

磋商文件

(服务类)

采购项目名称：陕西省市场监督管理局商用密码安全性评估项目项目(二次)

采购项目编号：GR25-CS-007.1B1

陕西省市场监督管理局信息中心

伟江项目管理咨询有限公司共同编制

2025年04月09日

第一章 竞争性磋商邀请

伟江项目管理咨询有限公司（以下简称“代理机构”）受陕西省市场监督管理局信息中心委托，拟对陕西省市场监督管理局商用密码安全性评估项目项目(二次)采用竞争性磋商采购方式进行采购，兹邀请供应商参加本项目的竞争性磋商。

一、项目编号：**GR25-CS-007.1B1**

二、项目名称：陕西省市场监督管理局商用密码安全性评估项目项目(二次)

三、磋商项目简介

本项目为陕西省市场监督管理局商用密码安全性评估项目项目（二次）。

四、邀请供应商

本次采购采取公告征集邀请磋商的供应商。

公告征集：本次竞争性磋商在“陕西省政府采购网（www.ccgp-shaanxi.gov.cn）”上以公告形式发布，兹邀请符合本次采购要求的供应商参加本项目的竞争性磋商。

五、供应商参加本次政府采购活动应具备的条件

（一）满足《中华人民共和国政府采购法》第二十二条规定；

（二）落实政府采购政策需满足的资格要求：

落实政府采购促进中小企业发展的相关政策：

采购包1（商用密码安全性评估项目项目）：属于专门面向中小企业采购。

（三）本项目的特定资格要求：

采购包1：

1、“商用密码检测机构资质证书”：供应商须具备国家密码管理局颁发的“商用密码检测机构资质证书”

六、电子化采购相关事项

本项目实行电子化采购，使用的电子化交易系统为：陕西省政府采购综合管理平台的项目电子化交易系统（以下简称“项目电子化交易系统”），登录方式及地址：通过陕西省政府采购网（<http://www.ccgp-shaanxi.gov.cn/>）首页供应商用户登录陕西省政府采购综合管理平台（以下简称“政府采购平台”），进入项目电子化交易系统。供应商应当按照以下要求，参与本次电子化采购活动。

（一）供应商应当自行在陕西省政府采购网-办事指南查看相应的系统操作指南，并严格按照操作指南要求进行系统操作。在登录、使用政府采购平台前，应当按照要求完成供应商注册和信息完善，加入政府采购平台供应商库。

（二）供应商应当使用纳入陕西省政府采购综合管理平台数字证书互认范围的数字证书及签章（以下简称“互认的证书及签章”）进行系统操作。供应商使用互认的证书及签章登录政府采购平台进行的一切操作和资料传递，以及加盖电子签章确认采购过程中制作、交换的电子数据，均属于供应商真实意思表示，由供应商对其系统操作行为和电子签章确认的事项承担法律责任。

已办理互认的证书及签章的供应商，校验互认的证书及签章有效性后，即可按照系统操作要求进行身份信息绑定、权限设置和系统操作；未办理互认的证书及签章的供应商，按要求办理互认的证书及签章并校验有效性后，按照系统操作要求进行身份信息绑定、权限设置和系统操作。互认的证书及签章的办理与校验，可查看陕西省政府采购网-办事指南-CA及签章服务。

供应商应当加强互认的证书及签章日常校验和妥善保管，确保在参加采购活动期间互认的证书及签章能够正常使用；供应商应当严格互认的证书及签章的内部授权管理，防止非授权操作。

（三）供应商应当自行准备电子化采购所需的计算机终端、软硬件及网络环境，承担因准备不足产生的不利后果。

（四）政府采购平台技术支持：

在线客服：通过陕西省政府采购网-在线客服进行咨询

技术服务电话：029-96702

CA及签章服务：通过陕西省政府采购网-办事指南-CA及签章服务进行查询

七、竞争性磋商文件获取时间、方式及地址

（一）磋商文件获取时间：详见采购公告或邀请书。

（二）在磋商文件获取开始时间前，采购人或代理机构将本项目磋商文件上传至项目电子化交易系统，向供应商提供。供应商通过项目电子化交易系统获取磋商文件。成功获取磋商文件的，供应商将收到已获取磋商文件的回执函。未成功获取磋商文件的供应商，不得参与本次采购活动，不得对磋商文件提起质疑。

成功获取磋商文件后，采购人或代理机构进行澄清或者修改的，澄清或者修改的内容可能影响响应文件编制的，采购人或代理机构将通过项目电子化交易系统发布澄清或者修改后的磋商文件，供应商应当重新获取磋商文件；澄清或者修改后的磋商文件发布日期距提交响应文件截止日期不足5日的，采购人或代理机构顺延提交响应文件的截止时间。供应商未重新获取磋商文件或者未按照澄清或者修改后的磋商文件编制响应文件进行响应的，自行承担不利后果。

注：获取的磋商文件主体格式包括pdf、word两种格式版本，其中以pdf格式为准。

八、首次响应文件提交截止时间及开启时间、地点、方式

（一）提交首次响应文件截止时间及开启时间：详见采购公告或邀请书。

（二）响应文件提交方式、地点：供应商应当在提交首次响应文件截止时间前，通过项目电子化交易系统提交响应文件。成功提交的，供应商将收到已提交响应文件的回执函。

九、磋商方式

本项目磋商小组与供应商通过项目电子化交易系统以在线方式进行磋商。磋商会议由磋商小组在线主持，供应商代表在线参加。供应商应随时关注项目电子化交易系统信息，及时参与在线磋商。供应商登录项目电子化交易系统，与磋商小组进行在线磋商、提交供应商响应表，供应商响应表应加盖供应商（法定名称）电子印章。

十、供应商信用融资

根据《陕西省财政厅关于加快推进我省中小企业政府采购信用融资工作的通知》（陕财办采〔2020〕15号）和《陕西省中小企业政府采购信用融资办法》（陕财办采〔2018〕23号）文件要求，为助力解决政府采购成交供应商资金不足、融资难、融资贵的困难，促进供应商依法诚信参加政府采购活动，有融资需求的供应商可登录陕西省政府采购网—陕西省政府采购金融服务平台（<http://www.ccgp-shaanxi.gov.cn/zcdservice/zcd/shanxi/>），选择符合自身情况的“政采贷”银行及其产品，凭项目成交结果、成交通知书等信息在线向银行提出贷款意向申请、查看贷款审批情况等。

十一、联系方式

采购人：陕西省市场监督管理局信息中心

地址：西安市二环北路东段739号

邮编：710000

联系人：陕西省市场监督管理局信息中心经办

联系电话：029-86138110

代理机构：伟江项目管理咨询有限公司

地址：西安市新城区龙首北路东段大明宫圣远广场A座8001

邮编：710000

联系人：吴斯琪

联系电话：029-81111916

采购监督机构：财政厅政府采购管理处

联系人：柴老师、杨老师

联系电话：029-68936409、029-68936410

第二章 供应商须知

2.1 供应商须知前附表

序号	应知事项	说明和要求
1	采购预算（实质性要求）	本项目各包采购预算金额如下： 采购包1：400,000.00元 供应商采购包报价高于采购包采购预算的，其响应文件将按无效处理。
2	最高限价（实质性要求）	详见第三章。 供应商的采购包响应报价高于最高限价的，其响应文件将按无效处理。
3	评审方法	综合评分法(详见第六章)。
4	是否接受联合体	采购包1：不接受 如以联合体响应的，联合体各方均应当具备本磋商文件要求的资格条件和能力。 （1）联合体各方均应具有承担本磋商项目必备的条件，如相应的人力、物力、资金等。 （2）磋商文件对供应商资格条件有特殊要求的，联合体各个成员都应当具备规定的相应资格条件。 （3）同一专业的单位组成的联合体，应当按照资质等级较低的单位确定联合体的资质等级。如：某联合体由三个单位组成，其中两个单位资质等级为甲级，另一单位资质等级为较甲级更低的乙级，则该联合体资质等级为乙级。
5	落实节能、环保产品政策	1.根据《财政部 发展改革委 生态环境部 市场监管总局关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9号）相关要求，政府采购节能产品、环境标志产品实施品目清单管理。财政部、发展改革委、生态环境部等部门确定实施政府优先采购和强制采购的产品类别，以品目清单的形式发布并适时调整。 2.本项目采购的无产品属于节能产品政府采购品目清单中应强制采购的产品范围，供应商应当提供国家确定的认证机构出具的、处于有效期之内的节能产品认证证书，否则作无效响应处理。 3.本项目采购的无产品属于节能产品政府采购品目清单中应优先采购的产品范围，本项目采购的无产品属于环境标志产品政府采购品目清单中应优先采购的产品范围，评审得分相同的，按供应商提供的优先采购产品认证证书数量由多到少顺序排列。
6	小微企业（监狱企业、残疾人福利性单位视同小微企业）价格扣除（仅非预留份额采购项目或预留份额采购项目中的非预留部分采购包适用）	（仅非预留份额采购项目或预留份额采购项目中的非预留部分采购包适用）根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）第九条和《关于进一步加大政府采购支持中小企业力度的通知》（财库〔2022〕19号）的规定。 关于本项目采购包中执行小微企业（监狱企业、残疾人福利性单位视同小微企业）价格扣除情况、具体扣除比例和规则详见第六章。 （其他情形）不适用。

7	充分、公平竞争保障措施（实质性要求）	<p>核心产品允许有多个，不同供应商提供了任意一个相同品牌的核心产品，即视为提供相同品牌的供应商。</p> <p>提供相同品牌产品且通过资格审查、符合性审查的不同供应商参加同一合同项下采购活动的，按一家供应商计算，评审后得分最高的同品牌供应商获得成交供应商推荐资格；最后评审得分相同的，由采购人或者采购人委托磋商小组采取随机抽取方式确定一个供应商获得成交供应商推荐资格，其他同品牌供应商不作为成交候选人。</p> <p>核心产品清单详见第三章。</p> <p>在符合性审查、有效报价环节提供核心产品品牌不足3个的，视为有效响应供应商不足3家。</p>
8	不正当竞争预防措施（实质性要求）	<p>在磋商过程中，磋商小组认为供应商报价明显低于其他通过符合性审查供应商的报价，有可能影响产品质量或者不能诚信履约的，磋商小组应当要求其在合理的时间内通过项目电子化交易系统进行书面说明，必要时提交相关证明材料。供应商提交的书面说明和相关证明材料，应当加盖供应商公章，在磋商小组要求的时间内通过项目电子化交易系统进行提交，否则提交的相关材料无效，视为不能证明其响应报价合理性。供应商不能证明其响应报价合理性的，磋商小组应当将其响应文件作为无效处理。</p>
9	磋商保证金	<p>采购包1保证金金额：6,000.00元</p> <p>缴交渠道：转账、支票、汇票等（需通过实体账户、户名及开户行信息）</p> <p>开户名称：伟江项目管理咨询有限公司</p> <p>开户银行：兴业银行股份有限公司西安未央路支行</p> <p>银行账号：456910100100163145</p>
10	标书费信息	免费获取
11	履约保证金（实质性要求）	采购包1：不缴纳
12	响应有效期（实质性要求）	提交首次响应文件的截止之日起不少于90天。
13	招标代理服务费（实质性要求）	<p>本项目收取代理服务费</p> <p>代理服务费用收取对象：中标/成交供应商</p> <p>代理服务费收费标准：本项目采购代理服务费以采购项目的成交金额作为收费基数，按照国家计委（计价格【2002】1980号）《招标代理服务收费管理暂行办法》规定的服务类收费标准收取。</p>
14	采购结果公告	采购结果将在陕西省政府采购网予以公告。
15	成交通知书	采购结果公告发布的同时，采购人或代理机构通过项目电子化交易系统向成交供应商发出成交通知书；成交供应商通过项目电子化交易系统获取成交通知书。
16	政府采购合同公告、备案	<p>政府采购合同签订之日起2个工作日内，采购人将政府采购合同在陕西省政府采购网予以公告；</p> <p>政府采购合同签订之日起7个工作日内，采购人将本项目采购合同通过政府采购平台进行备案。</p>
17	进口产品	不允许
18	是否组织潜在供应商现场考察	采购包1：组织现场踏勘：否

19	特殊情况	<p>出现下列情形之一的，采购人或者代理机构应当中止电子化采购活动，并保留相关证明材料备查：</p> <p>（一）交易系统发生故障（包括感染病毒、应用或数据库出错）而无法正常使用；</p> <p>（二）因组织场所停电、断网等原因，导致采购活动无法继续通过交易系统实施的；</p> <p>（三）其他无法保证电子化交易的公平、公正和安全的情况。</p> <p>出现上述的情形，不影响采购公平、公正的，采购人或者代理机构可以待上述情形消除后继续组织采购活动；影响或者可能影响采购公平、公正的，采购人或者代理机构应当依法终止采购活动。</p>
----	------	---

2.2总则

2.2.1适用范围

- 一、本磋商文件仅适用于本次竞争性磋商采购项目。
- 二、本磋商文件的最终解释权由陕西省市场监督管理局信息中心和伟江项目管理咨询有限公司享有。对磋商文件中供应商参加本次政府采购活动应当具备的条件，磋商项目技术、服务、商务及其他要求，评审细则及标准由陕西省市场监督管理局信息中心负责解释。除上述磋商文件内容，其他内容由伟江项目管理咨询有限公司负责解释。

2.2.2有关定义

- 一、“采购人”是指依法进行政府采购的各级国家机关、事业单位、团体组织。本次磋商的采购人是陕西省市场监督管理局信息中心。
- 二、“供应商”是指在按照磋商公告规定获取磋商文件，拟参加响应和向采购人提供货物、工程或服务的法人、其他组织或自然人。
- 三、“代理机构”是指政府采购集中采购机构和从事政府采购代理业务的社会中介机构。本项目的代理机构是伟江项目管理咨询有限公司。
- 四、“网上开启”是指供应商通过项目电子化交易系统在线完成签到、响应文件解密后，采购人或者采购代理机构通过项目电子化交易系统在线完成已解密响应文件的开启工作。
- 五、“电子评审”是指通过项目电子化交易系统在线完成资格审查小组、磋商小组组建，开展资格和符合性审查、比较与评价、出具磋商报告、推荐成交候选供应商等活动。

2.2.3响应费用（实质性要求）

供应商应自行承担参加竞争性磋商采购活动的全部费用。

2.3磋商文件

2.3.1磋商文件的构成

- 一、磋商文件是供应商准备响应文件和参加响应的依据，同时也是评审的重要依据。磋商文件用以阐明磋商项目所需的资质、技术、服务及报价等要求、磋商程序、有关规定和注意事项以及合同草案条款等。本磋商文件包括以下内容：
 - （一）竞争性磋商邀请；
 - （二）供应商须知；
 - （三）磋商项目技术、服务、商务及其他要求；
 - （四）资格审查；
 - （五）磋商过程中可实质性变动的内容；
 - （六）磋商办法；
 - （七）响应文件格式；
 - （八）拟签订采购合同文本。
- 二、供应商应认真阅读和充分理解磋商文件中所有的事项、格式条款和规范要求。供应商没有对磋商文件全面作出实质性

响应所产生的风险由供应商承担。

2.3.2磋商文件的澄清和修改

一、在提交首次响应文件截止时间前，采购人或者代理机构可以对已发出的磋商文件进行必要的澄清或者修改。

二、澄清或者修改的内容为磋商文件的组成部分，采购人或者代理机构将在陕西省政府采购网发布更正公告，供应商应及时关注本项目更正公告信息，按更正后公告要求进行响应。更正内容可能影响响应文件编制的，采购人或者代理机构将通过项目电子化交易系统发布更正后的磋商文件，供应商应依据更正后的磋商文件编制响应文件。若供应商未按前述要求进行响应的，自行承担不利后果。

2.4响应文件

2.4.1响应文件的语言

一、供应商提交的响应文件以及供应商与磋商小组在磋商过程中的所有来往书面文件均须使用中文。响应文件中如附有外文资料，主要部分要对应翻译成中文并附在相关外文资料后面。未翻译的外文资料，磋商小组将其视为无效材料。

二、翻译的中文资料与外文资料如果出现差异和矛盾时，以中文为准。涉嫌提供虚假材料的按照相关法律法规处理。

三、如因未翻译而造成对供应商的不利后果，由供应商承担。

2.4.2计量单位

除磋商文件中另有规定外，本项目均采用国家法定的计量单位。

2.4.3响应货币

本次项目均以人民币报价。

2.4.4知识产权

一、供应商应保证在本项目中使用的任何技术、产品和服务（包括部分使用），不会产生因第三方提出侵犯其专利权、商标权或其它知识产权而引起的法律和经济纠纷，如存在前述情形，由供应商承担所有相关责任。采购人享有本项目实施过程中产生的知识成果及知识产权。

二、供应商将在采购项目实施过程中采用自有或者第三方知识成果的，使用该知识成果后，供应商需提供开发接口和开发手册等技术资料，并承诺提供无限期支持，采购人享有使用权（含采购人委托第三方在该项目后续开发的使用权）。

三、如采用供应商所不拥有的知识产权，则在报价中必须包括合法使用该知识产权的相关费用。

四、构成本磋商文件的各组成部分，未经采购人书面同意，供应商不得擅自复印或用于非本磋商项目所需的其它目的。

2.4.5响应文件的组成（实质性要求）

供应商应按照磋商文件的规定和要求编制响应文件。

响应文件具体内容详见第七章。

2.4.6响应文件格式

一、供应商应按照磋商文件第七章中提供的“响应文件格式”填写相关内容。

二、对于没有格式要求的响应文件由供应商自行编写。

2.4.7响应报价（实质性要求）

一、供应商的报价是供应商响应磋商项目要求的全部工作内容的价格体现，包括供应商完成本项目所需的一切费用。

二、响应文件报价出现前后不一致的，按照磋商文件第六章磋商办法规定予以修正，修正后的报价经供应商通过项目电子化交易系统进行确认，并加盖供应商（法定名称）电子印章，供应商逾时确认的，其响应无效。

2.4.8响应有效期（实质性要求）

响应有效期详见第二章“供应商须知前附表”，响应文件未明确响应有效期或者响应有效期小于“供应商须知前附表”中响应有效期要求的，其响应文件按无效处理。

2.4.9响应文件的制作、签章和加密

一、投标文件应当根据招标文件进行编制，投标人应通过陕西省政府采购网-办事指南-CA及签章服务下载投标（响应）客户端，使用客户端编制投标文件。

二、供应商应按照客户端操作要求，对应磋商文件的每项实质性要求，逐一如实响应；未如实响应或者响应内容不符合磋商文件对应项的要求的，其响应文件作无效处理。

三、供应商完成响应文件编制后，应按照响应文件第1章明确的签章要求，使用互认的证书及签章对响应文件进行电子签章和加密。

四、磋商文件澄清或者修改的内容可能影响响应文件编制的，代理机构将重新发布澄清或者修改后的磋商文件，供应商应重新获取澄清或者修改后的磋商文件，按照澄清或者修改后的磋商文件进行响应文件编制、签章和加密。

2.4.10响应文件的提交（实质性要求）

一、供应商应当在提交首次响应文件截止时间前，通过项目电子化交易系统完成响应文件提交。

二、在提交首次响应文件截止时间后，代理机构不再接受供应商提交响应文件。供应商应充分考虑影响响应文件提交的各种因素，确保在提交首次响应文件截止时间前完成提交。

2.4.11响应文件的补充、修改（实质性要求）

响应文件提交截止时间前，供应商可以补充、修改或者撤回已成功提交的响应文件；对响应文件进行补充、修改的，应当先行撤回已提交的响应文件，补充、修改后重新提交。

供应商响应文件撤回后，视为未提交过响应文件。

2.5开启、资格审查、磋商和确定成交供应商

2.5.1磋商开启程序

一、本项目为竞争性磋商项目。网上开启的开始时间为响应文件提交截止时间。成功提交或解密电子响应文件的供应商不足3家的，不予开启，采购人或代理机构将终止采购活动。

二、磋商开启准备工作

开标/开启前30分钟内，供应商需登录项目电子化交易系统-“供应商开标大厅”-进入开标选择对应项目包组操作签到，签到完成后等待代理机构开标/开启。

三、解密响应文件（实质性要求）

响应文件提交截止时间后，成功提交响应文件的供应商符合响应文件规定数量的，代理机构将启动响应文件解密程序，解密时间为30分钟；供应商应在规定的解密时间内，使用互认的证书及签章通过项目电子化交易系统进行响应文件解密。供应商未在规定的解密时间内完成解密的，按无效响应处理。

开启过程中，各方主体均应遵守互联网有关规定，不得发表与采购活动无关的言论。供应商对开启过程和开启记录有疑义，以及认为采购人或代理机构相关工作人员有需要回避的情形的，及时向工作人员提出询问或者回避申请。采购人或代理机构对供应商提出的询问或者回避申请应当及时处理。

2.5.2查询及使用信用记录

开启结束后，采购人或代理机构根据《关于在政府采购活动中查询及使用信用记录有关问题的通知》（财库〔2016〕125号）的要求，通过“信用中国”网站（www.creditchina.gov.cn）、“中国政府采购网”网站（www.ccgp.gov.cn）等渠道，查询供应商在响应文件提交截止时间前的信用记录并保存信用记录结果网页截图，拒绝列入失信被执行人名单、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单中的供应商参加本项目的采购活动。

两个以上的自然人、法人或者其他组织组成一个联合体，以一个供应商的身份共同参加政府采购活动的，将对所有联合体成员进行信用记录查询，联合体成员存在不良信用记录的，视同联合体存在不良信用记录。

2.5.3资格审查

详见磋商文件第四章。

2.5.4磋商

详见磋商文件第六章。

2.5.5成交通知书

一、采购人或者磋商小组确认成交供应商后，代理机构在陕西省政府采购网发布成交结果公告、通过项目电子化交易系统

发出成交通知书，成交供应商通过项目电子化交易系统获取成交通知书。

二、成交通知书是采购人和成交供应商签订政府采购合同的依据，是合同的有效组成部分。如果出现政府采购法律法规、规章制度规定的成交无效情形的，将以公告形式宣布发出的成交通知书无效，成交通知书将自动失效，并依法重新确定成交供应商或者重新开展采购活动。

三、成交通知书对采购人和成交供应商均具有法律效力。

2.6 签订及履行合同和验收

2.6.1 签订合同

一、采购人应在成交通知书发出之日起三十日内与成交供应商签订采购合同。

二、采购人和成交供应商签订的采购合同不得对磋商文件确定的事项以及成交供应商的响应文件作实质性修改。

2.6.2 合同分包和转包（实质性要求）

2.6.2.1 合同分包

一、供应商根据磋商文件的规定和采购项目的实际情况，拟在成交后将成交项目的非主体、非关键性工作分包的，应当在响应文件中载明分包承担主体，分包承担主体应当具备相应资质条件且不得再次分包。分包供应商履行的分包项目的品牌、规格型号及技术要求等，必须与成交的一致。

二、分包履行合同的部分应当为采购项目的非主体、非关键性工作，不属于成交供应商的主要合同义务。

三、采购合同实行分包履行的，成交供应商就采购项目和分包项目向采购人负责，分包供应商就分包项目承担责任。履行分包项目事项应当具备法定资质规定要求的，分包供应商应当具备相应资质。

四、中小企业依据《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）规定的政策获取政府采购合同后，小型、微型企业不得将合同分包或转包给大型、中型企业，中型企业不得将合同分包或转包给大型企业。

采购包1：不允许合同分包。

2.6.2.2 合同转包

一、严禁成交供应商将本采购项目采购合同转包。本项目所称转包，是指成交供应商签订政府采购合同后，不履行合同约定的责任和义务，将其全部工程转给他人或者将其全部工程肢解以后以分包的名义分别转给其他单位承包的行为。

二、成交供应商转包的，视同拒绝履行政府采购合同，将依法追究法律责任。

2.6.3 合同公告

采购人应当自政府采购合同签订（双方当事人均已完成盖章）之日起2个工作日内，在陕西省政府采购网公告本项目采购合同，但合同中涉及国家秘密、商业秘密的内容除外。

2.6.4 合同备案

采购人自政府采购合同签订（双方当事人均已完成盖章）之日起7个工作日内，将本项目采购合同通过报同级财政部门备案。

2.6.5 采购人增加合同标的的权利

采购合同履行过程中，采购人需要追加与合同标的相同的货物、工程或者服务的，在不改变合同其他条款的前提下，可以与成交供应商协商签订补充合同，但所有补充合同的采购金额不得超过原合同采购金额的百分之十。

2.6.6 履行合同

一、合同一经签订，双方应严格履行合同规定的义务。

二、在合同履行过程中，如发生合同纠纷，合同双方应按照《中华人民共和国民法典》规定及合同条款约定进行处理。

2.6.7 履约验收方案

采购包1：

详见合同条款

2.6.8 资金支付

采购人按财政部门的相关规定及采购合同的约定进行支付。

2.7 纪律要求

2.7.1 磋商活动纪律要求

采购人、代理机构应保证磋商活动在严格保密的情况下进行，采购人、代理机构、供应商和磋商小组成员应当严格遵守政府采购法律法规规章制度和本项目磋商文件以及代理机构现场管理规定，接受采购人委派的监督人员的监督，任何单位和个人不得非法干预和影响磋商过程和结果。

对各供应商的商业秘密，磋商小组成员应予以保密，不得泄露给其他供应商。

2.7.2 供应商不得具有的情形（实质性要求）

供应商参加响应不得有下列情形：

一、有下列情形之一的，视为供应商串通响应：

- （一）不同供应商的响应文件由同一单位或者个人编制；
- （二）不同供应商委托同一单位或者个人办理磋商事宜；
- （三）不同供应商的响应文件载明的项目管理成员或者联系人员为同一人；
- （四）不同供应商的响应文件异常一致或者响应报价呈规律性差异；
- （五）不同供应商的响应文件相互混装。

二、提供虚假材料谋取成交；

三、采取不正当手段诋毁、排挤其他供应商；

四、与采购人或代理机构、其他供应商恶意串通；

五、向采购人或代理机构、磋商小组成员行贿或者提供其他不正当利益；

六、在磋商过程中与采购人或代理机构进行协商磋商；

七、成交后无正当理由拒不与采购人签订政府采购合同；

八、未按照磋商文件确定的事项签订政府采购合同；

九、将政府采购合同转包或者违规分包；

十、提供假冒伪劣产品；

十一、擅自变更、中止或者终止政府采购合同；

十二、拒绝有关部门的监督检查或者向监督检查部门提供虚假情况；

十三、法律法规规定的其他禁止情形。

供应商有上述情形的，按照规定追究法律责任，具有前述一至十一条情形之一的，其响应文件无效，或取消被确认为成交供应商的资格或认定成交无效。

2.7.3 采购人员及相关人员回避要求

政府采购活动中，采购人员及相关人员与供应商有下列利害关系之一的，应当回避：

- （一）参加采购活动前3年内与供应商存在劳动关系；
- （二）参加采购活动前3年内担任供应商的董事、监事；
- （三）参加采购活动前3年内是供应商的控股股东或者实际控制人；
- （四）与供应商的法定代表人或者负责人有夫妻、直系血亲、三代以内旁系血亲或者近姻亲关系；
- （五）与供应商有其他可能影响政府采购活动公平、公正进行的关系。

供应商认为采购人员及相关人员与其他供应商有利害关系的，可以向代理机构书面提出回避申请，并说明理由。代理机构将及时询问被申请回避人员，有利害关系的被申请回避人员应当回避。

2.8 询问、质疑和投诉

一、询问、质疑、投诉的接收和处理严格按照《中华人民共和国政府采购法》《中华人民共和国政府采购法实施条例》《政府采购质疑和投诉办法》等规定办理。

二、供应商询问、质疑的答复主体：

根据委托代理协议约定，供应商对采购文件中采购需求的询问、质疑由 伟江项目管理咨询有限公司 负责答复；供应商对除采购需求外的采购文件的询问、质疑由伟江项目管理咨询有限公司 负责答复；供应商对采购过程、采购结果的询问、质疑由 伟江项目管理咨询有限公司 负责答复。

三、供应商提出的询问，应当明确询问事项，如以书面形式提出的，应由供应商签字并加盖公章。

为提高采购效率，降低社会成本，鼓励询问主体对于不损害国家及社会利益或自身合法权益的问题或情形采用询问方式处理解决（包含但不限于文字错误、标点符号、不影响响应文件的编制的情形）。

四、供应商认为磋商文件、采购过程、中标或者成交结果使自己的权益受到损害的，可以在知道或者应知其权益受到损害之日起7个工作日内，以书面形式向采购人、代理机构提出质疑。供应商应在法定质疑期内一次性提出针对同一采购程序环节的质疑。供应商应知其权益受到损害之日，是指：

（一）对可以质疑的采购文件提出质疑的，为收到采购文件之日或者采购文件公告期限届满之日；

（二）对采购过程提出质疑的，为各采购程序环节结束之日；

（三）对中标或者成交结果提出质疑的，为中标或者成交结果公告期限届满之日。

五、本项目不接受在线提交质疑，供应商通过书面形式线下向采购人或代理机构提交质疑资料。

六、供应商提出质疑时应当准备的资料：

（一）质疑函正本1份；（政府采购供应商质疑函范本详见附件一）

（二）法定代表人或主要负责人授权委托书1份（委托代理人办理质疑事宜的需提供）；

（三）法定代表人或主要负责人身份证复印件1份；

（四）委托代理人身份证复印件1份（委托代理人办理质疑事宜的需提供）；

（五）针对质疑事项必要的证明材料（针对磋商文件提出的质疑，需提交从项目电子化交易系统获取的磋商文件回执单）。

接收质疑函方式：书面形式。

答复主体：代理机构

联系人：马建国

联系电话：029-81111916

地址：西安市新城区龙首北路东段大明宫圣远广场A座8001

邮编：710000

注：根据《中华人民共和国政府采购法》的规定，供应商质疑不得超出磋商文件、采购过程、采购结果的范围。

七、供应商对采购人或代理机构的质疑答复不满意，或者采购人或代理机构未在规定期限内作出答复的，供应商可以在答复期满后15个工作日内向同级财政部门提起投诉。

投诉受理单位：本采购项目同级财政部门。（政府采购供应商投诉书范本详见附件二）

第三章 磋商项目技术、服务、商务及其他要求

（注：带“★”的参数需求为实质性要求，供应商必须响应并满足的参数需求，采购人、采购代理机构应当根据项目实际需求合理设定，并明确具体要求。带“▲”号条款为允许负偏离的参数需求，若未响应或者不满足，将在综合评审中予以扣分处理。）

3.1采购项目概况

本项目为陕西省市场监督管理局商用密码安全性评估项目项目（二次）。

3.2服务内容及服务要求

3.2.1服务内容

采购包1：
采购包预算金额（元）：400,000.00
采购包最高限价（元）：400,000.00
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

序号	标的名称	数量	标的金额 （元）	计量 单位	所属行业	是否核 心产品	是否允许进 口产品	是否属于节 能产品	是否属于环境 标志产品
1	商用密码安 全性评估	1. 0 0	400,000. 00	项	软件和信息技 术服务业	否	否	否	否

3.2.2服务要求

采购包1：
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：商用密码安全性评估

参数性质	序号	技术要求名称	技术参数与性能指标
			<div>第一章项目概述</div> <div>1.1项目名称</div> <div>陕西省市场监督管理局商用密码安全性评估项目。</div> <div>1.2项目单位及实施单位</div> <div>项目单位：陕西省市场监督管理局信息中心 实施单位:陕西省市场监督管理局信息中心</div> <div>1.3等保方案编制单位</div>

1.4项目方案编制依据

政策法规文件：

- 《中华人民共和国网络安全法》
- 《中华人民共和国密码法》
- 《中华人民共和国数据安全法》
- 《中华人民共和国个人信息保护法》

标准规范文件：

- 《商用密码应用安全性评估管理办法》国家密码管理局3号令
- 《信息安全技术 信息系统安全等级保护基本要求》（GB/T 22239-2019）
- 《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）
- 《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）
- 《信息系统密码应用高风险判定指引》
- 《商用密码应用安全性评估量化评估规则》
- 《商用密码应用安全性评估FAQ（第三版）》
- 《商用密码应用安全性评估报告模板（2023版）》

1.5测评目标、测评范围、测评服务内容

测评目标：商用密码安全性评估涉及陕西省市场监督管理局的4个信息系统密码应用合规、正确和有效的、必要的、重要的步骤，通过测评我们将实现如下的短期目标和长期目标。短期目标：审计现有密码技术及管理措施；评估密码应用的合规性、正确性和有效性；及时发现系统存在的密码应用安全隐患；提供科学的评估报告和可操作的整改建议；提高人员密码安全管理及安全防护的意识。长期目标：提升信息系统抵抗威胁和安全攻击的能力，确保信息系统及其承载信息的持续安全；提升信息系统的整体安全水平，保障陕西省市场监督管理局信息系统的机密性、完整性、真实性和不可否认性。

测评范围：

序号	测评系统名称	定级情况
01	陕西省市场监督管理局市场主体综合业务系统	第三级
02	国家企业信用信息公示系统（陕西）-主体监管	第三级
03	陕西省市场监督管理局门户网站系统	第三级
04	陕西省“双随机、一公开”监管工作平台	第三级

测评服务内容：商用密码应用安全性评估的对象是采用密码技术、产品和服务集成建设的网络与信息系统，评估的内容包括密码应用安全的三个方面：合规性、正确性和有效性。

密码测评机构资格要求：根据《中华人民共和国密码法》《商用密码管理条例》等相关法律法规的规定，测评机构应该具备国家密码管理局颁发的“商用密码检测

机构资质证书”。

1.商用密码应用合规性评估

商用密码应用合规性评估是指判定信息系统使用的密码算法、密码协议、密钥管理是否符合法律法规的规定和密码相关国家标准、行业标准的有关要求，使用的密码产品和密码服务是否经过国家密码管理部门核准或由具备资格的机构认证合格。

2.商用密码应用正确性评估

商用密码应用正确性评估是指判定密码算法、密码协议、密钥管理、密码产品和服务使用是否正确，即系统中采用的标准密码算法、协议和密钥管理机制是否按照相应的密码国家和行业标准进行正确的设计和实现，自定义密码协议、密钥管理机制的设计和实现是否正确，安全性是否满足要求，密码保障系统建设或改造过程中密码产品和服务的部署和应用是否正确。

3.商用密码应用有效性评估

商用密码应用有效性评估是指判定信息系统中实现的密码保障系统是否在信息系统运行过程中发挥了实际效用，是否满足了信息系统的安全需求，是否切实解决了信息系统面临的安全问题。

1.6测评模式

完全外包服务。

1.7总投资及资金来源

总投资合计**400000.00**元

资金来源：财政资金（政府部门预算）

第二章项目单位概况

2.1项目单位与职能

省市场监督管理局是省政府直属机构，为正厅级。省市场监督管理局贯彻落实党中央、省委关于市场监督管理工作的方针政策和决策部署，在履行职责过程中坚持和加强党对市场监督管理工作的集中统一领导。主要职责是：

一、负责市场综合监督管理。贯彻执行国家有关市场监督管理的方针、政策和法律、法规、规章，组织起草有关市场监督管理的地方性法规、政府规章草案，制定有关政策、标准，组织实施质量强省战略、食品安全战略和标准化战略，拟订并组织实施有关规划，规范和维护市场秩序，营造诚实守信、公平竞争的市场环境。

二、负责市场主体统一登记注册。组织指导各类企业、农民专业合作社和从事经营活动的单位、个体工商户以及外国（地区）企业常驻代表机构等市场主体的登记注册工作。依法发布市场主体登记注册信息，建立市场主体信息公示和共享机制，依法公示和共享有关信息，加强信用监管，推动市场主体信用体系建设。

三、负责组织和指导市场监管综合执法工作。指导市场监管综合执法队伍整合和建设，推动实行统一的市场监管。组织查处和督办重大违法案件。规范市场监管行政执法行为。

四、负责反垄断统一执法。统筹推进竞争政策实施，指导实施公平竞争审查制度。依据授权负责垄断协议、滥用市场支配地位和滥用行政权力排除、限制竞争等反垄断执法工作。依法对经营者集中行为进行监督，并依据委托开展调查。指导陕西企业在国外的反垄断应诉工作。

五、负责监督管理市场秩序。依法监督管理市场交易、网络商品交易及有关服务的行为。组织指导查处价格收费违法违规、不正当竞争、违法直销、传销、侵犯商标专利知识产权和制售假冒伪劣行为。监督管理直销企业、直销员及其直销活动。指导广告业发展，监督管理广告活动。指导查处无照生产经营和相关无证生产经营行为。承担指导消费者权益保护及其网络体系建设工作，指导陕西省消费者保护组织开展消费维权工作。依法实施合同行政监督管理，组织指导查处合同欺诈等违法行为。管理动产抵押物登记，监督管理拍卖行为。

六、负责宏观质量管理。拟订并实施质量发展的措施办法。统筹质量基础设施建设与应用，会同有关部门组织实施重大工程设备质量监理制度，组织重大质量事故调查，建立并统一实施缺陷产品召回制度，负责产品防伪的相关工作。

七、负责产品质量安全监督管理。管理产品质量安全风险监控和监督抽查工作。建立并组织实施质量分级制度、质量安全追溯制度。组织实施工业产品生产许可管理。负责纤维质量监督工作。

八、负责特种设备安全监督管理。综合管理特种设备安全监察、监督工作。监督检查高耗能特种设备节能标准和锅炉环境保护标准的执行情况。

九、负责食品安全监督管理综合协调。组织制定有关食品安全的措施办法并组织实施。负责食品安全应急体系建设，组织指导重大食品安全事件应急处置和调查处理工作，监督事故查处落实情况。建立健全食品安全重要信息直报制度并组织实施和监督检查。承担省食品安全委员会日常工作。

十、负责食品安全监督管理。推动建立食品生产经营者主体责任的机制，健全食品安全追溯体系。建立覆盖食品生产、流通、消费全过程的监督检查制度和隐患排查治理机制并组织实施，防范区域性、系统性食品安全风险。组织落实国家食品安全检查制度计划、重大整顿治理方案。组织开展食品安全监督抽检、风险监测、核查处置和风险预警、风险交流工作。负责特殊食品备案、生产许可和监督管理工作。负责食盐质量安全监督管理。

十一、负责统一管理计量工作。推行法定计量单位，统筹规划量值传递溯源体系建设。制定并发布地方计量检定规程和技术规范。依法管理商品量、市场计量行为、计量仲裁检定、计量器具和计量技术机构及人员。规范计量数据使用。

十二、负责统一管理标准化工作。组织实施国家标准，负责地方标准相关工作，依法指导和监督团体标准、企业标准相关工作。组织对标准的实施情况开展评估和信息反馈。组织制定并实施标准化激励政策，规范标准化活动。组织参与制定国际标准、采用国际标准工作。承担统一社会信用代码、商品条码和标识管理工作。

十三、负责统一管理认证认可与检验检测工作。依法监督管理认证认可与检验检测工作。组织实施认证认可与检验检测监督管理的措施办法。协调推进检验检测

机构改革，监督规范认证认可及检验检测市场与活动，完善检验检测体系。指导认证认可与检验检测行业发展。

十四、负责市场监督管理科技和信息化建设、新闻宣传工作。按规定承担技术性贸易措施有关工作。

十五、管理省药品监督管理局、省知识产权局。

2.2项目实施单位与职责

陕西省市场监督管理局信息中心紧紧围绕省局全年工作目标任务要求，以服务全省市场监管工作为目标。主要职责为拟定全省市场监督管理系统信息化规划，指导全省各级市场监管部门信息化建设；承担全省市场监管系统平台的建设、运行和升级维护工作；动态监测全省各类媒体发布的广告，整理、汇总监测数据，定期发布监测报告。

第三章需求分析

3.1现状风险分析

3.1.1技术层面

3.1.1.1物理和环境安全

1) 风险分析

机房未使用密码技术对进入机房人员进行身份鉴别，存在非授权人员进入机房环境，对软硬件设备和数据有破坏的风险；

电子门禁系统对机房人员进出记录明文存储在电子门禁系统数据库中，视频监控数据明文存储在磁盘阵列中，未使用密码技术进行存储完整性保护，存在物理进出记录和视频记录遭到非授权篡改，以掩盖非授权人员进出情况的风险。

2) 密码应用需求

在机房部署符合GM/T 0036-2014 标准要求的电子门禁系统，基于SM4密码算法实现进出机房人员进行身份鉴别。在机房部署符合密码相关国家、行业标准要求的国密摄像机及密码模块，从而采用HSMC-SM3或SM2的数字签名算法对门禁进出记录和视频监控数据进行完整性保护。

3.1.1.2网络和通信安全

1) 风险分析

(1) 陕西省市场监督管理局与城市、各网络区域之间使TLS1.2/TLS1.3协议对通信实体进行身份鉴别，对数据传输通道进行机密性和完整性保护，使用的密码算法是不合规的密码算法，存在非法设备从外部接入内部网络，通信数据在信息系统外部被非授权截取、非授权篡改风险。

(2) 陕西省市场监督管理局子系统未使用密码技术建立安全的数据传输通道，实现数据传输机密性和完整性保护，存在通信数据在信息系统外部被非授权截取、非授权篡改风险。

(3) 运维人员通过SSH协议登录堡垒机对系统中的安全设备、安全组件进行集

中管理，未使用合规的密码协议建立安全管理通道，存在搭建的集中管理通道被非授权使用，或传输的管理数据被非授权获取和非授权篡改风险。

2)密码应用需求

应在通信前基于SSL VPN，采用TLCP协议和配置ECC-SM4-SM3密码套件，对通信双方进行身份认证，使用密码技术的机密性和真实性功能来实现防截获、防假冒和防重用，保证传输过程中鉴别信息的机密性和网络设备实体身份的真实性；应使用密码技术的完整性功能来保证网络边界和系统资源访问控制信息的完整性；应采用密码技术保证通信过程中数据的完整性；应采用密码技术保证通信过程中敏感信息数据字段或整个报文的机密性；应采用密码技术建立安全的信息传输通道，对网络中的安全设备或安全组件进行集中管理。

3.1.1.3设备和计算安全

1) 风险分析

设备管理员用户在政务外网通过浏览器，使用用户名口令登录平台设备，未使用密码技术对管理员登录进行身份鉴别，未使用合规的密码技术对管理员登录身份鉴别信息进行传输机密性保护，存在设备被非授权人员登录、身份鉴别数据被非授权获取或非授权使用等风险。

系统应用服务器中所有重要程序或文件在生成时未使用密码技术进行完整性和机密性保护，使用或读取这些程序和文件时，未对其进行完整性校验，存在重要程序或文件被非授权篡改、来源不可信风险，被窃取风险；

平台应用服务器、数据库服务器等设备日志均明文存储，未使用密码技术进行完整性和机密性保护，存在设备日志记录被非授权篡改风险。

2) 密码应用需求

在堡垒机前面部署经过认证且等级符合要求的SSL VPN网关，运维人员不能绕过VPN，访问到堡垒机，再通过堡垒机使用SSH2.0协议运维应用服务器和数据库服务器。

在应用服务区部署服务器密码机，应用系统中所有重要程序或文件在生成时通过调用服务器密码机使用SM2数字签名技术进行完整性保护；调用服务器密码机接口使用HMAC-SM3对应用服务器、数据库服务器等设备日志进行完整性保护。

在应用服务区部署数据库加密产品与文档加密产品，对数据库以及业务系统中涉及的重要业务数据，审计数据，鉴别数据，个人信息等进行分级分类保护，并进行加密保护，防止数据泄露风险。

3.1.1.4应用和数据安全

1) 风险分析

信息系统用户通过PC端浏览器使用用户名口令进行登录身份鉴别；均未使用密码技术对登录用户进行身份鉴别，存在应用被非授权人员登录风险。

信息系统用户身份鉴别信息、重要业务数据，个人信息数据等均为明文传输、存储，未使用密码技术进行传输、存储的机密性、完整性保护，存在身份鉴别数据、业务数据被窃取和非授权篡改风险。

2) 密码应用需求

使用USBKey以及签名验签服务器，基于SM2数字证书，完成挑战-响应协议，实现应用用户的身份鉴别。

在业务服务区部署符合密码相关国家、行业标准的服务器密码机，并部署通过

国密认证的数据库加密产品，使用SM4-CBC和HAMC-SM3，实现数据库内户身份鉴别信息、重要业务数据，个人信息数据等存储的机密性和完整性，实现对结构化数据的安全保护。

在业务服务区部署符合密码相关国家、行业标准的服务器密码机，并部署通过国密认证的文档加密产品，使用SM4-CBC和HAMC-SM3，实现应用系统中非机构化数据的机密性和完整性安全保障。重要针对数据包括用户身份鉴别信息、重要业务数据，个人信息数据等。

3.1.2管理层面

1) 风险分析

系统上线前，未开展密码应用安全性评估，未依据GB/T 39786-2021标准中的安全管理要求制定密码相关管理制度，不利于在信息系统中落实密码相关国家政策要求，发挥密码在信息系统安全中的基础支撑作用。

2) 风险控制需求分析

依据GB/T 39786-2021标准，制定信息系统密码应用建设方案，并委托密评机构对密码应用建设方案进行评估，评估通过后，建设密码保障系统，制定密码相关的管理制度，信息系统密码应用建设完成后，依据密码应用建设方案对信息系统进行密码应用安全性评估，评估通过后对系统进行逐步分批改造，逐步上线运行。

3.2需求分析

表1信息系统密码应用需求分析表

安全 层面	指标要求	系统密码应用需求	不适用说明
物理 和环 境安 全	身份鉴别	对人员物理访问进行身份鉴别，确保中心机房进入人员身份的真实性	无
	电子门禁记录数	对电子门禁系统中的中心机房人员出入记录进行存储完整性保护，防止被非授权篡改。	无
	据存储完整性		
	视频记录数据存	对视频监控系统中的中心机房内外监控音视频记录进行存储完整性保护，防止被非授权篡改。	无
	储完整性		
网络 和通 信安	密码服务	信息系统使用的密码服务应符合法律法规的相关要求。	无
	密码产品	采用的密码产品，应达到GB/T 37092二级及以上安全要求。	无
	身份鉴别	应对接入的实体身份的真实性进行鉴别，防止假冒实体的接入。	无
	通信数据完整性	应对接入网络信道的通信数据的完整性进行保护，防止数据被非授权篡改。	无
	通过程中重要数据的机密性	应对接入网络信道的通信重要数据的机密性进行保护，防止重要业务数据的窃取和泄露。	无
网络 和通 信安	网络边界访问控制信息完整性	对网络接入区边界设备访问控制信息进行完整性保护。	无

				全	设备接入认证	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。	系统中不涉及设备接入认证
					密码服务	信息系统使用的密码服务应符合法律法规的相关要求。	无
					密码产品	采用的密码产品,应达到GB/T 37092 二级及以上安全要求。	无
				设备和计算安全	设备登录身份鉴别	应对登录设备(主要包括服务器、网络设备、安全设备、安全组件)的用户身份真实性进行鉴别,防止终端计算机的设备冒用和系统管理的账号冒用。	无
					远程管理通道安全	应对设备远程登录管理建立安全的集中管理通道,对网络设备、服务器、安全设备、安全组件进行集中管理,防止集中管理通道被非授权使用,防止传输的管理数据被非授权获取和非授权篡改。	无
					系统资源访问控制信息完整性	对系统管理人员通过堡垒机对系统资源(网络设备、访问控制安全设备)进行配置管理的操作信息进行完整性保护,对管理人员的身份鉴别信息进行机密性保护,防止传输的管理数据被非授权篡改。	无
					重要信息资源安全标记完整性	不适用	系统中不涉及重要信息资源安全标记
					日志记录完整性	对系统设备的日志记录进行完整性保护。	无
					重要可执行程序完整性、重要可执行程序来源真实性	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	无
					密码服务	信息系统使用的密码服务应符合法律法规的相关要求。	
					密码产品	采用的密码产品,应达到GB/T 37092 二级及以上安全要求。	
				应用和数	应用系统身份鉴别	应对访问应用系统的用户身份真实性进行鉴别,防止假冒人员登录。	无
					应用系统访问控制信息完整性	对应用系统访问权限控制列表、数据库表访问控制信息进行完整性保护,防止被非授权篡改。	无
					应用系统中重要信息资源安全标记完整性	不适用	应用系统不涉及重要信息资源安全标记
					重要数据传输机密性	应对客户端计算机到应用系统之间传输的重要数据(包括身份鉴别数据、重要业务数据)进行机密性保护,防止重要数据被非授权泄露。	无

数据安全	重要数据存储机密性	应对应用系统服务器、存储集群上存储的重要数据（身份鉴别数据、重要业务数据、系统日志等）进行机密性保护，防范被非授权获取后的数据泄漏。	无
	重要数据传输完整性	宜对在客户端到应用系统的重要数据（身份鉴别数据、重要业务数据等）进行完整性保护，防止被非授权篡改。	无
	重要数据存储完整性	对应用系统服务器、存储集群上存储的重要数据（身份鉴别数据、重要业务数据、系统日志审计数据等）进行完整性保护，防止被非授权篡改。	无
	不可否认性	对可能涉及法律责任认定的行为进行数字签名。	无
	密码服务	信息系统使用的密码服务应符合法律法规的相关要求。	
	密码产品	采用的密码产品，应达到GB/T 37092 二级及以上安全要求。	
安全管理	管理制度	应制定密码应用安全管理制度、密钥管理规则，建立操作规程；应在管理策略中明确对密码安全管理制度定期进行修改、明确制度发布流程和制度执行过程中的记录留存要求。	无
	人员管理	应建立密码应用岗位责任制度、建立上岗人员培训制度、对上岗人员针对性地开展密码相关法律法规和密码管理制度培训、做到持证上岗，并定期对密码工作人员进行考核、建立密码工作人员保密制度和调离制度。	无
	建设运行	应制定密码应用方案、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。	无
	应急处置	应制定密码应用安全性事件应急响应预案，做好应急资源准备，明确密码应用安全事件处置的流程和要求、明确向属地密码管理部门上报事件发生情况及处置情况要求，明确对应急预案的培训和演练要求。	无

第四章测评对象与方法

4.1 测评指标的选择

商用密码安全性评估根据已经了解到的信息系统定级结果，从《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）和《信息安全技术 信息系统密码应用测评要求》（GB/T 43207-2023）中选择相应等级的安全要求作为测评指标。

4.2 测评对象的确定

4.2.1 测评对象确定原则

测评对象的选取应遵从以下原则：

- 1) 恰当性，选择的设备、软件系统等应能满足相应等级的测评强度要求；
- 2) 重要性，应抽查对被测系统来说重要的服务器、数据库和网络设备等；
- 3) 安全性，应抽查对外暴露的网络边界；
- 4) 共享性，应抽查共享设备和数据交换平台/设备；
- 5) 代表性，抽查应尽量覆盖系统各种设备类型、操作系统类型、数据库系统类型和应用系统类型。

4.2.2测评对象确定方法

首先，确定测评的系统边界范围。实际测试过程中，被测系统可能是一个很大系统的子系统，测评人员应根据实际情况，确定系统测评的范围，与被测系统不相关的系统不应纳入进来；

其次，分析被测系统边界内的物理环境、网络拓扑结构和外部边界连接情况、业务应用系统、以及与业务应用系统相关的重要的计算机硬件设备（包括服务器设备、客户端设备、存储器等）、网络硬件设备（包括交换机、路由器、各种适配器等）和密码设备（IC卡、智能密码钥匙、密码机、SSL VPN、IPSec VPN等）；

最后，依据《信息安全技术 信息系统密码应用测评要求》（GB/T 43207-2023），根据业务应用系统的业务种类及重要性、业务流程、业务数据重要性、业务安全保护等级、商用密码应用情况等，分析确定测评对象。

4.3测评对象的选择结果（样表）

4.3.1存储设备

编号	名称	设备厂商	型号	数量	操作系统	资产价值	备注
----	----	------	----	----	------	------	----

4.3.2应用系统

编号	系统名称	URL	资产价值	备注（简要说明系统业务功能）
----	------	-----	------	----------------

4.3.3安全设备

编号	设备名称	产品型号	设备厂商	资产价值	备注（简要说明系统业务功能）
----	------	------	------	------	----------------

4.3.4密码产品

编号	密码产品名称	密码产品功能描述	商用密码产品认证证书编号	涉及的密码算法	数量	资产价值	备注
----	--------	----------	--------------	---------	----	------	----

4.3.5关键数据

编号	数据类别	涉及密码应用	安全防护需求	资产价值
----	------	--------	--------	------

4.3.6安全相关人员

编号	姓名	岗位/角色	联系方式
----	----	-------	------

4.3.7安全管理文档

编号	文档名称	主要内容
----	------	------

4.3.8机房

编号	机房名称	位置	备注
----	------	----	----

4.4测评方法

本次测评现场实施过程中将综合采用访谈、文档审查、实地查看、配置检查和工具测试等五种测评方法。

商用密码应用安全性评估的测评方法如下：

1）访谈

访谈是测评人员通过与本次用户单位涉及的信息系统有关人员进行交流、讨论等活动，获取证据以证明本次用户单位涉及的信息系统商用密码应用是否有效的一种方法。

测评访谈的对象包括系统负责人、安全主管、物理安全负责人、系统管理员、安全管理员、安全审计员和密钥管理员等。

测评访谈的适用情况包括：

（1）对于总体测评要求，使用访谈方法了解本次用户单位涉及的信息系统密码应用的全局性信息，包括采用的密码算法、密码技术、密码产品和密码服务；

（2）对于技术要求，使用访谈方法了解本次用户单位涉及的信息系统密码应用的方向/策略性信息，包括在物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全方面采用的密码技术及实现机制；

（3）对于密钥管理要求，使用访谈方法了解本次用户单位涉及的信息系统密钥管理的方向/策略性和过程性信息，包括密钥生命周期管理机制及安全措施；

（4）对于安全管理要求，使用访谈方法了解本次用户单位涉及的信息系统密码安全管理的具体情况，包括制度建设及落实、人员管理、实施管理和应急管理的方方面面。

2）文档审查

文档审查是测评人员通过审阅与本次用户单位涉及的信息系统有关的设计文档、技术文档、资质证书及安全管理类文档，获取证据以证明本次用户单位涉及的信息系统商用密码应用是否合规、有效的一种方法。

本次测评文档审查的对象包括本次用户单位涉及的信息系统各类设计、技术文档、商用密码产品型号证书、安全管理体系文件等。

本次测评文档审查的适用情况包括：

（1）对于总体测评要求，审查各类设计、技术文档，了解本次用户单位涉及的信息系统密码应用的信息，确认密码算法、密码技术、密码产品和密码服务的合规性；

（2）对于技术要求，审查各类设计、技术文档，了解本次用户单位涉及的信息

系统在物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全方面采用的密码技术及实现机制，确认相关密码算法、密码协议和密码产品是否合规；

（3）对于密钥管理要求，审查密钥管理制度、密钥管理过程记录及相关技术文档，了解本次用户单位涉及的信息系统密钥生命周期管理机制及安全措施；

（4）对于安全管理要求，审查密码管理制度体系文档，了解本次用户单位涉及的信息系统密码安全管理的具体情况。

3）实地查看

实地查看是测评人员通过对测评对象进行现场观察、查验，获取证据以证明本次用户单位涉及的信息系统商用密码应用是否合规、有效的一种方法。

本次测评实地查看的对象包括密码系统、信息系统机房等。

本次测评实地查看的适用情况包括：

（1）对于总体测评要求，使用实地查看方法了解本次用户单位涉及的信息系统密码应用的全局性信息，包括密码算法、密码技术的实现方式、密码产品部署以及使用的密码服务等；

（2）对于技术要求，使用实地查看方法了解本次用户单位涉及的信息系统的物理安全保障情况、网络平台及设备部署；

（3）对于安全管理测评，使用实地查看方法了解岗位责任制的落实情况，确认设备与系统的管理和使用账号是否多人共用；

（4）对于密钥管理要求，一般不采用实地查看方法。

4）配置检查

配置检查是测评人员通过上机验证，获取证据以证明本次用户单位涉及的信息系统商用密码应用是否正确、有效的一种方法。

本次测评配置检查的对象包括各类设备、安全配置等。

本次测评配置检查的适用情况包括：

（1）对于总体测评要求，使用配置检查的方法确认各类密码产品所使用的密码算法；

（2）对于技术要求和密码管理要求，使用配置检查的方法确认具体的机制配置和运行实现；

（3）对管理要求，一般不采用配置检查方法。

5）工具测试

工具测试是测评人员通过对测评对象按照预定的方法/工具使其产生特定的行为等活动，查看、分析输出结果，获取证据以证明本次用户单位涉及的信息系统商用密码应用密码措施是否有效的一种方法。

测评工具测试的对象包括机制和设备等。

测评工具测试的适用情况包括：

（1）对于技术要求，验证本次用户单位涉及的信息系统身份认证、数据传输保护、敏感数据安全存储等密码安全机制或运行的正确性、有效性。

（2）对于管理要求，一般不采用工具测试方法。

第五章测评内容与测评实施

5.1 测评流程

测评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应贯穿整个测评过程。测评过程具体如图1所示。

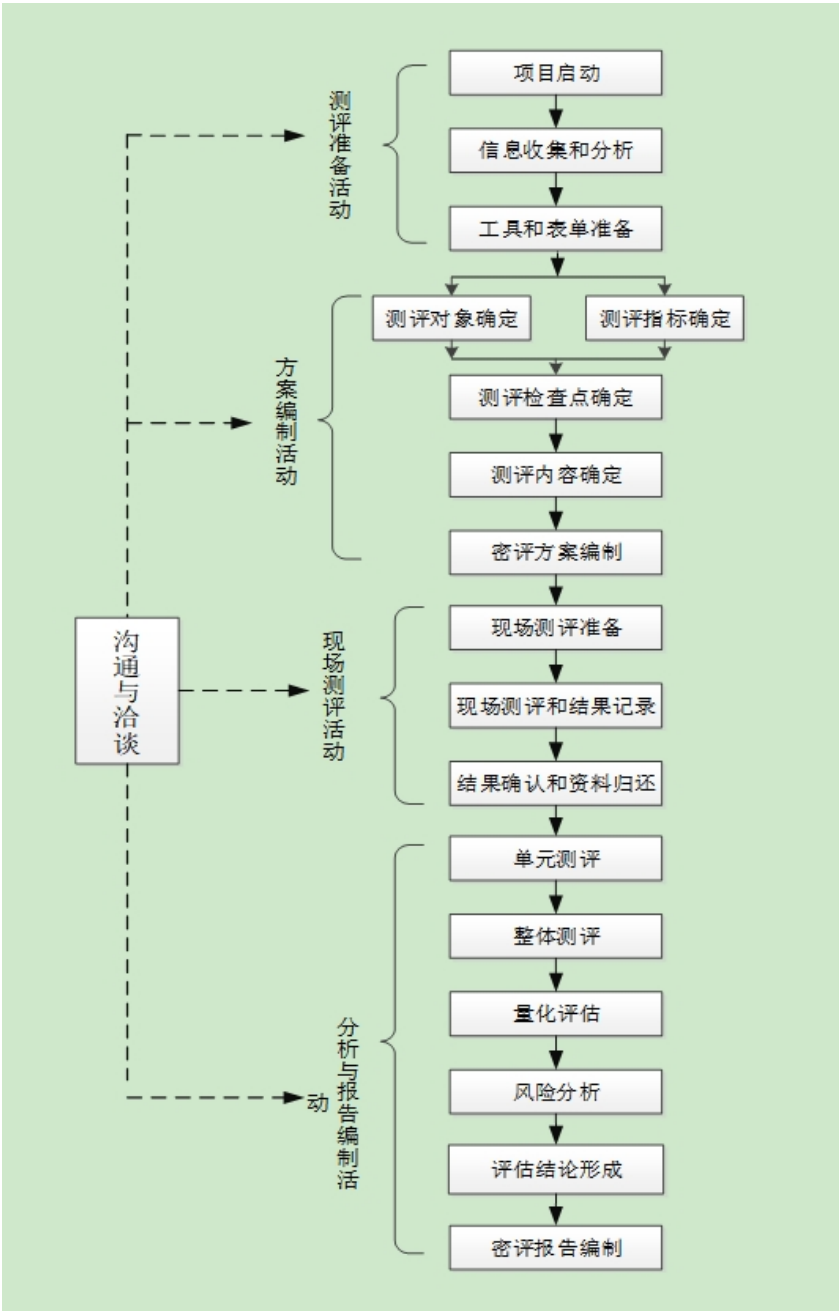


图1 测评过程流程图

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。

现场测评活动：本活动是开展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，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《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）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。

5.2测评指标和测评方法

参照《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）和《信息安全技术 信息系统密码应用测评要求》（GB/T 43207-2023），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。

5.2.1总体测评

5.2.1.1密码算法测评

密码算法测评将通过访谈、文档审查、实地查看和配置检查的方式测评本系统中使用的密码算法的合规性。

在内容上，密码算法测评实施过程涉及以下测评单元。

序号	测评单元	测评指标	测评方法
1	密码算法合规性检查	信息系统中使用的密码算法应当符合法律、法规的规定和密码相关国家标准、行业标准的有关要求。	1、访谈系统管理员，查看技术文档，并实地查看密码系统，了解系统使用的算法名称、用途、何处使用、执行设备及其实现方式（软件、硬件或固件）； 2、通过文档审查、配置检查，核查系统使用的密码算法是否以国家标准或行业标准形式发布，或取得国家密码管理部门同意其使用的证明文件。

5.2.1.2密码技术测评

密码技术测评将通过访谈、文档审查、实地查看和配置检查的方式测评本系统中使用的密码技术的合规性。

在内容上，密码技术测评实施过程涉及以下测评单元。

序号	测评单元	测评指标	测评方法
1	密码技术合规性检查	信息系统中使用的密码技术应遵循密码相关国家标准和行业标准。	1、访谈系统管理员，查看技术文档，并实地查看密码系统，了解系统使用的密码技术； 2、核查系统使用的密码技术是否符合相关国家标准或行业标准。

5.2.1.3密码产品测评

密码产品测评将通过访谈、文档审查和实地查看的方式测评本系统中使用的密码产品的合规性，如服务器密码机、签名验签服务器、时间戳服务器、SSL VPN、IPSec VPN、智能密码钥匙、电子签章系统等。

在内容上，密码产品测评实施过程涉及以下测评单元。

序号	测评单元	测评指标	测评方法
----	------	------	------

1	密码产品 合规性检查	信息系统中使用的密码产品与密码模块应通过国家密码管理部门核准。	1、访谈系统管理员，查看技术文档，并实地查看密码系统，了解系统使用的密码产品和密码模块； 2、核查密码产品和密码模块是否获得国家密码管理部门颁发的密码产品型号证书，或国家密码管理部门认可的商用密码测评机构出具的合格检测报告。
---	---------------	---------------------------------	---

5.2.1.4 密码服务测评

密码服务测评将通过访谈、文档审查和实地查看的方式测评本系统中使用的密码服务的合规性。

在内容上，密码服务测评实施过程涉及以下测评单元。

序号	测评单元	测评指标	测评方法
1	密码服务合规性检查	信息系统中使用的密码服务应通过国家密码管理部门许可。	1、访谈系统管理员，查看技术文档，并实地查看密码系统，了解系统使用的密码服务； 2、核查密码服务是否获得密码服务许可证，核查密码服务提供方是否为商用密码产品生产单位、是否具有相应的密码应用研发服务能力。

5.2.2 密码技术应用测评

5.2.2.1 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，主要涉及信息系统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。

序号	测评指标	测评项	测评方法
1	身份鉴别	应使用密码技术的真实性功能来保护物理访问控制身份鉴别信息，保证重要区域进入人员身份的真实性。	1、访谈物理安全负责人，并查看相关技术文档，了解信息系统机房电子门禁系统的身份鉴别措施； 2、核查电子门禁系统是否具有商用密码产品型号证书； 3、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。 4、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	电子门禁记录数据完整性	应使用密码技术的完整性功能来保证电子门禁系统进出记录的完整性。	<p>1、访谈物理安全负责人，并查看相关技术文档，了解信息系统机房电子门禁系统进出记录的完整性保护措施；</p> <p>2、核查电子门禁系统是否具有商用密码产品型号证书；</p> <p>3、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；</p> <p>4、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。</p>
3	视频记录数据完整性	应使用密码技术的完整性功能来保证视频监控音像记录的完整性。	<p>1、访谈物理安全负责人，并查看相关技术文档，了解信息系统机房视频监控系统视频监控音像记录数据的完整性保护技术及实现机制；</p> <p>2、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型号证书，密码算法、密码协议是否符合相关密码标准；</p> <p>3、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。</p>
4	密码产品	宜采用符合GM/T 0028的二级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理。	<p>1、访谈系统管理员，并查阅相关技术文档，了解系统的密码实现机制；</p> <p>2、查看系统中用于密码运算和密钥管理的密码模块是否为二级及以上、是否符合GM/T 0028，硬件密码产品是否通过国家密码管理部门核准。</p>

5.2.2.2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，主要涉及网络设备、安全设备集中管理、以及业务应用系统客户端与服务端之间的通信。

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。

序号	测评单元	测评指标	测评方法
----	------	------	------

1	身份鉴别	应在通信前基于密码技术对通信双方进行身份认证，使用密码技术的机密性和真实性功能来实现防截获、防假冒和防重用，保证传输过程中鉴别信息的机密性和网络设备实体身份的真实性。	<p>1、查看设计文档中业务应用系统客户端与服务端之间的通信双方身份认证采用的密码技术及实现机制；</p> <p>2、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 0009-2023）等有关密码国家标准和行业标准；</p> <p>3、查看身份鉴别采用的密码设备是否获得国家密码管理部门颁发的商用密码产品型号证书；</p> <p>4、如果采用IPSEC/SSL VPN等密码产品进行身份鉴别，使用Wireshark验证传输过程中鉴别信息机密性的有效性。</p>
2	访问控制信息完整性	应使用密码技术的完整性功能来保证网络边界和系统资源访问控制信息的完整性。	<p>1、查看系统是否使用以及使用何种密码技术对网络边界和系统资源访问控制信息进行完整性保护；</p> <p>2、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国家密码管理部门颁发的商用密码产品型号证书。</p>
3	通信数据完整性	应采用密码技术保证通信过程中数据的完整性。	<p>1、查看技术文档中业务应用系统客户端与服务端之间等通信过程中数据采用的完整性保护技术及实现机制；</p> <p>2、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；</p> <p>3、使用Wireshark捕获并分析通信数据，验证通信数据完整性保护的有效性；</p>
4	通信数据机密性	应采用密码技术保证通信过程中敏感信息数据字段或整个报文的机密性。	<p>1、查看技术文档中业务应用系统客户端与服务端之间等网络通信中敏感数据采用的机密性保护技术及实现机制；</p> <p>2、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；</p> <p>3、使用Wireshark捕获并分析通信数据，验证通信数据机密性保护的有效性。</p>
5	设备接入认证	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。	不适用。

6	密码产品	宜采用符合GM/T 0028的二级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理。	1、访谈系统管理员，并查阅相关技术文档，了解系统的密码实现机制； 2、查看系统中用于密码运算和密钥管理的密码模块是否为二级及以上、是否符合GM/T 0028，硬件密码产品是否通过国家密码管理部门核准。
---	------	--	---

5.2.2.3 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。

序号	测评单元	测评指标	测评方法
1	身份鉴别	应使用密码技术对登录的用户进行身份标识和鉴别，身份标识具有唯一性，鉴别信息具有复杂度要求并定期更换。	1、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； 2、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有效性； 3、核查主机用户身份鉴别过程中使用的密码产品是否获得国家密码管理部门颁发的商用密码产品型号证书； 4、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； 5、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	远程管理管理通道安全	在远程管理时，应使用密码技术的机密性功能来实现鉴别信息的防窃听。	1、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； 2、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国家密码管理部门颁发的密码产品型号证书，密码算法是否符合法规和密码相关标准的要求； 3、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保护技术的有效性。

3	访问控制 信息完整性	应使用密码技术的完整性功能来保证系统资源访问控制信息的完整性。	<p>1、查看相关技术文档，访谈系统管理员，了解设备访问控制信息完整性保护密码技术及实现机制；</p> <p>2、查看系统是否使用以及使用何种密码技术对系统资源访问控制信息进行完整性保护；</p> <p>3、查看是否使用国家密码管理部门认可的密码算法；密码设备是否获得国家密码管理部门颁发的商用密码产品型号证书。</p>
4	安全标记的完整性	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。	不适用。
5	日志记录完整性	应使用密码技术的完整性功能来对日志记录进行完整性保护。	<p>1、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；</p> <p>2、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。</p>
6	重要可执行程序完整性、重要可执行程序来源真实性	应采用可信计算技术建立从系统到应用的信任链，实现系统运行过程中重要程序或文件完整性保护。	<p>1、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；</p> <p>2、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；</p> <p>3、核查重要程序或文件完整性所使用的密码产品是否获得国家密码管理部门颁发的商用密码产品型号证书；</p> <p>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；</p> <p>4、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。</p>
7	密码产品	宜采用符合GM/T 0028的二级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理。	<p>1、访谈系统管理员，并查阅相关技术文档，了解系统的密码实现机制；</p> <p>2、查看系统中用于密码运算和密钥管理的密码模块是否为二级及以上、是否符合GM/T 0028，硬件密码产品是否通过国家密码管理部门核准。</p>

5.2.2.4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，主要涉及应用系统鉴别数据、业务

数据、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。

序号	测评单元	测评指标	测评方法
1	身份鉴别	应使用密码技术对登录的用户进行身份标识和鉴别，实现身份鉴别信息的防截获、防假冒和防重用，保证应用系统用户身份的真实性。	1、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； 2、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保护技术的有效性； 3、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国家密码管理部门颁发的商用密码产品型号证书。
2	访问控制信息完整新	应使用密码技术的完整性功能来保证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信息的完整性。	1、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； 2、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； 3、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；密码产品是否获得国家密码管理部门颁发的商用密码产品型号证书；相关密码功能是否正确有效。
3	重要信息资源安全标记的完整性	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。	不适用。
4	数据传输机密性	应采用密码技术保证重要数据在传输过程中的机密性，包括但不限于鉴别数据、重要业务数据和重要用户信息等。	1、查看相关技术文档，了解应用系统中鉴别数据、业务数据、配置数据等重要数据在传输过程中的机密性保护技术及实现机制； 2、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； 3、查看所使用的密码算法、身份鉴别协议是否符合有关密码国家标准和行业标准。

5	数据存储机密性	应采用密码技术保证重要数据在存储过程中的机密性，包括但不限于鉴别数据、重要业务数据和重要用户信息等。	<p>1、查看相关技术文档，了解应用系统中鉴别数据、业务数据、配置数据、审计数据等重要数据的机密性保护技术及实现机制；</p> <p>2、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型号证书；</p> <p>3、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；</p> <p>4、查看所使用的密码算法、身份鉴别协议是否符合有关密码国家标准和行业标准。</p>
6	数据传输完整性	应采用密码技术保证重要数据在传输过程中的完整性，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用户信息等。	<p>1、查看相关技术文档，了解应用系统中鉴别数据、业务数据、配置数据等重要数据在传输过程中的完整性保护技术及实现机制；</p> <p>2、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；</p> <p>3、查看所使用的密码算法、身份鉴别协议是否符合有关密码国家标准和行业标准。</p>
7	数据存储完整性	应采用密码技术保证重要数据在存储过程中的完整性，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用户信息、重要可执行程序等。	<p>1、查看相关技术文档，了解应用系统中鉴别数据、业务数据、配置数据、审计数据等重要数据存储过程中的完整性保护技术及实现机制；</p> <p>2、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型号证书；</p> <p>3、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；</p> <p>4、查看所使用的密码算法、身份鉴别协议是否符合有关密码国家标准和行业标准。</p>
8	行为的不可否认性	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。	不适用。

9	密码产品	宜采用符合GM/T 0028的二级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理。	1、访谈系统管理员，并查阅相关技术文档，了解应用系统的密码实现机制； 2、查看系统中用于密码运算和密钥管理的密码模块是否为二级及以上、是否符合GM/T 0028，硬件密码产品是否通过国家密码管理部门核准。
---	------	--	---

5.2.3 密钥管理测评

密钥管理测评将通过访谈、文档审查、配置核查的方式测评本系统涉及的密钥管理体系及安全机制；对于已经取得国家密码管理部门型号认可的密码产品、模块等，不对产品/模块自身的密钥管理体系和安全机制进行测评。

密钥管理测评主要涉及数字证书对应公私钥、用于身份认证和操作日志签名验签的签名密钥对、用于数据加解密的加密密钥对、用于通信保护的会话密钥等生命周期管理以及密钥管理员和相关密钥管理制度等。

在内容上，密钥管理层面测评实施过程涉及以下各测评单元。

序号	测评单元	测评指标	测评方法
1	生成	密钥生成使用的随机数应符合GM/T 0005要求，密钥应在符合GM/T 0028的密码模块中产生；密钥应在密码模块内部产生，不得以明文方式出现在密码模块之外；应具备检查和剔除弱密钥的能力。	1、结合技术文档，访谈密钥管理员，了解系统在密钥生成过程中所使用的随机数生成器是否是经过了国家密码管理部门批准的硬件物理噪声源随机数生成器； 查看系统内随机数生成器的运行状态，确认其功能是否有效； 2、结合技术文档，访谈密钥管理员，了解系统内部所使用的密钥何时生成、以何种形式存在于系统之中，确认密钥是否会以明文形式存在于密码模块之外； 3、结合技术文档，访谈密钥管理员，了解受检系统是否具备检查并剔除弱密钥的能力；如果系统具备此能力，则访谈了解系统使用了何种技术实现此功能。

2	存储	<p>密钥应加密存储，并采取严格的安全防护措施，防止密钥被非法获取；密钥加密密钥应存储在符合GM/T 0028的二级及以上密码模块中。</p>	<p>1、结合技术文档，访谈密钥管理员，了解系统内部所有密钥是否均以密文形式进行存储，了解系统使用了何种密码算法对受保护密钥进行了加密处理，且相关加密算法是否经过了国家密码管理部门认可；</p> <p>2、结合技术文档，访谈密钥管理员，了解密钥加密密钥的分配、管理、使用及存储机制，了解相关的技术实施细节；</p> <p>3、结合技术文档，访谈密钥管理员，了解系统内部是否具备完善的密钥访问权限控制机制，以保护明文密钥及密文密钥不被非法获取、篡改或使用。</p>
3	分发	<p>密钥分发应采取身份鉴别、数据完整性、数据机密性等安全措施，应能够抗截取、假冒、篡改、重放等攻击，保证密钥的安全性。</p>	<p>1、结合技术文档，访谈密钥管理员，了解系统内部是否具有较为完善的密钥分发机制，了解系统采用了何种密钥分发方式（离线分发方式、在线分发方式、混合分发方式）；</p> <p>2、访谈密钥管理员，了解系统是否具有完善的身份鉴别机制，以保护相关密钥不被非法获取、使用或修改；</p> <p>3、如果系统中部分密钥以离线方式分发给了不同的密钥使用者，则访谈密钥管理员，了解在密码传递过程中，系统使用了哪些密码技术对密钥进行了处理，以保证其机密性、完整性与真实性，且系统所使用的密码算法或专用密码存储设备是否经过了国家密码管理部门认可；</p> <p>4、如果系统中部分密钥以在线方式分发给了密钥使用者，则访谈密钥管理员，了解在密码传递过程中，系统使用了何种密码技术对密钥进行了处理，以保证机密性、完整性与真实性，且相关密钥算法、安全协议、安全设备是否经了国家密码管理部门认可；</p> <p>5、如果系统使用了混合方式将不同类型的密钥分发给了不同的密钥使用者，则访谈密钥管理员，了解系统在何时使用了在线方式对密钥进行了分发，且在密钥分发期间系统使用了哪些专用网络安全设备、专用安全存储设备，且相关设备、算法或协议是否经过了国家密码管理部门认可。</p>

4	导入与导出	应采取安全措施，防止密钥导入导出时被非法获取或篡改、并保证密钥的正确性。	<p>1、结合技术文档，访谈密钥管理员，了解在密钥导入、导出过程中系统采用了何种安全措施来保证此操作的安全性及密钥的正确性；</p> <p>2、结合技术文档，访谈密钥管理员，了解在密钥导入、导出过程中系统是否采用了密钥拆分的方法将密钥拆分成若干的密钥片段分发不同的密钥携带者，从而实现安全的密钥导出操作；了解被导出的密钥片段是否经过了加密处理，以密文形式存在于各传输载体之中，且相关的密钥加密算法是否经过了国家密码管理部门认可；</p> <p>3、访谈密钥管理员，了解在密钥导入、导出过程中系统是否使用了专用密码存储设备存储，查看存储设备是否经过了国家密码管理部门认可；</p> <p>4、访谈密钥管理员，了解在密钥导入、导出过程中系统是否可保证相关密码服务中不被中断。</p>
5	使用	密钥应明确用途，并按用途正确使用；对于公钥密码体制，在使用公钥之前应对其进行验证；应有安全措施防止密钥的泄露和替换；密钥泄露时，应停止使用，并启动相应的应急处理和响应措施。应按照密钥更换周期要求更换密钥；应采取有效的安全措施，保证密钥更换时的安全性。	<p>1、结合技术文档，访谈密钥管理员，了解系统内部是否具有严格的密钥使用管理机制，以保证所有密钥均具有明确的用途且各类密钥均可被正确地使用、管理；</p> <p>2、访谈密钥管理员，了解系统是否具有公钥认证机制，以鉴别公钥的真实性与完整性，相应公钥密码算法是否符合法规和密码相关标准的要求；</p> <p>3、访谈密钥管理员，了解系统采用了何种安全措施来防止密钥被泄露或替换，是否使用了密码算法，且相关算法是否符合法规和密码相关标准的要求；</p> <p>4、访谈密钥管理员，了解系统是否可定期更换密钥，了解详细的密钥更换处理流程；对测试用户进行密钥更换操作，查看密钥更换过程是否安全；</p> <p>5、访谈密钥管理员，了解当密钥泄露时系统是否具备应急处理和响应措施。</p>

6	备份与恢复	应制定明确的密钥备份策略，采用安全可靠的密钥备份恢复机制，对密钥进行备份或恢复；密钥备份或恢复应进行记录，并生成审计信息；审计信息包括备份或恢复的主体、备份或恢复的时间等。	<p>1、结合技术文档，访谈密钥管理员，了解系统内部是否具有较为完善的密钥恢复备份机制，了解系统中密钥的备份策略，备份密码的存储方式、存储位置技术细节内容；</p> <p>2、访谈密钥管理员，了解系统内部是否使用了专用存储设备来存储、管理相关备份密钥；</p> <p>3、查看系统中备份密钥的存储状态，验证密钥备份功能的正确性与有效性；查看系统所使用的备份密钥存储设备是否经过了国家密码管理部门核准；</p> <p>4、访谈密钥管理员，了解系统内部是否具有较为完善的密钥备份审计信息，了解系统中密钥备份操作的审计内容（审计信息至少包括备份或恢复的主体、备份或恢复的时间等）、审计记录存储方式、存储位置等技术细节内容；查看系统中的密钥备份审计记录，验证密钥备份审计功能的正确性和有效性。</p>
7	归档	应采取有效的安全措施，保证归档密钥的安全性和正确性；归档密钥只能用于解密该密钥加密的历史信息或验证该密钥签名的历史信息；密钥归档应进行记录，并生成审计信息；审计信息包括归档的密钥、归档的时间等；归档密钥应进行数据备份，并采用有效的安全措施。	<p>1、结合技术文档，访谈密钥管理员，了解系统内部是否具有较为完善的密钥归档机制，了解系统中密钥的归档策略、归档密钥的存储方式、存储位置等技术细节内容；</p> <p>2、访谈密钥管理员，了解系统内部归档密钥的使用策略，以保证相关密钥归档后只能对历史数据进行处理，而不能被再次分配给新用户；</p> <p>3、访谈密钥管理员，了解系统内部是否具有较为完善的密钥归档操作审计功能，了解与归档密钥相关的审计内容（审计信息至少包括归档的密钥、归档的时间等）、审计策略、技术实施细节等；查看系统中的密钥4、归档审计记录，验证密钥归档审计功能的正确性和有效性；</p> <p>5、访谈密钥管理员，了解系统内部是否具有安全的归档密钥备份机制，了解与密钥备份相关的技术实施细节。</p>

8	销毁	应具有在紧急情况下销毁密钥的措施。	<p>1、结合技术文档，访谈密钥管理员，了解系统内部是否具有较为完善的应急密钥销毁措施，了解系统在何种情况下将启动密钥销毁操作；</p> <p>2、访谈密钥管理员，了解系统内部在执行密钥销毁操作时，如何处理系统内保存的原有加密文件；</p> <p>3、访谈密钥管理员，了解系统内部在执行密钥销毁操作时，如何更新用户正在使用的密钥；</p> <p>4、访谈密钥管理员，了解系统内部在执行密钥销毁操作时，是否可生成较为完善的审计记录，系统是否具有较为安全的防护措施以保障相关审计记录的正确性与完整性。</p>
---	----	-------------------	--

5.2.4 安全管理测评

5.2.4.1 制度测评

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，制度层面测评实施过程涉及以下各测评单元。

序号	测评单元	测评指标	测评方法
1	制定密码安全管理制度	应制定密码安全管理制度及操作规范、安全操作规范。密码安全管理制度应包括密码建设、运维、人员、设备、密钥等密码管理相关内容。	核查各项安全管理制度、安全操作规范和配套的操作规程是否覆盖包括密码建设、运维、人员、设备、密钥等密码管理相关内容。
2	定期修订安全管理制度	应定期对密码管理制度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的安全管理制度进行修订。	<p>1、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；</p> <p>2、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。</p>
3	明确管理制度发布流程	应明确相关管理制度发布流程。	<p>1、访谈安全主管是否具有管理制度发布流程；</p> <p>2、核查是否具有管理制度发布文件，文件的内容是否包含了制度的制定和发布流程、格式要求及版本编号等相关内容。</p>

5.2.4.2 人员测评

人员测评将通过访谈、文档审查、实地查看的方式，测评本系统的人员安全管

			<p>理保障情况，主要涉及系统负责人、安全主管、系统管理员、安全管理员、安全审计员、密钥管理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。</p> <p>在内容上，人员层面测评实施过程涉及以下各测评单元。</p>
序号	测评单元	测评指标	测评方法
1	了解并遵守密码相关法律法规	应了解并遵守密码相关法律法规。	访谈系统负责人并随机抽查1-2位与密码相关的人员（系统管理员、安全管理员、安全审计员、密钥管理员等），确认是否了解并遵守商用密码相关法律法规。
2	正确使用密码相关产品	应能够正确使用商用密码产品。	访谈系统负责人并随机抽查1-2位与密码相关的人员（系统管理员、安全管理员、安全审计员、密钥管理员等），确认是否能够正确使用商用密码产品。
3	建立岗位责任及人员培训制度	应根据相关密码管理政策、数据安全保密政策，结合组织实际情况，设置密钥管理人员、安全审计人员、密码操作人员等关键岗位；建立相应岗位责任制度，明确相关人员在安全系统中的职责和权限，对关键岗位建立多人共管机制；密钥管理、安全审计、密码操作人员职责互相制约互相监督，相关设备与系统的管理和使用账号不得多人共用。	<p>1、访谈系统负责人，确认是否进行了密码安全管理岗位的划分；</p> <p>2、核查人员安全管理制度及相关记录表单，确认是否明确配备了密钥管理、安全审计、密码设备操作岗位人员；</p> <p>3、访谈安全主管是否明确相关人员在密码设备管理与密钥系统管理中的职责和权限；</p> <p>4、核查人员安全管理制度及岗位设置相关文档是否明确了相关人员在密码设备管理与密钥系统管理中的职责和权限；</p> <p>5、访谈安全主管，并核查岗位设置相关文档，明确是否对关键岗位配备了多人；核查人员安全管理制度及岗位设置相关文档，确认密钥管理、安全审计、密码操作岗位人员职责是否交叉；</p> <p>6、访谈系统管理员、安全管理员、安全审计员及密钥管理员，实地查看设备及系统登录过程，确认设备与系统的管理和使用账号是否多人共用。</p>
4		应建立人员培训制度，对于涉及密码的操作和管理以及密钥管理人员进行专门培训。	<p>1、核查人员安全管理制度中是否包含具体的人员培训制度；</p> <p>2、访谈安全主管，并核查记录表单类文档，确认是否对涉及密码的操作和管理以及密钥管理人员进行了专门培训。</p>

5	设置密码管理和技术岗位并定期考核	应建立人员考核制度，定期进行岗位人员考核，建立健全奖惩制度。	1、核查人员安全管理制度中是否包含具体的人员考核制度和奖惩措施； 2、访谈安全主管，并核查记录表单类文档，确认是否定期进行岗位人员考核。
6	建立关键岗位人员保密制度和调离制度	应建立关键岗位人员保密制度和调离制度，签订保密合同，承担保密义务。	1、核查人员安全管理制度中是否包含具体的关键岗位人员保密制度和调离制度； 2、核查关键岗位人员是否签订了保密合同，保密合同中是否有保密范围、保密责任、违约责任、合同的有效期限和责任人签字等内容。

5.2.4.3 实施测评

实施测评将通过访谈、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，实施层面测评实施过程涉及以下各测评单元。

序号	测评单元	测评指标	测评方法
1	规划	信息系统规划阶段，责任单位应依据密码相关标准，制定密码应用方案，组织测评机构进行评审，评审意见作为项目规划立项的重要材料。	1、核查在规划阶段，是否依据密码相关标准，制定密码应用方案； 2、访谈系统负责人，并核查责任单位是否组织测评机构对安全建设方案进行评审、有无评审报告。
2		通过测评机构审定后的方案应作为建设、验收和测评的重要依据。	核查系统建设、验收和测评是否依据测评机构审定后的方案。
3	建设	应按照国家相关标准，制定实施方案，方案内容应包括但不限于信息系统概述、安全需求分析、密码系统设计方案、密码产品清单（包括产品资质、功能及性能列表和产品生产单位等）、密码系统安全管理与维护策略、密码系统实施计划等。	核查在建设阶段，是否按照国家相关标准制定实施方案，方案内容是否包括且不少于信息系统概述、安全需求分析、密码系统设计方案、密码产品清单（包括产品资质、功能及性能列表和和生产单位等）、密码系统安全管理与维护策略、密码系统实施计划等。
4		应选用经国家密码管理部门核准的密码产品、许可的密码服务。	核查系统使用的密码产品是否经国家密码管理部门核准，密码服务是否经国家密码管理部门许可。

5	运行	信息系统投入运行前，应经密码测评机构进行安全性评估，评估通过方可投入正式运行。	核查信息系统投入运行前，责任单位是否进行了密码安全性评估，是否具有评估报告。
---	----	---	--

5.2.4.4 应急测评

应急测评将通过访谈、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，应急层面测评实施过程涉及以下各测评单元。

序号	测评单元	测评指标	测评方法
1	应急预案	制定应急预案，做好应急资源准备，当事件发生时，按照应急预案结合实际情况及时处置。	1、核查是否根据安全事件等级制定了相应的应急预案及管理制度，应急预案中是否明确了应急事件处理流程及其他管理措施。 2、访谈安全主管是否发生过安全事件；如有安全事件发生，核查应急处置记录，确认是否按照应急预案结合实际情况及时处置。
2	事件处置	事件发生后，应及时向信息系统的上级主管部门进行报告。	访谈安全主管，了解系统安全事件发生后的上报流程；核查安全事件发生后，是否及时向信息系统的上级主管部门进行报告。
3	向有关主管部门上报处置情况	事件处置完成后，应及时向同级的密码主管部门报告事件发生情况及处置情况。	1、访谈安全主管，了解系统安全事件处置完成后的上报流程； 2、核查安全事件处置完成后，是否及时向同级的密码主管部门报告事件发生情况及处置情况。

5.3 测评工具及接入点

5.3.1 测评工具

商用密码应用安全性评估使用的测评工具如下：

序号	名称/型号（或版本）	用途
1	Wireshark	协议分析工具。对被测系统网络和通信安全、设备和计算安全、应用和数据安全方面进行检测分析□通过对通信双方、用户身份鉴别等通信数据包进行抓取，分析系统应用的密码技术的完整性、机密性服务是否有效。
2	Bus Hound串口协议分析工具	USB、串口数据报文分析（APDU），对智能密码钥匙所使用的密码算法进行抓取分析，并对密码算法正确性进行验证。
3	IPSec/SSL 安全协议分析平台	IPSec、SSL报文分析和报告输出
4	密码算法正确性验证系统	算法合规性验证

5.3.2 工具接入点

测试工具接入点应根据被测系统的密码应用领域、网络拓扑结构、访问控制策略、主机存放位置等情况，合理选取接入点。工具测试接入点有以下基本、共性的原则：

从被测系统边界外接入时，测试工具一般接在系统边界设备（通常为交换机）上。在该点接入漏洞扫描器，扫描探测被测系统的主机、网络设备对外暴露的商用密码安全漏洞情况。在该接入点接入协议分析工具，可以捕获应用程序的网络数据包，查看其安全加密和完整性保护情况。在该接入点使用渗透测试工具集，试图利用被测试系统的主机或网络设备的商用密码安全漏洞，跨过系统边界，侵入被测系统主机或网络设备。

从系统内部与测评对象不同网段接入时，测试工具一般接在与被测对象不在同一网段的内部核心交换机上。在该点接入扫描器，可以直接扫描测试内部各主机和网络设备对本单位其他不同网络所暴露的商用密码安全漏洞情况。在该接入点接入网络拓扑发现工具，可以探测信息系统的网络拓扑情况。

在系统内部与测评对象同一网段内接入时，测试工具一般接在与被测对象在同一网段的交换机上。在该点接入扫描器，可以在本地直接测试各被测主机、网络设备对本地网络暴露的商用密码安全漏洞情况。一般来说，该点扫描探测出的漏洞数应该是最多的，它说明主机、网络设备在没有网络安全保护措施下的商用密码安全状况。

依据以上原则，并结合实际情况，选取相应接入点对本次用户单位涉及的信息系统进行现场工具测试。

第六章 整体测评与风险分析

6.1 整体测评与测评实施

商用密码应用安全性评估的整体测评，是在单元测评的基础上，评价信息系统密码应用的整体安全保护能力有没有缺失，是否能够对抗相应等级的安全威胁。

整体测评主要从安全控制间、层面间、区域间（包括物理区域和逻辑区域）等方面进行测评，主要实现：

- 1）针对测评对象“部分符合”及“不符合”要求的单个测评项，分析与该测评项相关的其他测评项能否和它发生关联关系，发生什么样的关联关系，这些关联关系产生的作用是否可以“弥补”该测评项的不足，以及该测评项的不足是否会影响与其有关联关系的其他测评项的测评结果。
- 2）针对测评对象“部分符合”及“不符合”要求的单个测评项，分析与该测评项相关的其他层面的测评对象能否和它发生关联关系，发生什么样的关联关系，这些关联关系产生的作用是否可以“弥补”该测评项的不足，以及该测评项的不足是否会影响与其有关联关系的其他测评项的测评结果。
- 3）针对测评对象“部分符合”及“不符合”要求的单个测评项，分析与该测评项相关的其他区域的测评对象能否和它发生关联关系，发生什么样的关联关系，这些关联关系产生的作用是否可以“弥补”该测评项的不足，以及该测评项的不足是否会影响

响与其有关联关系的其他测评项的测评结果。

6.2 风险分析

商用密码应用安全性评估的风险分析，是依据信息系统密码应用的相关规范和标准，采用风险分析的方法分析测评结果中存在的安全问题可能对被测系统安全造成的影响，主要实现：

1) 结合单元测评的结果汇总和整体测评结果，将物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、密钥管理、安全管理等层面中各个测评对象的测评结果再次汇总分析，统计符合情况。

2) 根据威胁类型和威胁发生频率，判断测评结果汇总中部分符合项或不符合项所产生的安全问题被威胁利用的可能性，可能性的取值范围为高、中和低。

3) 根据资产价值的高低，判断测评结果汇总中部分符合项或不符合项所产生的安全问题被威胁利用后，对被测系统的业务信息安全和系统服务安全造成的影响程度，影响程度取值范围为高、中和低。

4) 综合2)和3)的结果，测评机构根据自身经验和相关国家标准要求，对被测系统面临的安全风险进行赋值，风险值的取值范围为高、中和低。

5) 结合被测系统的安全保护等级对风险分析结果进行评价，即对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益造成的风险。如果存在高风险项，则认为信息系统面临高风险；同时也需要考虑多个中低风险叠加可能导致的高风险问题。

第七章 项目质量管理

7.1 风险规避

在测评过程中，可能会对被测系统造成影响。根据测评范围和测评方法，应充分考虑委托方业务需求和特点，制订测评实施计划，合理安排测评项目，确保测评工作不会对委托方的网络系统运行和业务系统产生显著影响或破坏，尽可能地降低对被测系统的影响。

为了尽可能减小对被测系统正常运行的干扰，省局拟采取以下的措施对测评过程中可能产生的风险予以规避和控制。

7.1.1 敏感信息泄露

风险描述：泄露被测信息系统信息，如网络拓扑、IP地址、加密机制、业务流程、安全隐患和有关文档信息等。

规避方式：在测评委托书中约定保密协议，签订相关合同、保密协议，通过法律进行约束和限制；在组建测评项目组后，对于项目组成员明确规定保密义务，特别是系统配置信息和安全隐患等。

7.1.2 验证测试影响系统正常运行

风险描述：在现场测评时，需对设备 and 应用系统进行一定的验证测试工作。验

证测试可能占用系统资源，对系统的运行造成一定的影响，甚至出现误操作，引起系统崩溃或数据丢失、损坏。

规避方式：与委托方沟通，要求提前做好数据备份和应急恢复措施；协商测评时间和测评强度，避开业务高峰，或者在周末进行；规范验证测试流程，由操作熟练的人员（建议由委托方的系统管理人员）进行测试。

7.1.3工具测试影响系统正常运行

风险描述：在现场测评时，可能会使用一些测评工具进行测试。测评工具可能会产生冗余数据写入，同时可能会对系统的负载造成一定的影响，可能对信息系统中的服务器和网络通讯造成一定影响甚至伤害。

规避方式：与委托方沟通，要求提前做好数据备份和应急恢复措施；明确测试工具接入方式及环境要求；协商测评时间，避开业务高峰，或者在周末进行；控制扫描的并发数量和扫描强度；及时清除工具测试残留数据。

7.2文件控制

在密码应用评估过程中，可能形成的过程文件如下：

- 《总体测评记录表》
- 《物理和环境安全现场测评记录表》
- 《网络和通信安全现场测评记录表》
- 《设备和计算安全现场测评记录表》
- 《应用和数据安全现场测评记录表》
- 《密钥管理现场测评记录表》
- 《制度现场测评记录表》
- 《人员现场测评记录表》
- 《实施现场测评记录表》
- 《应急现场测评记录表》
- 《商用密码应用安全性评估报告》

商用密码应用安全性评估的过程需要形成相关的文件及记录。

7.3保密管理

为保障被测系统安全，应对测评实施过程中获得的数据和结果严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据和结果进行任何侵害测评委托单位利益的行为。具体保密控制措施如下：

在测评委托书中约定保密要求，签订相关合同、保密协议，通过法律进行约束和限制；

对项目组成员明确规定保密义务，特别是系统配置信息和安全隐患等；

配备密评专用计算机，拆除无线、蓝牙、摄像头等外联模块，禁止接入互联网；配备密评专用移动存储介质；

被测系统相关资料和测评过程文档严禁在连接互联网的计算机上存储和处理，严禁在互联网上传输；

			<p>现场测评工作结束后，归还测评过程中借阅的所有文档资料，由测评委托单位相关人员签字确认。</p> <h2>第八章交付物</h2> <p>《商用密码应用安全性评估实施计划》</p> <p>《商用密码应用安全性评估测评方案》（每系统一份）</p> <p>《商用密码应用安全性评估报告》（每系统一份）</p> <p>《整改建议报告》</p>
--	--	--	---

3.2.3人员配置要求

采购包1：
详见采购需求

3.2.4设施设备要求

采购包1：
详见采购需求

3.2.5其他要求

采购包1：
详见采购需求

3.3商务要求

3.3.1服务期限

采购包1：
3个月

3.3.2服务地点

采购包1：
采购人指定地点

3.3.3考核（验收）标准和方法

采购包1：
详见合同条款

3.3.4支付方式

采购包1：
分期付款

3.3.5支付约定

采购包1： 付款条件说明： 合同签订后，达到付款条件起 7 日内，支付合同总金额的 90.00%。

采购包1： 付款条件说明： 服务完成后，达到付款条件起 7 日内，支付合同总金额的 10.00%。

3.3.6违约责任及争议解决的方法

采购包1：
详见合同条款

3.4其他要求

详见采购需求

第四章 资格审查

资格审查由采购人或代理机构组建的资格审查小组依据法律法规和磋商文件的规定，对响应文件中的资格证明等进行审查，以确定投标人是否具备投标资格，并出具资格审查报告。

资格审查标准及要求如下：

4.1一般资格审查

采购包1：

序号	资格审查要求概况	评审点具体描述	关联格式
1	供应商应具备《中华人民共和国政府采购法》第二十二条规定的条件	供应商需在项目电子化交易系统中按要求填写《投标函》完成承诺并进行电子签章。	供应商资质证明文件.d OCX 响应函
2	供应商应提供健全的财务会计制度的证明材料；	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。	供应商资质证明文件.d OCX
3	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； 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，不得再参加该采购项目的其他采购活动。	供应商需在项目电子化交易系统中按要求填写《投标函》完成承诺并进行电子签章。	响应函

4.2落实政府采购政策资格审查

采购包1：

序号	资格审查要求概况	评审点具体描述	关联格式
1	本采购包专门面向中小企业采购	参与的供应商（联合体）服务全部由符合政策要求的中小企业承接。	中小企业声明函 残疾人福利性单位声明函 监狱企业的证明文件

4.3特殊资格审查

采购包1：

序号	资格审查要求概况	评审点具体描述	关联格式
1	“商用密码检测机构资质证书”	供应商须具备国家密码管理局颁发的“商用密码检测机构资质证书”	供应商资质证明文件.d OCX

第五章 磋商过程中可实质性变动的内容

磋商小组可以根据磋商文件和磋商情况实质性变动第三章“磋商项目技术、服务、商务及其他要求”、第八章“拟签订采购合同文本”，但不得变动磋商文件中的其他内容。实质性变动的内容，须经采购人代表确认。

在磋商过程中，磋商小组根据项目实际需要制定磋商内容，在获得采购人代表确认的前提下，可以根据磋商情况实质性变动相关内容。磋商小组对磋商文件作出的实质性变动是磋商文件的有效组成部分，磋商小组应及时通知所有参加磋商的供应商。

第六章 磋商办法

6.1 总则

一、根据《中华人民共和国政府采购法》《中华人民共和国政府采购法实施条例》《政府采购竞争性磋商采购方式管理暂行办法》《陕西省政府采购评审专家管理实施办法》等法律法规，结合本采购项目特点制定本竞争性磋商评审方法。

二、评审工作由代理机构组织，具体评审事务由依法组建的磋商小组负责。

三、评审工作应遵循客观、公正、审慎的原则，并以相同的磋商程序 and 标准对待所有的供应商。

四、本项目采取电子评审，通过项目电子化交易系统完成评审工作。磋商小组成员、采购人、代理机构和供应商应当按照本磋商文件规定和项目电子化交易系统操作要求开展或者参加评审活动。

五、评审过程中的书面材料往来均通过项目电子化交易系统传递，评审委员会成员使用互认的证书及签章进行签名后生效，供应商通过互认的证书及签章加盖其电子印章后生效。出现无法在线签章的特殊情况，评审委员会成员可以线下签署评标报告，由代理机构对原件扫描后以附件形式上传。

六、评审过程应当独立、保密，任何单位和个人不得非法干预评审活动。供应商非法干预评审活动的，其响应文件将作无效处理；代理机构、采购人及其工作人员、采购人监督人员非法干预评审活动的，将依法追究其责任。

6.2 磋商小组

评审专家是采取随机方式在政府采购平台的专家库系统（以下简称专家库系统）抽取/由采购人根据《陕西省政府采购评审专家管理实施办法》（陕财办采〔2018〕20号）的规定，报主管部门同意后自行选定。

一、磋商小组成员应当满足并适应电子化采购评审的工作需要，使用已身份认证并具备签章功能的证书，登录项目电子化交易系统进入项目评审功能模块确认身份、签到、推荐磋商小组组长。采购人代表可以使用采购人代表专用签章确认评审意见。

二、磋商小组成员获取解密后的响应文件，开展评审活动。出现应当回避的情形时，磋商小组成员应当主动回避；代理机构按规定申请补充抽取评审专家；无法及时补充抽取的，采购人或者代理机构应当封存供应商响应文件，按规定重新组建磋商小组，解封响应文件后，开展评审活动。

三、磋商小组按照磋商文件规定的磋商程序、评分方法和标准进行评审，并独立履行下列职责：

- （一）熟悉和理解磋商文件；
- （二）审查供应商响应文件等是否满足磋商文件要求，并作出评价；
- （三）根据需要要求采购组织单位对磋商文件作出解释；根据需要要求供应商对响应文件有关事项作出澄清、说明或者更正；
- （四）推荐成交候选供应商，或者受采购人委托确定成交供应商；
- （五）起草资格审查报告、评审报告并进行签署；
- （六）向采购组织单位、财政部门或者其他监督部门报告非法干预评审工作的行为；
- （七）法律、法规和规章规定的其他职责。

6.3 评审程序

6.3.1 熟悉和理解磋商文件和停止评审

一、磋商小组正式评审前，应当对磋商文件进行熟悉和理解，内容主要包括磋商文件中供应商资格条件要求、采购项目技术、服务和商务要求、磋商办法和标准、政府采购政策要求以及政府采购合同主要条款等。

二、本磋商文件有下列情形之一的，磋商小组应当停止评审：

- （一）磋商文件的规定存在歧义、重大缺陷的；
- （二）磋商文件明显以不合理条件对供应商实行差别待遇或者歧视待遇的；

- （三）采购项目属于国家规定的优先、强制采购范围，但是磋商文件未依法体现优先、强制采购相关规定的；
- （四）采购项目属于政府采购促进中小企业发展的范围，但是磋商文件未依法体现促进中小企业发展相关规定的；
- （五）磋商文件将供应商的资格条件列为评分因素的；
- （六）磋商文件载明的成交原则不合法的；
- （七）磋商文件有违反国家其他有关强制性规定的情形。

出现上述应当停止评审情形的，磋商小组应当通过项目电子化交易系统向采购组织单位提交相关说明材料，说明停止评审的情形和具体理由。除上述情形外，磋商小组不得以任何方式和理由停止评审。

出现上述应当停止评审情形的，采购组织单位应当通过项目电子化交易系统书面告知参加采购活动的供应商，并说明具体原因，同时在陕西省政府采购网公告。采购组织单位认为磋商小组不应当停止评审的，可以书面报告采购项目同级财政部门依法处理，并提供相关证明材料。

6.3.2符合性审查

一、磋商小组依据本磋商文件的实质性要求，对符合资格的响应文件进行审查，以确定其是否满足本磋商文件的实质性要求。本项目的符合性审查事项必须以本磋商文件的明确规定的实质性要求为依据。

二、在符合性审查过程中，如果出现磋商小组成员意见不一致的情况，按照少数服从多数的原则确定，但不得违背政府采购基本原则和磋商文件规定。

三、磋商小组对所有响应文件进行审查后，确定参加磋商的供应商名单。

符合性审查标准见下表：

采购包1：

序号	符合审查要求概况	评审点具体描述	关联格式
1	不正当竞争预防措施（实质性要求）	<p>1.在磋商过程中，磋商小组认为供应商的报价明显低于其他实质性响应的供应商报价，有可能影响产品质量或者不能诚信履约的，磋商小组应当要求其在评审现场合理的时间内提供成本构成书面说明，并提交相关证明材料。书面说明应当按照国家财务会计制度的规定要求，逐项就供应商提供的货物、工程和服务的主营业务成本（应根据供应商企业类型予以区别）、税金及附加、销售费用、管理费用、财务费用等成本构成事项详细陈述。</p> <p>2.供应商提交的相关证明材料，应当加盖供应商（法定名称）电子印章，在磋商小组要求的时间内通过项目电子化交易系统进行提交，否则提交的相关证明材料无效。供应商不能证明其报价合理性的，磋商小组应当将其响应文件作为无效处理。</p>	<p>响应文件封面 标的清单 报价表 响应函 商务偏离表.docx</p>

6.3.3磋商

一、磋商小组按照磋商文件的规定与邀请参加磋商的供应商分别进行磋商，磋商顺序由磋商小组确定。

二、磋商小组所有成员集中与单一供应商对技术、服务、合同条款等内容分别进行一轮或多轮的磋商。在磋商中，磋商的任何一方不得透露与磋商有关的其他供应商的技术资料、价格和其他信息。

三、磋商小组可以根据磋商文件和磋商情况实质性变动第三章“磋商项目技术、服务、商务及其他要求”、第八章“拟签订采购合同文本”，但不得变动磋商文件中的其他内容。实质性变动的内容，须经采购人代表确认。

四、对磋商文件作出的实质性变动是磋商文件的有效组成部分，磋商小组应通过项目电子化交易系统，将变动情况同时通

知所有参加磋商的供应商。磋商过程中，磋商小组可以根据磋商情况调整磋商轮次。

五、磋商过程中，磋商文件变动的，供应商应当按照磋商文件的变动情况和磋商小组的要求就磋商文件变动部分，以“供应商响应表”形式在线提交磋商小组。“供应商响应表”作为响应文件的组成部分，响应文件应加盖供应商（法定名称）电子印章，否则无效。

六、经最终磋商后，响应文件仍有下列情况之一的，应按照无效响应处理：

- （一）响应文件仍不能实质响应磋商文件可实质性变动的实质性要求的；
- （二）响应文件中仍有磋商文件规定的其他无效响应情形的。

七、磋商小组对供应商在磋商、评审过程中的书面交换材料，未按要求加盖电子印章或签字的，视同未提交书面交换材料。

八、磋商小组在最终磋商后，对所有响应文件的有效性、完整性和响应程度进行审查后，确定最后报价的供应商名单。

九、磋商过程中，磋商任何一方不得透露与磋商有关的其他供应商的技术资料、价格和其他信息。

十、磋商过程中，磋商小组发现或者知晓供应商存在违法行为的，应当磋商报告中予以记录，并向本级财政部门报告，依法应将该供应商响应文件作无效处理的，应当作无效处理。

6.3.4最后报价

一、方案评审

采购包1：磋商/谈判/协商文件能够详细列明采购标的的技术、服务要求，磋商/谈判/协商结束后，磋商/谈判/协商小组可以根据磋商/谈判/协商情况要求所有实质性响应的供应商在规定时间内提交最后报价，提交最后报价的供应商不得少于3家。

二、磋商小组开启报价后，供应商应随时关注项目电子化交易系统信息提醒，登录项目电子化交易系统，通过“等候大厅”进行报价并签章后提交。

三、供应商在未提高响应文件中承诺的标准情况下，其最后报价不得高于对该项目之前的报价，否则，磋商小组将对其响应文件作无效处理，并通过电子化交易系统告知供应商，说明理由。

四、供应商最后报价属于明显低价不正当竞争的，磋商小组应按照“供应商须知前附表”第8项规定处理。

五、供应商未在响应文件提交截止时间内提交报价或未按要求进行报价的，视为无效响应，由供应商自行承担不利后果。

六、供应商未按磋商小组要求在规定时间内提交最后报价的，视为其退出磋商。

七、最后报价一旦提交后，供应商不得以任何理由撤回。

八、最后报价为有效报价应符合下列条件：

- （一）供应商所提供的最后报价是在规定的时间内提交。
- （二）供应商的最后报价应加盖供应商（法定名称）电子印章。
- （三）供应商的最后报价应符合磋商文件的要求。
- （四）最后报价唯一，且不高于最高限价。

九、最后报价出现下列情况的，不需要供应商澄清，按以下原则处理：

- （一）报价中的大写金额和小写金额不一致的，以大写金额为准，但大写金额出现文字错误，导致金额无法判断的除外；
- （二）单价金额小数点或者百分比有明显错位的，应以总价为准，并修改单价；
- （三）总价金额与按单价汇总金额不一致的，以单价汇总金额计算结果为准；

同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的最后报价经加盖供应商（法定名称）电子印章后产生约束力，供应商不确认的，其最后报价无效。

6.3.5解释、澄清有关问题

一、评审过程中，磋商小组认为磋商文件有关事项表述不明确或需要说明的，可以提请代理机构书面解释。代理机构的解释不得改变磋商文件的原义或者影响公平、公正，解释事项如果涉及供应商权益的以有利于供应商的原则进行解释。

二、对响应文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，磋商小组应当要求供应商作出必要的澄清、说明或者更正，并给予供应商必要的反馈时间。供应商应当按磋商小组的要求进行澄清、说明或者更正。供应商的

澄清、说明或者更正不得超出响应文件的范围或者改变响应文件的实质性内容。澄清不影响响应文件的效力，有效的澄清、说明或者更正材料是响应文件的组成部分。

三、供应商的澄清、说明或者更正需进行电子签章，应当不超出响应文件的范围、不实质性改变响应文件的内容、不影响供应商的公平竞争、不导致响应文件从不响应磋商文件变为响应磋商文件的条件。下列内容不得澄清：

- （一）供应商响应文件中不响应磋商文件规定的技术参数指标和商务应答；
- （二）供应商响应文件中未提供的证明其是否符合磋商文件资格、符合性规定要求的相关材料。
- （三）供应商响应文件中的材料因印刷、影印等不清晰而难以辨认的。

四、响应文件报价出现前后不一致的情形，按照本章前述规定予以处理，不需要供应商澄清。

五、代理机构宣布评审结束之前，供应商应通过项目电子化交易系统随时关注评审消息提示，及时响应磋商小组发出的澄清、说明或更正要求。供应商未能及时响应的，自行承担不利后果。

六、磋商小组应当积极履行澄清、说明或者更正的职责，不得滥用权力。

6.3.6比较与评价

磋商小组应当按照磋商文件规定的评标细则及标准，对符合性检查合格的响应文件进行商务和技术评估，综合比较和评价。

6.3.7复核

评审结束后，磋商小组应当进行复核，特别要对拟推荐为成交候选供应商的、报价最低的、响应文件被认定为无效的进行重点复核。

评审结果汇总完成后，磋商小组拟出具磋商报告前，代理机构应当组织2名以上的工作人员，在采购现场监督人员的监督之下，依据有关的法律制度和磋商文件对评审结果进行复核，出具复核报告。代理机构复核过程中，磋商小组成员不得离开评审现场。

除资格检查认定错误、分值汇总计算错误、分项评分超出评分标准范围、客观评分不一致、经磋商小组一致认定评分畸高、畸低的情形外，采购人或者代理机构不得以任何理由组织重新评审。采购人、代理机构发现磋商小组未按照磋商文件规定的评审标准进行评审的，应当重新开展采购活动，并同时书面报告本级财政部门。

6.3.8推荐成交候选供应商

磋商小组应当根据综合评分情况，按照评审得分由高到低顺序推荐如下成交候选供应商，并编写磋商报告。

采购包1： 3家； 评审得分相同的，按照最后报价由低到高的顺序推荐。评审得分且最后报价相同的，按照技术指标优劣顺序推荐。评审得分且最后报价且技术指标得分均相同的，成交候选供应商并列。

6.3.9编写磋商报告

磋商小组推荐成交候选供应商后，应向代理机构出具磋商报告。磋商报告应当包括以下主要内容：

- （一）邀请供应商参加采购活动的具体方式和相关情况；
- （二）响应文件开启日期和地点；
- （三）获取磋商文件的供应商名单和磋商小组成员名单；
- （四）评审情况记录和说明，包括对供应商响应文件审查情况、磋商情况、报价情况等；
- （五）提出的成交候选供应商的排序名单及理由。

磋商报告应当由磋商小组全体人员签字或加盖电子签章认可。磋商小组成员对磋商报告有异议的，磋商小组按照少数服从多数的原则推荐成交候选供应商，采购程序继续进行。对磋商报告有异议的磋商小组成员，应当在报告上签署不同意见并说明理由，由磋商小组记录相关情况。磋商小组成员拒绝在磋商报告上签字或加盖电子签章又不书面说明其不同意见和理由的，视为同意磋商报告。

6.3.10评审争议处理规则

在磋商过程中，对于符合性审查、对响应文件作无效响应处理的及其他需要共同认定的事项存在争议的，应当以少数服从多数的原则作出结论，但不得违背磋商文件规定。持不同意见的磋商小组成员应当在磋商报告中签署不同意见及理由，否则视

为同意评审报告。持不同意见的磋商小组成员认为认定过程和结果不符合法律法规或者磋商文件规定的，应当及时向采购人或代理机构书面反映。采购人或代理机构收到书面反映后，应当书面报告采购项目同级财政部门依法处理。

6.4 评审办法及标准

- 一、磋商小组只对通过资格审查的响应文件，根据磋商文件的要求采用相同的评审程序、评分办法及标准进行评价和比较。
- 二、磋商小组成员应依据磋商文件规定的评分标准和方法独立对每个有效响应的文件进行评价、打分，然后汇总每个供应商每项评分因素的得分。

6.4.1 评分办法

本次评审采用综合评分法，由磋商小组采用综合评分法对提交最后报价的供应商的响应文件和最后报价进行综合评分。综合评分法，是指响应文件满足磋商文件全部实质性要求且按评审因素的量化指标评审得分最高的供应商为成交候选供应商的评审方法。

6.4.2 评分标准

采购包1:

评审因素		评审标准			
分值构成		详细评审 90.0000 分 报价得分 10.0000 分			
评审因素分类	评审项	详细描述	分值	客观/主观	关联格式
	业绩	供应商提供 2022年1月 至今同类项目业绩，每提供一个业绩证明计 2分 ，满分 4分 。（业绩以合同签订时间为准。）	4.0000	客观	响应方案说明.docx
	项目负责人及团队建设	1 、整体人员配置满足项目要求，配制科学合理。按其响应程度计 0~5分 。 2 、拟投入员岗位分工明晰、职责明确。按其响应情况，按其响应程度计 0~5分 。（提供人员在投标单位开标日前 6个月 内任一月的社保缴费证明并加盖公章。）	10.0000	主观	响应方案说明.docx
	企业综合实力	1 、供应商具备质量管理体系认证证书且认证范围应与密码测评相关，提供得 3分 ； 2 、供应商具备信息安全管理体系认证证书且认证范围应与密码测评相关，提供得 3分 。	6.0000	客观	响应方案说明.docx

详细评审	售后服务	提供售后服务方案，在项目实施所在地设立相应的技术支持及售后服务机构（提供有效的办公场所证明材料），针对该项目有售后服务体系、计划及措施，售后服务条款或承诺周全、具体、优质。（1）售后服务体系标准规范，方案详细周全，措施得当，承诺优质等计（3-6]分；（2）缺乏标准化售后服务体系，方案粗略，措施简单，符合行业标准计（1-3]分；不提供的不得分。	6.0000	主观	响应方案说明.docx
	成果管理制度方案	供应商提供成果管理制度方案，方案至少包含：1、成果资料管理制度；2、移交工作制度。（1）方案全面完整、切实可行、满足本项目实际需求,得（7-10]分；（2）方案基本完整、可行性较高、基本满足本项目实际需求得（3-7]分；（3）方案不完整、可行性低得（0-3]分；不提供不得分。	10.0000	主观	响应方案说明.docx
	服务质量保障	供应商提供对本项目的质量保证措施方案，方案至少包含：1、结合实际情况制定质量控制目标及措施；2、制定进度控制目标及措施；3、合同管理；4、文档管理措施等。（1）方案全面完整、切实可行、满足本项目实际需求,得（6-9]分；（2）方案基本完整、可行性较高、基本满足本项目实际需求得（3-6]分；（3）方案不完整、可行性低得（0-3]分；不提供不得分。	9.0000	主观	响应方案说明.docx
	合理化建议	供应商针对本项目有明确的合理化建议。（1）方案全面完整、切实可行、满足本项目实际需求,得（3-5]分；（2）方案基本完整、可行性较高、基本满足本项目实际需求得（1-3]分；（3）方案不完整、可行性低得（0-1]分；不提供不得分。	10.0000	主观	响应方案说明.docx

重难点分析	<p>供应商提供针对本项目的重难点分析，方案至少包含：1、重点分析及控制措施；2、难点分析及控制措施。</p> <p>（1）方案全面完整、切实可行、满足本项目实际需求,得（3-5）分；（2）方案基本完整、可行性较高、基本满足本项目实际需求得（1-3）分；（3）方案不完整、可行性低得（0-1）分；不提供不得分。</p>	5.0000	主观	响应方案说明.docx
应急方案	<p>供应商提供针对本项目的应急方案，方案至少包含：1、对后期服务的保证措施、能够处理各类紧急事项的措施；2、保证项目实施，能够保证在规定的时间内解决问题。</p> <p>（1）方案全面完整、切实可行、满足本项目实际需求,得（7-10）分；（2）方案基本完整、可行性较高、基本满足本项目实际需求得（3-7）分；（3）方案不完整、可行性低得（0-3）分；不提供不得分。</p>	10.0000	主观	响应方案说明.docx
保密方案	<p>供应商提供针对本项目的保密方案，方案至少包含：1、测试过程的保密承诺；2、相应的保密措施及保密管理制度等。切合项目具体情况，责任明确，服务定位清晰，能有效保障本项目实施</p> <p>（1）方案全面完整、切实可行、满足本项目实际需求,得（7-10）分；（2）方案基本完整、可行性较高、基本满足本项目实际需求得（3-7）分；（3）方案不完整、可行性低得（0-3）分；不提供不得分。</p>	10.0000	主观	响应方案说明.docx

	项目测试方案	供应商为本项目提供针对性测试方案。方案至少包含：1、测试计划；2、测试目标；3、测试方法；4、测试组织；5、测试进度等（1）方案全面完整、切实可行、满足本项目实际需求,得（7-10]分；（2）方案基本完整、可行性较高、基本满足本项目实际需求得（3-7]分；（3）方案不完整、可行性低得（0-3]分；不提供不得分。	10.0000	主观	响应方案说明.docx
价格分	价格分	满足磋商文件要求且最后报价最低的供应商的价格为磋商基准价。各供应商的价格分统一按照下列公式计算：磋商报价得分=（磋商基准价/最后磋商报价）×价格权值。	10.0000	客观	报价表 标的清单

价格扣除

序号	情形	适用对象	比例	说明	关联格式
无					

6.5 终止采购活动

出现下列情形之一的，采购人或者代理机构应当终止竞争性磋商采购活动，发布项目终止公告并说明原因，重新开展采购活动：

- （一）因情况变化，不再符合规定的竞争性磋商采购方式适用情形的；
- （二）出现影响采购公正的违法、违规行为的；
- （三）除《政府采购竞争性磋商采购方式管理暂行办法》第二十一条第三款规定的情形外，在采购过程中符合要求的供应商或者报价未超过采购预算的供应商不足3家的（财政部另有规定的除外）；
- （四）法律法规规定的其他情形。

6.6 确定成交供应商

- 一、评审结束后，代理机构在评审结束之日起2个工作日内将磋商报告及有关资料送交采购人。
- 二、采购人在收到磋商报告后5个工作日内，在磋商报告确定的成交候选供应商名单中按顺序确定成交供应商。成交候选供应商并列的，由采购人采取随机抽取的方式确定成交供应商。
- 三、采购人逾期未确定成交供应商且不提出异议的，视为确定磋商报告提出的排序第一的供应商为成交供应商。
- 四、根据采购人确定的成交供应商，代理机构在陕西省政府采购网上发布成交结果公告，同时向成交供应商发出成交通知书。

6.7 评审专家在政府采购活动中承担以下义务

- （一）遵守评审工作纪律；
- （二）按照客观、公正、审慎的原则，根据采购文件规定的评审程序、评审方法和评审标准进行独立评审；
- （三）不得泄露评审文件、评审情况和在评审过程中获悉的商业秘密；
- （四）及时向监督管理部门报告评审过程中的违法违规情况，包括采购组织单位向评审专家作出倾向性、误导性的解释或者说明情况，供应商行贿、提供虚假材料或者串通情况，其他非法干预评审情况等；

（五）发现采购文件内容违反国家有关强制性规定或者存在歧义、重大缺陷导致评审工作无法进行时，停止评审并通过项目电子化交易系统向采购组织单位书面说明情况，说明停止评审的情形和具体理由；

（六）配合答复处理供应商的询问、质疑和投诉等事项；

（七）法律、法规和规章规定的其他义务。

6.8 评审专家在政府采购活动中应当遵守以下工作纪律

（一）遵行《中华人民共和国政府采购法》第十二条和《中华人民共和国政府采购法实施条例》第九条及财政部关于回避的规定。

（二）评审前，应当将通讯工具或者相关电子设备交由采购组织单位统一保管。

（三）评审过程中，不得与外界联系，因发生不可预见情况，确实需要与外界联系的，应当在监督人员监督之下办理。

（四）评审过程中，不得干预或者影响正常评审工作，不得发表倾向性、引导性意见，不得修改或细化磋商文件确定的评审程序、评审方法、评审因素和评审标准，不得接受供应商主动提出的澄清和解释，不得征询采购人代表的意见，不得协商评分，不得违反规定的评审格式评分和撰写评审意见，不得拒绝对自己的评审意见签字确认。

（五）在评审过程中和评审结束后，不得记录、复制或带走任何评审资料，不得向外界透露评审内容。

（六）服从评审现场采购组织单位的现场秩序管理，接受评审现场监督人员的合法监督。

（七）遵守有关廉洁自律规定，不得私下接触供应商，不得收受供应商及有关业务单位和个人的财物或好处，不得接受采购组织单位的请托。

第七章 响应文件格式

采购包1:

分册名称: 投标响应文件分册

详见附件: 响应文件封面

详见附件: 响应函

详见附件: 中小企业声明函

详见附件: 残疾人福利性单位声明函

详见附件: 监狱企业的证明文件

详见附件: 报价表

详见附件: 标的清单

详见附件: 商务偏离表.docx

详见附件: 响应方案说明.docx

详见附件: 供应商资质证明文件.docx

第八章 拟签订采购合同文本

详见附件：合同参考格式.docx

