM2密码算法使用规范》（GM/T 0009-2012）等密码相关国家标准和行业标准； 查看身份鉴别采用的密码设备是否获得商用密码产品认证证书；

序号	测评单元	测评指标	测评对象	测评方法
				使用Wireshark验证传输过程中鉴别信息机密性的合规性和有效性。
2	通信数据完整性	宜采用密码技术保证通信过程中数据的完整性。	信息系统与网络边界外建立的网络通信信道，以及提供通信保护功能的设备或组件、密码产品。	查看技术文档中运维人员远程管理系统内的服务器、网络和安全设备、各业务应用系统时，采用的通信数据完整性保护技术及实现机制； 查看通信数据完整性保护所使用的密码产品是否经过了国家密码管理部门核准，密码算法是否符合法规和密码相关标准的要求； 使用Wireshark捕获并分析通信数据，验证通信数据完整性保护的合规性和有效性。
3	通信过程中重要数据的机密性	应采用密码技术保证通信过程中重要数据的机密性。	信息系统与网络边界外建立的网络通信信道，以及提供通信保护功能的设备或组件、密码产品。	查看技术文档中运维人员远程管理系统内的服务器、网络和安全设备、各业务应用系统时，采用的通信数据机密性保护技术及实现机制； 查看通信数据机密性保护所使用的密码产品是否经过了国家密码管理部门核准，密码算法是否符合法规和密码相关标准的要求； 使用Wireshark捕获并分析通信数据，验证通信数据机密性保护的合规性和有效性。
4	网络边界访问控制信息的完整性	宜采用密码技术保证网络边界访问控制信息的完整性。	信息系统与网络边界外建立的网络通信信道，以及提供网络边界访问控制功能的设备或组件、密码产品。	查看系统是否使用以及使用何种密码技术对网络边界访问控制信息进行完整性保护； 查看访问控制信息完整性保护所使用的密码算法是否符合法规和密码相关标准的要求，密码设备是否经获得商用密码产品认证证书。
5	安全接入认证	可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，确保接入的设备身份真实性。	信息系统内部网络，以及提供设备入网接入认证功能的设备或组件、密码产品。	查看系统是否使用以及使用何种密码技术对安全接入进行安全接入保护； 查看保护所使用的密码算法是否符合法规和密码相关标准的要求，密码设备是否经获得商用密码产品认证证书。

（三）设备和计算安全测评

设备和计算安全测评将通过访谈、文档审查、配置检查和工具测试的方式测评本系统的网络设备、安全设备、主机操作系统、数据库管理系统、密码设备的安全保障及密码应用情况。

在内容上，设备和计算安全层面测评实施过程涉及以下各测评单元。

表3设备和计算安全测评工作内容

序号	测评单元	测评指标	测评对象	测评方法
1	身份鉴别	应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。	通用设备（及其操作系统、数据库管理系统）、网络及安全设备、密码设备、各类虚拟设备，以及提供身份鉴别功能的密码产品。	结合设计文档，访谈系统管理员和数据库管理员，了解用户在本地登录核心服务器或核心数据库时，系统对用户实施身份鉴别的过程中是否采用了密码技术对主机标识信息进行密码保护，并明确其所采用的密码技术； 核查主机用户身份鉴别过程中使用的密码产品是否获得商用密码产品认证证书； 检查主机用户身份鉴别过程是否使用国家密码管理部门认可的密码算法；如果采用了口令鉴别方式，使用Wireshark验证口令鉴别过程中采用的密码保护技术的合规性和有效性； 查看主机配置信息，确认身份标识是否具有唯一性、身份鉴别信息的复杂度是否符合要求； 查看主机配置信息及鉴别信息更换记录，确认鉴别信息是否定期更换。
2	远程管理通道安全	远程管理设备时，应采用密码技术建立安全的信息传输通道。	通用设备、网络及安全设备、密码设备、各类虚拟设备，以及提供安全的信息传输通道的密码产品。	访谈系统管理员，并查阅相关技术文档，了解网络设备、安全设备、服务器、数据库管理系统、密码设备等远程管理时是否采用密码技术对远程管理用户身份标识信息进行机密性保护； 核查远程管理鉴别信息机密性保护所使用的密码产品是否获得商用密码产品认证证书，密码算法是否符合法规和密码相关标准的要求； 如果采用IPSec或SSL协议进行远程管理，使用Wireshark验证口令鉴别过程中采用的密码技术的合规性和有效性。
3	系统资源访问控制	宜采用密码技术保	通用设备（及其操作系统、数据库管理系统）	查看相关技术文档，访谈系统管理员，了解系统资源访问控

序号	测评单元	测评指标	测评对象	测评方法
	信息完整性	证系统资源访问控制信息的完整性。	、网络及安全设备、密码设备、各类虚拟设备，以及提供完整性保护功能的密码产品。	制信息完整性保护密码技术及实现机制； 查看是否使用国家密码管理部门认可的密码算法；密码设备是否获得商用密码产品认证证书。
4	重要信息资源安全标记完整性	宜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。	通用设备（及其操作系统、数据库管理系统）、网络及安全设备、密码设备、各类虚拟设备，以及提供完整性保护功能的密码产品。	查看相关技术文档，访谈系统管理员，了解重要信息资源安全标记完整性保护密码技术及实现机制； 查看是否使用国家密码管理部门认可的密码算法；密码设备是否获得商用密码产品认证证书。
5	日志记录完整性	宜采用密码技术保证日志记录的完整性。	通用设备（及其操作系统、数据库管理系统）、网络及安全设备、密码设备、各类虚拟设备，以及提供完整性保护功能的密码产品。	审阅技术文档，访谈安全审计员，了解日志信息完整性保护密码技术及实现机制； 如果采用了密码技术，检查系统是否使用国家密码管理部门认可的密码算法、协议；密码设备是否经过了国家密码管理部门核准，相关密码功能是否正确有效。
6	重要可执行程序完整性、重要可执行程序来源真实性	宜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。	通用设备（及其操作系统、数据库管理系统）、网络及安全设备、密码设备、各类虚拟设备，以及提供完整性保护和来源真实性功能的密码产品。	查看技术文档中关于可信计算技术建立从系统到应用信任链的实现机制； 查看技术文档中关于系统运行过程中重要程序或文件完整性保护技术及实现机制； 核查重要程序或文件完整性所使用的密码产品是否获得商用密码产品认证证书； 尝试在系统运行过程中对重要程序或文件进行篡改，验证完整性保护技术及实现机制的有效性； 查看所使用的密码算法、密码协议是否符合有关密码国家标准和行业标准。

（四）应用和数据安全测评

应用和数据安全测评将通过访谈、文档审查、配置检查和工具测试的方式测评本系统的应用和数据安全保障及密码应用情况，主要涉及鉴别数据、关键业务数据、重要用户信息、配置数据、审计数据、重要可执行程序等关键数据。

在内容上，应用和数据安全层面测评实施过程涉及以下各测评单元。

表4应用和数据安全测评工作内容

序号	测评单元	测评指标	测评对象	测评方法

序号	测评单元	测评指标	测评对象	测评方法
1	身份鉴别	应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。	业务应用，以及提供身份鉴别功能的密码产品。	结合设计文档访谈应用系统管理员，了解被测应用系统在对用户实施身份鉴别的过程中是否使用了密码技术对假冒的身份标识信息进行有效鉴别，并明确其所采用的密码技术和密码产品； 核查应用系统用户身份鉴别过程中使用的密码产品是否获得商用密码产品认证证书； 检查应用系统用户身份鉴别过程是否使用国家密码管理部门认可的密码算法；如果采用了口令鉴别方式，使用Wireshark验证口令鉴别过程中采用的密码技术的合规性和有效性。
2	访问控制信息完整性	宜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。	业务应用，以及提供完整性保护功能的密码产品。	查看相关技术文档，访谈应用系统管理员，了解系统如何对业务应用系统访问控制策略、数据库表访问控制信息和重要信息资源敏感标记等重要信息进行完整性保护； 如果重要信息采用了完整性保护，了解是否使用密码技术对重要信息进行完整性保护； 如果采用了密码技术，查验系统是否使用国家密码管理部门认可的密码算法、密码协议；密码产品是否获得商用密码产品认证证书；相关密码功能是否正确有效。
3	重要信息资源安全标记完整性	宜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	业务应用，以及提供完整性保护功能的密码产品。	查看相关技术文档，访谈系统管理员，了解重要信息资源安全标记完整性保护密码技术及实现机制； 查看是否使用国家密码管理部门认可的密码算法；密码设备是否获得商用密码产品认证证书。
4	重要数据传输机密性	应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。	业务应用，以及提供机密性保护功能的密码产品。	查看相关技术文档，了解应用系统中鉴别数据、重要业务数据、重要用户信息等重要数据在传输过程中的机密性保护技术及实现机制； 使用Wireshark验证应用系统中重要数据在传输过程中机密性保护的有效性； 查看所使用的密码算法是否符合密码相关国家标准和行业标准。

序号	测评单元	测评指标	测评对象	测评方法
5	重要数据存储机密性	应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。	业务应用，以及提供机密性保护功能的密码产品。	查看相关技术文档，了解应用系统中鉴别数据、重要业务数据和重要用户信息等在存储过程中的机密性保护技术及实现机制； 如果采用了密码产品进行存储机密性保护，核查密码产品是否具有商用密码产品认证证书； 通过读取硬盘中的数据或捕获分析进出存储机密性保护所采用的密码产品的数据，验证应用系统中重要数据在存储过程中机密性保护的有效性； 查看所使用的密码算法是否符合密码相关国家标准和行业标准。
6	重要数据传输完整性	宜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。	业务应用，以及提供完整性保护功能的密码产品。	查看相关技术文档，了解应用系统中鉴别数据、重要审计数据、重要用户信息等重要数据在传输过程中的完整性保护技术及实现机制； 使用Wireshark验证应用系统中重要数据在传输过程中完整性保护的有效性； 查看所使用的密码算法是否符合密码相关国家标准和行业标准。
7	重要数据存储完整性	宜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。	业务应用，以及提供完整性保护功能的密码产品。	查看相关技术文档，了解应用系统中鉴别数据、业务数据、审计数据等重要数据在存储过程中的完整性保护技术及实现机制； 如果采用了密码产品进行存储完整性保护，核查密码产品是否具有商用密码产品认证证书； 通过读取硬盘中的数据或捕获分析进出存储完整性保护所采用的密码产品的数据，验证应用系统中重要数据在存储过程中完整性保护的有效性； 查看所使用的密码算法是否符合密码相关国家标准和行业标准。
8	不可否认性	在可能涉及法律责任认定的应用中，宜采用密码技术提供数据原发证据和数据接收证据，实	业务应用，以及提供不可否认性功能的密码产品。	审阅技术文档，访谈安全审计员，了解被测应用系统是否具有不可否认性功能； 如果实现了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，了解是否使用密码技术、采用了何种密码技术； 如果采用了密码技术，检查系统

序号	测评单元	测评指标	测评对象	测评方法
		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。		是否使用国家密码管理部门认可的密码算法、协议；如果使用第三方电子认证服务，则应对密码服务进行核查。

（五）管理制度测评

管理制度测评将通过访谈和文档审查的方式，测评本系统的密码安全管理制度是否能够保证密码应用的适宜性、充分性和有效性，主要涉及安全主管等访谈对象和密码安全管理制度、安全操作规范、管理制度发布流程、制度审定或论证记录等文档。

在内容上，管理制度层面测评实施过程涉及以下各测评单元。

表5制度管理测评工作内容

序号	测评单元	测评指标	测评对象	测评方法
1	具备密码应用安全管理制度	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。	安全管理制度类文档。	核查各项安全管理制度是否包括密码人员管理、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。
2	密钥管理规则	应根据密码应用方案建立相应密钥管理规则。	密码应用方案、密钥管理制度及策略类文档。	核查是否有通过评估的密码应用方案，并核查是否根据密码应用方案建立相应密钥管理规则（如密钥管理制度及策略类文档中的密钥全生存周期的安全性保护相关内容）且对密钥管理规则进行评审，以及核查信息系统中密钥是否按照密钥管理规则进行生存周期的管理。
3	建立操作规程	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。	操作规程类文档。	核查是否对密码相关管理人员或操作人员的日常管理操作建立操作规程。
4	定期修订安全管理制度	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，对存在不足或需要改进之处进行修订。	安全管理制度类文档、操作规程类文档、记录表单类文档。	访谈安全主管是否定期对密码安全管理制度体系的合理性和适用性进行审定； 核查是否具有安全管理制度的审定或论证记录，如果对制度做过修订，核查是否有修订版本的安全管理制度。
5	明确管理制度发布流程	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。	安全管理制度类文档、操作规程类文档、记录表单类文档。	访谈安全主管是否具有管理制度发布流程； 核查相关密码应用安全管理制度和操作规程是否具有相应明确的发布流程和版本控制。

序号	测评单元	测评指标	测评对象	测评方法
6	制度执行过程记录留存	应具有密码应用操作规程的相关执行记录并妥善保存。	安全管理制度类文档、记录表单类文档。	访谈管理员，制度执行过程中是否形成记录；如形成查看相关记录信息是否完善。

（六）人员管理测评

人员管理测评将通过访谈、文档审查、实地查看的方式，测评本系统的人员安全管理保障情况，主要涉及系统负责人、安全主管、系统管理员、安全审计员、密钥管理员、密码操作员等访谈对象以及人员安全管理制度、保密合同、记录表单等文档，并对设备与系统的管理和使用账号进行实地查看。

在内容上，人员管理层面测评实施过程涉及以下各测评单元。

表6人员管理测评工作内容

序号	测评单元	测评指标	测评对象	测评方法
1	了解并遵守密码相关法律法规和密码管理制度	相关人员应了解并遵守密码相关法律法规、密码应用安全管理制度。	系统相关人员（包括系统负责人、安全主管、密钥管理员、密码审计员、密码操作员等）。	核查系统相关人员是否了解并遵守密码相关法律法规和密码应用安全管理制度。
2	建立密码应用岗位责任制度	应建立密码应用岗位责任制度，明确各岗位在安全系统中的职责和权限。 1）根据密码应用的实际情况，设置密钥管理员、密码安全审计员、密码操作员等关键安全岗位； 2）对关键岗位建立多人共管机制； 3）密钥管理、密码安全审计、密码操作人员职责互相制约互相监督，其中密钥管理员岗位不可与密码审计员、密码操作员等关键安全岗位兼任； 4）相关设备与系统的管理和使用账号不得多人共用。	安全管理制度类文档、系统相关人员（包括系统负责人、安全主管、密钥管理员、密码审计员、密码操作员等）。	核查安全管理制度类文档是否根据密码应用的实际情况，设置密钥管理员、密码审计员、密码操作员等关键安全岗位并定义岗位职责；核查是否对关键岗位建立多人共管机制，并确认密钥管理员岗位人员是否不兼任密码审计员、密码操作员等关键安全岗位；核查相关设备与系统的管理和使用账号是否有多人共用情况。

序号	测评单元	测评指标	测评对象	测评方法
3	建立上岗人员培训制度	应建立上岗人员培训制度，对于涉及密码的操作和管理的人员进行专门培训，确保其具备岗位所需专业技能。	安全管理制度类文档和记录表单类文档、系统相关人员（包括系统负责人、安全主管、密钥管理员、密码审计员、密码操作员等）。	核查安全教育和培训计划文档是否具有针对涉及密码的操作和管理的人员的培训计划；核查安全教育和培训记录是否有密码培训人员、密码培训内容、密码培训结果等的描述。
4	定期进行安全岗位人员考核	应定期对密码应用安全岗位人员进行考核。	安全管理制度类文档和记录表单类文档、系统相关人员（包括系统负责人、安全主管、密钥管理员、密码审计员、密码操作员等）。	核查安全管理制度文档是否包含具体的人员考核制度和惩戒措施；核查人员考核记录内容是否包括安全意识、密码操作管理技能及相关法律法规；核查记录表单类文档确认是否定期进行岗位人员考核。
5	建立关键岗位人员保密制度和调离制度	应建立关键人员保密制度和调离制度，签订保密合同，承担保密义务。	安全管理制度类文档和记录表单类文档、系统相关人员（包括系统负责人、安全主管、密钥管理员、密码审计员、密码操作员等）。	核查人员离岗的管理文档是否规定了关键岗位人员保密制度和调离制度等；核查保密协议是否有保密范围、保密责任、违约责任、协议的有效期限和责任人的签字等内容。

（七）建设运行测评

实施建设运行测评将通过访谈、文档审查的方式，测评本系统规划、建设、运行管理的安全措施，主要涉及系统负责人等访谈对象以及密码应用方案、方案评审意见、实施方案、商用密码产品清单及资质等文档。

在内容上，建设运行层面测评实施过程涉及以下各测评单元。

表7建设运行测评工作内容

序号	测评单元	测评指标	测评对象	测评方法
1	制定密码应用方案	应依据密码相关标准和密码应用需求，制定密码应用方案。	密码应用方案。	核查在信息系统规划阶段，是否依据密码相关标准和信息系统密码应用需求，制定密码应用方案，并核查方案是否通过评估。
2	制定密钥安全管理策略	应根据密码应用方案，确定系统涉及的密钥种类、体系及其生命周期环节，各环节安全管理要求参照《信息安全技术 信息系统密码应用基本要求》附录A。	密码应用方案、密钥管理制度及策略类文档。	核查是否有通过评估的密码应用方案，并核查是否根据密码应用方案，确定系统涉及的密钥种类、体系及其生存周期环节；若信息系统没有相应的密码应用方案，则参照附录A密钥生存周期管理检查要点核查密钥生存周期的各个环节是否符合要求。

序号	测评单元	测评指标	测评对象	测评方法
3	制定实施方案	应按照应用方案实施建设。	密码实施方案。	核查是否有通过评估的密码应用方案，并核查是否按照密码应用方案，制定密码实施方案。
4	投入运行前进行密码应用安全性评估	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。	密码应用安全性评估报告、系统负责人。	核查信息系统投入运行前，是否组织进行密码应用安全性评估；核查是否具有系统投入运行前编制的密码应用安全性评估报告且系统通过评估。
5	定期开展密码应用安全性评估及攻防对抗演习	在运行过程中，应严格执行既定的密码应用安全管理制度，应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。	密码应用安全管理制度、密码应用安全性评估报告、攻防对抗演习报告、整改文档。	核查信息系统投入运行后，责任单位是否严格执行既定的密码应用安全管理制度，定期开展密码应用安全性评估及攻防对抗演习，并具有相应的密码应用安全性评估报告及攻防对抗演习报告；核查是否根据评估结果制定整改方案，并进行相应整改。

（八）应急处置测评

应急处置测评将通过访谈、文档审查的方式，测评本系统应急体系的完备情况，主要涉及安全主管等访谈对象以及系统应急预案、应急相关管理制度、应急处置记录等文档。

在内容上，应急处置层面测评实施过程涉及以下各测评单元。

表8应急处置测评工作内容

序号	测评单元	测评指标	测评对象	测评方法
1	应急策略	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。	密码应用应急处置方案、应急处置记录类文档。	核查是否根据密码应用安全事件等级制定了相应的密码应用应急策略并对应急策略进行评审， 应急策略中是否明确了密码应用安全事件发生时的应急处理流程及其他管理措施，并遵照执行； 若发生过密码应用安全事件，核查是否立即启动应急处置措施并具有相应的处置记录。
2	事件处置	事件发生后，应及时向信息系统主管部门进行报告。	密码应用应急处置方案、安全事件报告。	核查密码应用安全事件发生后，是否及时向信息系统主管部门进行报告。
3	向有关主管部门上报处置情况	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。	密码应用应急处置方案、安全事件发生情况及处置情况报告。	核查密码应用安全事件处置完成后，是否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，如事件处置完成后， 向相关部门提交安全事件发生情况及处置情况报告。

4.1.3.1 处理机制要求

4.1.3.2.1　等级保护测评服务处理机制要求

应按照国家相关要求，从“定级-备案-等级测评-安全建设整改-配合监督检查”5个环节配合采购单位做好等级保护工作。其中针对等级测评工作过程，依据《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）和《信息安全技术网络安全等级保护测评过程指南》（GB/T28449-2018）等国家关于信息系统安全等级保护的相关标准和规范要求，要求参选人严格按照下列流程开展工作：

测评准备阶段：是开展等级测评工作的前提和基础，是整个等级测评过程有效性的保证。测评准备工作是否充分直接关系到后续工作能否顺利开展。本活动的主要任务是掌握被测系统的详细情况，准备测试工具，为编制测评方案做好准备。

方案编制阶段：是开展等级测评工作的关键活动，为现场测评提供最基本的文档和指导方案。本活动的主要任务是确定与被测信息系统相适应的测评对象、测评指标及测评内容等，并根据需要重用或开发测评指导书，形成测评方案。

现场测评阶段：是开展等级测评工作的核心活动。本活动的主要任务是按照测评方案的总体要求，严格按照测评指导书执行，分步实施所有测评项目，以了解系统的真实保护情况，获取足够证据，发现系统存在的安全问题。

分析与报告编制阶段：是给出等级测评工作结果的活动，是总结被测系统整体安全保护能力的综合评价活动。本活动的主要任务是根据现场测评结果和《信息安全技术网络安全等级保护实施指南》的有关要求，通过单项测评结果判定、单元测评结果判定、整体测评和风险分析等方法，找出整个系统的安全保护现状与相应等级的保护要求之间的差距，并分析这些差距导致被测系统面临的风险，从而给出等级测评结论，形成《XXX系统网络安全等级保护测评报告》文本。

建设整改咨询阶段：建设整改咨询工作以等级测评发现的安全问题为工作重点，以及测评报告中安全建设整改建议;将信息系统的安全建设整改需求落实到可操作的安全技术和管理上，提出能够实现的技术参数或制度及其具体规范。并依据测评报告中安全建设整改建议开展建设整改工作时，服务商将提供建设整改过程中的与建设整改相关的咨询服务。

4.1.3.2.2　商用密码安全性评估处理机制要求

商用密码应用安全性评估工作依据《信息安全技术信息系统密码应用基本要求》、《信息系统密码应用测评要求》、《信息系统密码应用测评过程指南》标准，工作过程分为四项基本测评活动：测评准备活动、方案编制活动、现场测评活动、分析与报告编制活动。测评双方之间的沟通与洽谈贯穿整个测评过程。

测评准备活动：本活动是开展测评工作的前提和基础，本活动的主要任务是掌握被测系统的详细情况，准备测评工具，为编制测评方案做好准备。

方案编制活动：本活动是开展测评工作的关键活动，本活动的主要任务是确定与被测系统相适应的测评对象、测评指标及测评内容等，形成测评方案，为实施现场测评提供依据。

现场测评活动：本活动是开展测评工作的核心活动。主要任务是按照测评方案的总体要求，分步实施所有测评项目，包括单项测评、测评单元和整体测评等方面，以了解系统的真实保护情况，获取足够证据，发现系统存在的密码应用安全性问题。

分析与报告编制活动：本活动是给出测评工作结果的活动，是总结被测系统商用密码整体安全保护能力的综合评价活动。本活动的主要任务是根据现场测评结果和《信息系统密码应用基本要求》等文件的有关要求，通过单项测评结果判定、测评单元结果判定、整体测评和风险分析等方法，找出整个系统商用密码的安全保护现状与相应等级的保护要求之间的差距，并分析这些差距导致被测系统面临的风险，从而给出测评结论，形成测评报告文本。

整改咨询阶段：建设整改咨询工作以测评发现的问题为重点，编写信息系统密码测评整改建议；开展建设整改工作时，投标人提供建设整改相关的咨询服务。

2.7.2人员配置要求

密码测评项目组要求测评人员不少于5人，其中，包含项目经理1人，项目组成员不少于4人。项目负责人与项目组成员要求具备“商用密码应用安全性评估人员测评能力考核合格证书”。

2.7.3其他要求

供应商须完全满足业主对本项目的所有要求及技术参数。