

招 标 文 件

(服务类)

采购项目名称：陕西省公安机关执法办案综合管理平台建设项目

采购项目编号：**DQA-2024072-ZB**

省公安厅机关

陕西德勤招标有限公司共同编制

2024年10月09日

第一章 投标邀请

陕西德勤招标有限公司（以下简称“代理机构”）受省公安厅机关委托，拟对陕西省公安机关执法办案综合管理平台建设项目进行国内公开招标，兹邀请符合本次招标要求的供应商参加投标。

一、采购项目编号：DQA-2024072-ZB

二、采购项目名称：陕西省公安机关执法办案综合管理平台建设项目

三、招标项目简介

本次项目建设应按照《关于分批次组织开展全国执法办案数据治理和汇聚上报工作的通知》、《公安机关接报案与立案工作规定》、《公安机关执法细则》等相关工作规定，全面整合执法办案和监督管理数据资源，规范相关业务标准，联通部省数据汇聚渠道，加强执法大数据智能应用服务，为下一步部平台数据反哺、数据应用提供有力数据支撑。调整完善执法办案业务流程，拓展执法监督业务，建设全省统一管理执法办案管理中心应用，助推我省法治公安建设质量变革、效率变革、动力变革。本项目分6个标包，分别为：1包软件平台开发、2包硬件设备购置、3包等级保护测评服务、4包密码应用安全性评估、5包第三方软件测评、6包平台建设监理。

四、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：

无

（三）本项目的特定资格要求：

采购包1：

1、营业执照等主体资格证明文件：提供有效存续的企业营业执照（副本）/事业单位法人证书/专业服务机构执业许可证/民办非企业单位登记证书。

2、财务状况报告：提供2023年度经审计的财务报告（成立时间至提交投标文件截止时间不足一年的可提供成立后任意时段的资产负债表），或其递交投标文件截止之日前三个月内基本开户银行出具的资信证明，或信用担保机构出具的投标担保函(以上三种形式的资料提供任何一种即可)。

3、书面声明：提供书面声明，包括声明具有履行合同所必需的设备和专业技术能力；未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。

4、社保缴纳证明：提供递交投标文件截止之日前一年内任意一个月的社会保障资金缴存单据或社保机构开具的社会保险参保缴费情况证明。依法不需要缴纳社会保障资金的投标供应商应提供相关证明文件。

5、税收缴纳证明：提供递交投标文件截止之日前一年内任意一个月的依法缴纳税收的相关凭据（时间以税款所属日期为准、税种至少包含增值税或企业所得税），凭据应有税务机关或代收机关的公章或业务专用章。依法免税或无须缴纳税收的投标供应商，应提供相应证明文件。

6、近三年无重大违法、违纪书面声明：提供《近三年无重大违法、违纪书面声明》。

7、信用记录：投标供应商未被列入“信用中国”网站记录的“失信被执行人”或“重大税收违法案件当事人”名单；不处于“中国政府采购网”记录的“政府采购严重违法失信行为记录名单”中的禁止参加政府采购活动期间。（以采购人或采购代理机构开标当天查询结果为准）；

8、控股管理关系：提供直接控股和管理关系清单。若与其他投标人存在单位负责人为同一人或者存在直接控股、管理关系的，则投标无效。

9、法定代表人授权委托书：法定代表人参加投标的，须提供本人身份证复印件；法定代表人授权他人参加投标的，须提供法定代表人授权委托书。招标文件中凡是需要法定代表人盖章之处，非法人单位的负责人均参照执行。法人的分支机构参与投标时，除提供《法定代表人授权委托书》外，还须同时提供总公司给分支机构出具的授权书。

10、本项目不接受联合体投标，不允许分包：投标供应商应提供《非联合体不分包投标声明》，视为独立投标，不分包。

采购包2：

1、营业执照等主体资格证明文件：提供有效存续的企业营业执照（副本）/事业单位法人证书/专业服务机构执业许可证/民办非企业单位登记证书。

2、财务状况报告：提供**2023**年度经审计的财务报告（成立时间至提交投标文件截止时间不足一年的可提供成立后任意时段的资产负债表），或其递交投标文件截止之日前三个月内基本开户银行出具的资信证明，或信用担保机构出具的投标担保函(以上三种形式的资料提供任何一种即可)。

3、书面声明：提供书面声明，包括声明具有履行合同所必需的设备和专业技术能力；未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。

4、社保缴纳证明：提供递交投标文件截止之日前一年内任意一个月的社会保障资金缴存单据或社保机构开具的社会保险参保缴费情况证明。依法不需要缴纳社会保障资金的投标供应商应提供相关证明文件。

5、税收缴纳证明：提供递交投标文件截止之日前一年内任意一个月的依法缴纳税收的相关凭据（时间以税款所属日期为准、税种至少包含增值税或企业所得税），凭据应有税务机关或代收机关的公章或业务专用章。依法免税或无须缴纳税收的投标供应商，应提供相应证明文件。

6、近三年无重大违法、违纪书面声明：提供《近三年无重大违法、违纪书面声明》。

7、信用记录：投标供应商未被列入“信用中国”网站记录的“失信被执行人”或“重大税收违法案件当事人”名单；不处于“中国政府采购网”记录的“政府采购严重违法失信行为记录名单”中的禁止参加政府采购活动期间。（以采购人或采购代理机构开标当天查询结果为准）；

8、控股管理关系：提供直接控股和管理关系清单。若与其他投标人存在单位负责人为同一人或者存在直接控股、管理关系的，则投标无效。

9、法定代表人授权委托书：法定代表人参加投标的，须提供本人身份证复印件；法定代表人授权他人参加投标的，须提供法定代表人授权委托书。招标文件中凡是需要法定代表人盖章之处，非法人单位的负责人均参照执行。法人的分支机构参与投标时，除提供《法定代表人授权委托书》外，还须同时提供总公司给分支机构出具的授权书。

10、本项目不接受联合体投标，不允许分包：投标供应商应提供《非联合体不分包投标声明》，视为独立投标，不分包。

采购包3：

1、营业执照等主体资格证明文件：提供有效存续的企业营业执照（副本）/事业单位法人证书/专业服务机构执业许可证/民办非企业单位登记证书。

2、财务状况报告：提供**2023**年度经审计的财务报告（成立时间至提交投标文件截止时间不足一年的可提供成立后任意时段的资产负债表），或其递交投标文件截止之日前三个月内基本开户银行出具的资信证明，或信用担保机构出具的投标担保函(以上三种形式的资料提供任何一种即可)。

3、书面声明：提供书面声明，包括声明具有履行合同所必需的设备和专业技术能力；未为本项目提供整体设计、规范编制或者项目管理、监理等服务。

4、社保缴纳证明：提供递交投标文件截止之日前一年内任意一个月的社会保障资金缴存单据或社保机构开具的社会保险参保缴费情况证明。依法不需要缴纳社会保障资金的投标供应商应提供相关证明文件。

5、税收缴纳证明：提供递交投标文件截止之日前一年内任意一个月的依法缴纳税收的相关凭据（时间以税款所属日期为准、税种至少包含增值税或企业所得税），凭据应有税务机关或代收机关的公章或业务专用章。依法免税或无须缴纳税收的投

标供应商，应提供相应证明文件。

6、近三年无重大违法、违纪书面声明：提供《近三年无重大违法、违纪书面声明》。

7、信用记录：投标供应商未被列入“信用中国”网站记录的“失信被执行人”或“重大税收违法案件当事人”名单；不处于“中国政府采购网”记录的“政府采购严重违法失信行为记录名单”中的禁止参加政府采购活动期间。（以采购人或采购代理机构开标当天查询结果为准）；

8、控股管理关系：提供直接控股和管理关系清单。若与其他投标人存在单位负责人为同一人或者存在直接控股、管理关系的，则投标无效。

9、法定代表人授权委托书：法定代表人参加投标的，须提供本人身份证复印件；法定代表人授权他人参加投标的，须提供法定代表人授权委托书。招标文件中凡是需要法定代表人盖章之处，非法人单位的负责人均参照执行。法人的分支机构参与投标时，除提供《法定代表人授权委托书》外，还须同时提供总公司给分支机构出具的授权书。

10、本项目不接受联合体投标，不允许分包：投标供应商应提供《非联合体不分包投标声明》，视为独立投标，不分包。

11、特殊资格要求：具备《网络安全等级测评与检测评估机构服务认证证书》。

采购包4：

1、营业执照等主体资格证明文件：提供有效存续的企业营业执照（副本）/事业单位法人证书/专业服务机构执业许可证/民办非企业单位登记证书。

2、财务状况报告：提供2023年度经审计的财务报告（成立时间至提交投标文件截止时间不足一年的可提供成立后任意时段的资产负债表），或其递交投标文件截止之日前三个月内基本开户银行出具的资信证明，或信用担保机构出具的投标担保函(以上三种形式的资料提供任何一种即可)。

3、书面声明：提供书面声明，包括声明具有履行合同所必需的设备和专业技术能力；未为本项目提供整体设计、规范编制或者项目管理、监理等服务。

4、社保缴纳证明：提供递交投标文件截止之日前一年内任意一个月的社会保障资金缴存单据或社保机构开具的社会保险参保缴费情况证明。依法不需要缴纳社会保障资金的投标供应商应提供相关证明文件。

5、税收缴纳证明：提供递交投标文件截止之日前一年内任意一个月的依法缴纳税收的相关凭据（时间以税款所属日期为准、税种至少包含增值税或企业所得税），凭据应有税务机关或代收机关的公章或业务专用章。依法免税或无须缴纳税收的投标供应商，应提供相应证明文件。

6、近三年无重大违法、违纪书面声明：提供《近三年无重大违法、违纪书面声明》。

7、信用记录：投标供应商未被列入“信用中国”网站记录的“失信被执行人”或“重大税收违法案件当事人”名单；不处于“中国政府采购网”记录的“政府采购严重违法失信行为记录名单”中的禁止参加政府采购活动期间。（以采购人或采购代理机构开标当天查询结果为准）；

8、控股管理关系：提供直接控股和管理关系清单。若与其他投标人存在单位负责人为同一人或者存在直接控股、管理关系的，则投标无效。

9、法定代表人授权委托书：法定代表人参加投标的，须提供本人身份证复印件；法定代表人授权他人参加投标的，须提供法定代表人授权委托书。招标文件中凡是需要法定代表人盖章之处，非法人单位的负责人均参照执行。法人的分支机构参与投标时，除提供《法定代表人授权委托书》外，还须同时提供总公司给分支机构出具的授权书。

10、本项目不接受联合体投标，不允许分包：投标供应商应提供《非联合体不分包投标声明》，视为独立投标，不分包。

11、特殊资格要求：具备国家密码管理部门同意其开展商用密码应用安全性评估的证明资料。

采购包5：

1、营业执照等主体资格证明文件：提供有效存续的企业营业执照（副本）/事业单位法人证书/专业服务机构执业许可证/民办非企业单位登记证书。

- 2、财务状况报告：提供**2023**年度经审计的财务报告（成立时间至提交投标文件截止时间不足一年的可提供成立后任意时段的资产负债表），或其递交投标文件截止之日前三个月内基本开户银行出具的资信证明，或信用担保机构出具的投标担保函(以上三种形式的资料提供任何一种即可)。
- 3、书面声明：提供书面声明，包括声明具有履行合同所必需的设备和专业技术能力；未为本项目提供整体设计、规范编制或者项目管理、监理等服务。
- 4、社保缴纳证明：提供递交投标文件截止之日前一年内任意一个月的社会保障资金缴存单据或社保机构开具的社会保险参保缴费情况证明。依法不需要缴纳社会保障资金的投标供应商应提供相关证明文件。
- 5、税收缴纳证明：提供递交投标文件截止之日前一年内任意一个月的依法缴纳税收的相关凭据（时间以税款所属日期为准、税种至少包含增值税或企业所得税），凭据应有税务机关或代收机关的公章或业务专用章。依法免税或无须缴纳税收的投标供应商，应提供相应证明文件。
- 6、近三年无重大违法、违纪书面声明：提供《近三年无重大违法、违纪书面声明》。
- 7、信用记录：投标供应商未被列入“信用中国”网站记录的“失信被执行人”或“重大税收违法案件当事人”名单；不处于“中国政府采购网”记录的“政府采购严重违法失信行为记录名单”中的禁止参加政府采购活动期间。（以采购人或采购代理机构开标当天查询结果为准）；
- 8、控股管理关系：提供直接控股和管理关系清单。若与其他投标人存在单位负责人为同一人或者存在直接控股、管理关系的，则投标无效。
- 9、法定代表人授权委托书：法定代表人参加投标的，须提供本人身份证复印件；法定代表人授权他人参加投标的，须提供法定代表人授权委托书。招标文件中凡是需要法定代表人盖章之处，非法人单位的负责人均参照执行。法人的分支机构参与投标时，除提供《法定代表人授权委托书》外，还须同时提供总公司给分支机构出具的授权书。
- 10、本项目不接受联合体投标，不允许分包：投标供应商应提供《非联合体不分包投标声明》，视为独立投标，不分包。
- 11、特殊资格要求：投标供应商须具备检验检测机构资质认定(CMA)证书或CNAS实验室认可证书。
- 采购包6:
- 1、营业执照等主体资格证明文件：提供有效存续的企业营业执照（副本）/事业单位法人证书/专业服务机构执业许可证/民办非企业单位登记证书。
- 2、财务状况报告：提供**2023**年度经审计的财务报告（成立时间至提交投标文件截止时间不足一年的可提供成立后任意时段的资产负债表），或其递交投标文件截止之日前三个月内基本开户银行出具的资信证明，或信用担保机构出具的投标担保函(以上三种形式的资料提供任何一种即可)。
- 3、书面声明：提供书面声明，包括声明具有履行合同所必需的设备和专业技术能力；未为本项目提供整体设计、规范编制或者项目管理、检测等服务。
- 4、社保缴纳证明：提供递交投标文件截止之日前一年内任意一个月的社会保障资金缴存单据或社保机构开具的社会保险参保缴费情况证明。依法不需要缴纳社会保障资金的投标供应商应提供相关证明文件。
- 5、税收缴纳证明：提供递交投标文件截止之日前一年内任意一个月的依法缴纳税收的相关凭据（时间以税款所属日期为准、税种至少包含增值税或企业所得税），凭据应有税务机关或代收机关的公章或业务专用章。依法免税或无须缴纳税收的投标供应商，应提供相应证明文件。
- 6、近三年无重大违法、违纪书面声明：提供《近三年无重大违法、违纪书面声明》。
- 7、信用记录：投标供应商未被列入“信用中国”网站记录的“失信被执行人”或“重大税收违法案件当事人”名单；不处于“中国政府采购网”记录的“政府采购严重违法失信行为记录名单”中的禁止参加政府采购活动期间。（以采购人或采购代理机构开标当天查询结果为准）；
- 8、控股管理关系：提供直接控股和管理关系清单。若与其他投标人存在单位负责人为同一人或者存在直接控股、管理关系的，则投标无效。

9、法定代表人授权委托书：法定代表人参加投标的，须提供本人身份证复印件；法定代表人授权他人参加投标的，须提供法定代表人授权委托书。招标文件中凡是需要法定代表人盖章之处，非法人单位的负责人均参照执行。法人的分支机构参与投标时，除提供《法定代表人授权委托书》外，还须同时提供总公司给分支机构出具的授权书。

10、本项目不接受联合体投标，不允许分包：投标供应商应提供《非联合体不分包投标声明》，视为独立投标，不分包。

五、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

六、招标文件获取时间、方式及地址

（一）招标文件获取时间：详见采购公告

（二）在招标文件获取开始时间前，采购人或代理机构将本项目招标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招标文件。成功获取招标文件的，供应商将收到已获取招标文件的回执函。未成功获取招标文件的供应商，不得参与本次采购活动，不得对招标文件提起质疑。

成功获取招标文件后，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投标文件编制的，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招标文件，供应商应当重新获取招标文件；澄清或者修改后的招标文件发布日期距提交投标文件截止日期不足15日的，采购人或代理机构顺延提交投标文件的截止时间。供应商未重新获取招标文件或者未按照澄清或者修改后的招标文件编制投标文件进行投标的，自行承担不利后果。

七、投标文件提交截止时间及开标时间、地点、方式

（一）投标文件提交截止时间及开标时间：详见采购公告

（二）投标文件提交方式、地点：供应商应当在投标文件提交截止时间前，通过项目电子化交易系统提交投标文件。成功提交的，供应商将收到已提交投标文件的回执函。

（三）本项目采取网上开标，即采购人或代理机构通过项目电子化交易系统“开标/开启大厅”组织在线开标。

八、本投标邀请在陕西省政府采购网以公告形式发布

九、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，凭项目中标（成交）结果、中标（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、联系方式

采购人：省公安厅机关

地址：西安市未央区凤城二路19号

邮编：710000

联系人：潘警官

联系电话：029-86166900

代理机构：陕西德勤招标有限公司

地址：陕西省西安市高新区丈八一路1号汇鑫中心D座2206室

邮编：710065

联系人：贾旭鸣

联系电话：029-81169855

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 投标人须知

2.1 投标人须知前附表

序号	应知事项	说明和要求
1	采购预算（实质性要求）	<p>本项目各包采购预算金额如下：</p> <p>采购包1：19,729,700.00元</p> <p>采购包2：12,675,200.00元</p> <p>采购包3：260,000.00元</p> <p>采购包4：320,000.00元</p> <p>采购包5：425,000.00元</p> <p>采购包6：612,600.00元</p> <p>投标人的采购包投标报价高于采购包采购预算的，其投标文件将按无效处理。</p>
2	最高限价（实质性要求）	<p>详见第三章。</p> <p>投标人的采购包投标报价高于最高限价的，其投标文件将按无效处理。</p>
3	评标方法	<p>采购包1：综合评分法</p> <p>采购包2：综合评分法</p> <p>采购包3：综合评分法</p> <p>采购包4：综合评分法</p> <p>采购包5：综合评分法</p> <p>采购包6：综合评分法</p> <p>（详见第五章）</p>
4	是否接受联合体	<p>采购包1：不接受</p> <p>采购包2：不接受</p> <p>采购包3：不接受</p> <p>采购包4：不接受</p> <p>采购包5：不接受</p> <p>采购包6：不接受</p> <p>如以联合体响应的，联合体各方均应当具备本招标文件要求的资格条件和能力。</p> <p>（1）联合体各方均应具有承担本项目必备的条件，如相应的人力、物力、资金等。</p> <p>（2）招标文件对投标人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。</p> <p>（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乙级，则该联合体资质等级等级为乙级。</p>

5	落实节能、环保产品政策	<p>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。</p> <p>2.本项目采购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，否则作无效投标处理。</p> <p>3.本项目采购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，本项目采购信创云管理服务器、信创云虚拟化服务器、信创云分布式存储服务器、信创云备份存储服务器、国产大数据节点服务器、GPU服务器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/响应报价相同的，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。</p>
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）	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五章。
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>使用综合评分法的采购项目，提供相同品牌产品且通过资格审查、符合性审查的不同投标人参加同一合同项下投标的，按一家投标人计算，评审后得分最高的同品牌投标人获得中标人推荐资格；评审得分相同的，由采购人或者采购人委托评标委员会采取随机抽取方式确定一个投标人获得中标人推荐资格，其他同品牌投标人不作为中标候选人。</p> <p>采用最低评标价法的采购项目，提供相同品牌产品的不同投标人参加同一合同项下投标的，以其中通过资格审查、符合性审查且报价最低的参加评标；报价相同的，由采购人或者采购人委托评标委员会按照随机抽取方式确定一个参加评标的投标人，其他投标无效。</p> <p>核心产品清单详见第三章。</p> <p>在符合性审查环节提供核心产品品牌不足3个的，视为有效投标人不足3家。</p>
8	不正当竞争预防措施（实质性要求）	在评标过程中，评标委员会认为投标人投标报价明显低于其他通过符合性审查投标人的投标报价，有可能影响产品质量或者不能诚信履约的，评标委员会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。投标人提交的书面说明，应当加盖投标人公章，在评标委员会要求的时间内通过项目电子化交易系统进行提交，否则视为不能证明其投标报价合理性。投标人不能证明其投标报价合理性的，评标委员会应当将其投标文件作为无效投标处理。

9	投标保证金	采购包1保证金金额：300,000.00元 采购包2保证金金额：250,000.00元 采购包3保证金金额：5,000.00元 采购包4保证金金额：6,000.00元 采购包5保证金金额：8,000.00元 采购包6保证金金额：12,000.00元 缴交渠道：电子保函,转账、支票、汇票等（需通过实体账户、户名及开户行信息） 开户名称：陕西德勤招标有限公司 开户银行：光大银行西安丈八东路支行 银行账号：52880188000025295
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 采购包2：不缴纳 采购包3：不缴纳 采购包4：不缴纳 采购包5：不缴纳 采购包6：不缴纳
12	投标有效期（实质性要求）	提交投标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）	本项目收取代理服务费 代理服务费用收取对象：中标/成交供应商 代理服务费收费标准：中标金额100万元以下，费率1.5%，中标金额100-500万元，费率1.1%，中标金额500-1000万元，费率0.8%，中标金额1000-5000万元，费率0.5%,采购代理服务收费按差额定率累进法计算，若代理服务费核算后低于5000元按5000元计取。
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	中标通知书	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中标供应商发出中标通知书；中标供应商通过项目电子化交易系统获取中标通知书。
16	政府采购合同公告、备案	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； 政府采购合同签订之日起7个工作日内，采购人将政府采购合同报本级财政部门备案。
17	进口产品	不允许
18	是否组织潜在投标人现场考察	采购包1：组织现场踏勘：否 采购包2：组织现场踏勘：否 采购包3：组织现场踏勘：否 采购包4：组织现场踏勘：否 采购包5：组织现场踏勘：否 采购包6：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）而无法正常使用的；</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废标。</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）而无法正常使用的；</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。出现上述的情形，不影响采购公平、公正的，采购人或者采购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，采购人或者采购代理机构应当依法废标。</p>
----	------	--

2.2总则

2.2.1适用范围

- 一、本招标文件仅适用于本次公开招标采购项目。
- 二、本招标文件的最终解释权由省公安厅机关和陕西德勤招标有限公司享有。对招标文件中供应商参加本次政府采购活动应当具备的条件，招标项目技术、服务、商务及其他要求，评标细则及标准由省公安厅机关负责解释。除上述招标文件内容，其他内容由陕西德勤招标有限公司负责解释。

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。本次招标的采购人是省公安厅机关。
- 二、“投标人”是指按照采购公告规定获取了招标文件，拟参加投标和向采购人提供货物、工程或服务的法人、其他组织或者自然人。
- 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陕西德勤招标有限公司。
- 四、“网上开标”是指代理机构通过项目电子化交易系统在线完成签到、开标、唱标和记录等活动，供应商通过项目电子化交易系统在线完成投标文件解密、参与开标活动。
- 五、“电子评标”是指通过项目电子化交易系统在线完成资格审查小组和评审小组组建，开展资格和符合性审查、比较与评价、出具评标报告、推荐中标候选供应商等活动。

2.3招标文件

2.3.1招标文件的构成

- 一、招标文件是投标人准备投标文件和参加投标的依据，同时也是资格审查、评标的重要依据。招标文件用以阐明招标项目所需的资质、技术、服务及报价等要求、招标投标程序、有关规定和注意事项以及合同主要条款等。本招标文件包括以下内容：
 - （一）投标邀请；
 - （二）投标人须知；
 - （三）招标项目技术、服务、商务及其他要求；
 - （四）资格审查；
 - （五）评标办法；
 - （六）投标文件格式；
 - （七）拟签订采购合同文本。

二、投标人应认真阅读和充分理解招标文件中所有的事项、格式条款和规范要求。投标人没有对招标文件全面作出实质性响应所产生的风险由投标人承担。

2.3.2 招标文件的澄清和修改

一、在投标文件提交截止时间前，采购人或者代理机构可以对已发出的招标文件进行必要的澄清或者修改。

二、澄清或者修改的内容为招标文件的组成部分，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，投标人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。更正内容可能影响投标文件编制的，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招标文件，投标人应依据更正后的招标文件编制投标文件。若投标人未按前述要求进行投标响应的，自行承担不利后果。

2.4 投标文件

2.4.1 投标文件的语言

一、投标人提交的投标文件以及投标人与采购人或代理机构就有关投标的所有来往书面文件均须使用中文。投标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，评标委员会将其视为无效材料。

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投标人的不利后果，由投标人承担。

2.4.2 计量单位

除招标文件中另有规定外，本项目均采用国家法定的计量单位。

2.4.3 投标货币

本次项目均以人民币报价。

2.4.4 知识产权

一、投标人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，如因专利权、商标权或其它知识产权而引起法律和经济纠纷，由投标人承担所有相关责任。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、投标人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，投标人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、如采用投标人所不拥有的知识产权，则在投标报价中必须包括合法使用该知识产权的相关费用。

2.4.5 投标文件的组成

投标人应当按照招标文件的要求编制投标文件。投标文件应当对招标文件提出的要求和条件作出明确响应。

投标文件具体内容详见第六章。

2.4.6 投标文件格式

一、投标人应按照招标文件第六章中提供的“投标文件格式”填写相关内容。

二、对于没有格式要求的投标文件由投标人自行编写。

2.4.7 投标报价（实质性要求）

一、投标人的报价是投标人响应招标项目要求的全部工作内容的价格体现，包括投标人完成本项目所需的一切费用。

二、投标人每种货物及服务内容只允许有一个报价，并且在合同履行过程中是固定不变的，任何有选择或可调整的报价将不予接受，并按无效投标处理。

三、投标文件报价出现前后不一致的，按照招标文件第五章评标办法规定予以修正，修正后的报价经投标人通过项目电子化交易系统进行确认，并加盖投标人（法定名称）电子印章，投标人未在规定时间内确认的，其投标无效。

2.4.8 投标有效期（实质性要求）

投标有效期详见第二章“投标人须知前附表”，投标文件未明确投标有效期或者投标有效期小于“投标人须知前附表”中投标有效期要求的，其投标文件按无效处理。

2.4.9 投标文件的制作、签章和加密（实质性要求）

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、投标人应按照客户端操作要求，对应招标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招标文件对应项的要求的，其投标文件作无效处理。

三、投标人完成投标文件编制后，应按照招标文件第一章明确的签章要求，使用互认的证书及签章对投标文件进行电子签章和加密。

四、招标文件澄清或者修改的内容可能影响投标文件编制的，代理机构将重新发布澄清或者修改后的招标文件，投标人应重新获取澄清或者修改后的招标文件，按照澄清或者修改后的招标文件进行投标文件编制、签章和加密。

2.4.10 投标文件的提交

一、（实质性要求）投标人应当在投标文件提交截止时间前，通过项目电子化交易系统完成投标文件提交。

二、在投标文件提交截止时间后，采购人或者代理机构不再接受投标人提交投标文件。投标人应充分考虑影响投标文件提交的各种因素，确保在投标文件提交截止时间前完成提交。

2.4.11 投标文件的补充、修改、撤回（实质性要求）

投标文件提交截止时间前，投标人可以补充、修改或者撤回已成功提交的投标文件；对投标文件进行补充、修改的，应当先行撤回已提交的投标文件，补充、修改后重新提交。

供应商投标文件撤回后，视为未提交过投标文件。

2.5 开标、资格审查、评标和中标

2.5.1 开标及开标程序

一、本项目为网上开标项目。网上开标的开始时间为投标文件提交截止时间。成功提交或解密电子投标文件的投标人不足3家的，不予开标，采购人或代理机构将作废标处理。

二、开标准备工作

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。

投标文件提交截止时间前30分钟，投标人登录项目电子化交易系统-“开标/开启大厅”参与开标。

三、解密投标文件（实质性要求）

投标文件提交截止时间后，成功提交投标文件的投标人符合招标文件规定数量的，代理机构将启动投标文件解密程序，解密时间为30分钟；投标人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投标文件解密。投标人未在规定的解密时间内完成解密的，按无效投标处理。

四、开标

解密时间截止或者所有投标人投标文件均完成解密后（以发生在先的时间为准），由代理机构通过项目电子化交易系统对投标人名称、投标文件解密情况、投标报价进行展示。

开标过程中，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。投标人对开标过程和开标记录有疑义，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投标人提出的询问或者回避申请应当及时处理。

投标人完成投标文件解密后，自主决定是否参加网上在线开标，未参加的，视同认可开标结果。

2.5.2 查询及使用信用记录

开标结束后，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，查询投标人在投标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，以一个投标人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

详见招标文件第四章。

2.5.4 评标

详见招标文件第五章。

2.5.5 中标通知书

一、采购人或者评标委员会确认中标供应商后，代理机构在陕西省政府采购网发布中标结果公告、通过项目电子化交易系统发出中标通知书，中标供应商通过项目电子化交易系统获取中标通知书。

二、中标通知书是采购人和中标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、规章制度规定的中标无效情形的，将以公告形式宣布发出的中标通知书无效，中标通知书将自动失效，并依法重新确定中标供应商或者重新开展采购活动。

三、中标通知书对采购人和中标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、采购人应在中标通知书发出之日起三十日内与中标人签订采购合同。

二、采购人和中标人签订的采购合同不得对招标文件确定的事项以及中标人的投标文件作实质性修改。

2.6.2 合同分包和转包（实质性要求）

2.6.2.1 合同分包

一、投标人根据招标文件的规定和采购项目的实际情况，拟在中标后将中标项目的非主体、非关键性工作分包的，应当在投标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。

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，不属于中标人的主要合同义务。

三、采购合同实行分包履行的，中标人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。

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。

采购包2：不允许合同分包。

采购包3：不允许合同分包。

采购包4：不允许合同分包。

采购包5：不允许合同分包。

采购包6：不允许合同分包。

2.6.2.2 合同转包

一、严禁中标供应商将本项目转包。本项目所称转包，是指将本项目转给他人或者将本项目全部肢解以后以分包的名义分别转给他人的行为。

二、中标供应商转包的，视同拒绝履行政府采购合同，将依法追究法律责任。

2.6.3 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或者服务的，在不改变合同其他条款的前提下，可以与中标人协商签订补充合同，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。

2.6.4 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。

2.6.5履约验收方案

采购包1:

以采购合同相关条款要求为准。

采购包2:

以采购合同相关条款要求为准。

采购包3:

以采购合同相关条款要求为准。

采购包4:

以采购合同相关条款要求为准。

采购包5:

以采购合同相关条款要求为准。

采购包6:

以采购合同相关条款要求为准。

2.6.6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评标活动纪律要求

采购人、代理机构应保证评标活动在严格保密的情况下进行，采购人、代理机构、投标人和评标委员会成员应当严格遵守政府采购法律法规规章制度和本项目招标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评标过程和结果。

对各投标人的商业秘密，评标委员会成员应予以保密，不得泄露给其他投标人。

2.7.2投标人不得具有的情形（实质性要求）

投标人参加投标不得有下列情形：

一、有下列情形之一的，视为投标人串通投标：

- （一）不同投标人的投标文件由同一单位或者个人编制；
- （二）不同投标人委托同一单位或者个人办理投标事宜；
- （三）不同投标人的投标文件载明的项目管理成员或者联系人员为同一人；
- （四）不同投标人的投标文件异常一致或者投标报价呈规律性差异；
- （五）不同投标人的投标文件相互混装；

二、提供虚假材料谋取中标；

三、采取不正当手段诋毁、排挤其他投标人；

四、与采购人或代理机构、其他投标人恶意串通；

五、向采购人或代理机构、评标委员会成员行贿或者提供其他不正当利益；

六、在招标过程中与采购人或代理机构进行协商谈判；

七、中标后无正当理由拒不与采购人签订政府采购合同；

八、未按照招标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。

投标人有上述情形的，按照规定追究法律责任，具有前述一至十三条情形之一的，其投标文件无效，或取消被确认为中标供应商的资格或认定中标无效。

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投标人有下列利害关系之一的，应当回避：

- (1) 参加采购活动前3年内与投标人存在劳动关系；
- (2) 参加采购活动前3年内担任投标人的董事、监事；
- (3) 参加采购活动前3年内是投标人的控股股东或者实际控制人；
- (4) 与投标人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；
- (5) 与投标人有其他可能影响政府采购活动公平、公正进行的关系。

投标人认为采购人员及相关人员与其他投标人有利害关系的，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，供应商对招标文件中采购需求的询问、质疑由 陕西德勤招标有限公司 负责答复；供应商对除采购需求外的采购文件的询问、质疑由陕西德勤招标有限公司 负责答复；供应商对采购过程、采购结果的询问、质疑由 陕西德勤招标有限公司 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（包括但不限于文字错误、标点符号、不影响投标文件的编制的情形）。

四、供应商认为采购文件、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（针对招标文件提出的质疑，需提交从项目电子化交易系统获取的招标文件回执单）。

答复主体：代理机构

联系人：贾旭鸣

联系电话：029-81169855

地址：陕西省西安市高新区丈八一路1号汇鑫中心D座2206室

邮编：710065

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招标文件、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 招标项目技术、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

本次项目建设应按照《关于分批次组织开展全国执法办案数据治理和汇聚上报工作的通知》、《公安机关接报案与立案工作规定》、《公安机关执法细则》等相关工作规定，全面整合执法办案和监督管理数据资源，规范相关业务标准，联通部省数据汇聚渠道，加强执法大数据智能应用服务，为下一步部平台数据反哺、数据应用提供有力数据支撑。调整完善执法办案业务流程，拓展执法监督业务，建设全省统一管理执法办案管理中心应用，助推我省法治公安建设质量变革、效率变革、动力变革。本项目分6个标包，分别为：1包软件平台开发、2包硬件设备购置、3包等级保护测评服务、4包密码应用安全性评估、5包第三方软件测评、6包平台建设监理。

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）：19,729,700.00

采购包最高限价（元）：19,729,700.00

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	服务	1.00	19,729,700.00	项	软件和信息技术服务业	否	否	否	否

采购包2：

采购包预算金额（元）：12,675,200.00

采购包最高限价（元）：12,675,200.00

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	服务	1.00	12,675,200.00	项	工业	否	否	否	是

采购包3：

采购包预算金额（元）：260,000.00

采购包最高限价（元）：260,000.00

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	服务	1. 0 0	260,000. 00	项	软件和信息技术服务业	否	否	否	否

采购包4:

采购包预算金额（元）：320,000.00

采购包最高限价（元）：320,000.00

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	服务	1. 0 0	320,000. 00	项	软件和信息技术服务业	否	否	否	否

采购包5:

采购包预算金额（元）：425,000.00

采购包最高限价（元）：425,000.00

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	服务	1. 0 0	425,000. 00	项	软件和信息技术服务业	否	否	否	否

采购包6:

采购包预算金额（元）：612,600.00

采购包最高限价（元）：612,600.00

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	服务	1. 0 0	612,600. 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：服务

参数性质	序号	技术参数与性能指标
		<p>1.项目概述</p> <p>1.1建设背景</p> <p>本次项目建设应按照《关于分批次组织开展全国执法办案数据治理和汇聚上报工作的通知》、《公安机关接报案与立案工作规定》、《公安机关执法细则》等相关工作规定，全面整合执法办案和监督管理数据资源，规范相关业务标准，联通部省数据汇聚渠道，加强执法大数据智能应用服务，为下一步部平台数据反哺、数据应用提供有力数据支撑。调整完善执法办案业务流程，拓展执法监督业务，建设全省统一管理执法办案管理中心应用，助推我省法治公安建设质量变革、效率变革、动力变革。</p> <p>1.2项目意义</p> <p>按照陕西省《数字政府建设“十四五”规划》，以及省委改革办关于新发展阶段推进创造型、引领型改革的工作部署，坚持以问题导向、需求导向、目标导向为原则，以政法协同办案流程、节点为依托，设计公安部门数据协同标准和规范，并满足信创要求，构建具有陕西特色的政法一体化协同办案体系。</p> <p>2.建设目标</p> <p>2.1政务目标</p> <p>坚持以总书记新时代中国特色社会主义思想为指导，认真学习贯彻总书记网络强国战略思想，深入贯彻中央政法工作会议上总书记重要讲话精神，紧紧围绕党和国家工作大局以及新时代政法工作新任务新要求，牢固树立互联网思维、创新思维、系统思维，坚持开放共享的理念。以刑事诉讼跨部门大数据协同办案平台建设为着力点，坚决破除政法领域信息孤岛、数据壁垒、网络梗阻，力争实现政法机关“设施联通、网络畅通、平台贯通、数据融通、业务联通”的五通总目标。</p> <p>2022年公安部下发的《公安信息化建设“十四五”规划》中明确要求省级公安机关一是要升级电子卷宗、电子签名、电子指纹捺印等功能，逐步实现文书卷宗电子化、无纸化；二是要升级省级政法跨部门协同功能，梳理明确政法跨部门协同办理业务需求，加强侦查环节证据材料的审查功能，开发跨部门业务协同，逐步实现电子卷宗、法律文书等办案信息在政法部门间快速流转和执法办案业务的跨部门协同办理，提升政法协同办案效率。</p> <p>2.2业务目标</p> <p>本次项目建设借助云计算、大数据等新技术，新建政法协同办案系统、升级改造违法犯罪人员信息系统，以政法跨部门协同办案，调整完善执法办案业务流程为核心实现以下业务目标：</p> <p>（1）实现政法跨部门协同办案</p> <p>通过本项目的建设，促进公安、检察院、法院、司法等政法部门之间的数据共享与业务协同，从而打破信息壁垒，显著提升案件处理的效率与质量。</p> <p>（2）全面落实《公安机关执法细则》</p> <p>通过本平台的建设，从业务流程、文书、执法监督等方面确保《公安机关执法细则》的各项要求得到全面贯彻落实，从而规范执法行为，保障其合法化，进而提升执法质量与效果。</p> <p>（3）支撑受立案制度改革</p> <p>为贯彻公安部《公安机关接报案与立案工作规定》的相关要求，本项目将对接报案、立案、办理</p>

、结案等关键环节进行规范化、标准化管理，以支持并完善受立案制度的改革。

（4）数据标准匹配及汇聚

本项目将遵循公安部法综平台执法办案主题库标准，实现陕西省执法办案业务数据的生成、治理，并统一向部法综平台进行数据汇聚。涵盖范围广泛，包括人员、组织、场所、装备、物品、文书、笔录、卷宗、警情业务、案件业务、中心业务数据表。

（5）统一管理全省执法办案管理中心

本项目将实现省级层面统一的执法办案管理中心应用，业务内容覆盖案卷管理、涉案财物管理、办案区管理、音视频管理等，旨在规范执法管理业务，并有效整合基层相关数据，提升管理效能。

（6）提升公检法司对违法犯罪人员的监管业务协同

实现全省政法三级检察机关、人民法院、司法行政、监狱、司法矫正等部门在对诉讼当事人采取强制措施至刑罚执行、减假暂、司法矫正等刑事诉讼活动全过程的文书、函件、报告、批复等材料网上流转、监督、数据共享和业务协同。

政法协同办案系统，系统业务覆盖案件办理、政法协同、执法办案管理中心、智能笔录、智能电子卷宗、执法监督。系统业务覆盖层级为省、市、区县、派出所四级民警。

违法犯罪人员信息系统，业务包含收押接待、管理教育、巡视监控、医疗管理、所领导、分析研判等。系统业务覆盖层级为省、市、区县监管场所、监管支队、监管总队民警和分管领导。

2.3 信息化目标

1. 陕西省政法跨部门大数据办案平台（总平台）项目信息化目标

项目建设层级覆盖陕西省各政法机关办理刑事案件人员，包含协同办案服务系统、数据共享交换系统、统一消息平台、标准规范体系、安全体系、运营服务、运维服务和基础软硬件设施，通过相关信息化建设实现刑事案件线上协同流转，强化数据融合、持续深度汇聚政法各类数据，深化信息共享和执法监督应用，提升全省政法干警协同办案工作效率。

2. 陕西省公安机关执法办案综合管理平台信息化目标

（1）本期项目新建1套政法协同办案系统，系统业务覆盖案件办理、政法协同、执法办案管理中心、智能笔录、智能电子卷宗、阳光执法、执法监督。系统业务覆盖层级为省、市、区县、派出所四级民警。

（2）本期项目扩建1套违法犯罪人员信息系统，业务包含收押接待、管理教育、巡视监控、医疗管理、所领导、分析研判等。系统业务覆盖层级为省、市、区县监管场所、监管支队、监管总队民警和分管领导。

（3）本期项目硬件环境依托三秦警务云（信创云--新建）提供服务器资源与信创环境，不再单独采购。采购成品软件包括45套国产操作系统、16套国产数据库和5套中间件。

（4）本期项目的数据治理与共享建设，包括数据迁移和数据治理实施服务。

（5）本项目所需的应用支撑能力由陕西省公安厅三秦警务云（信创云--新建）统一提供，不再单独建设。项目建设中需要与三秦警务云（信创云--新建）公共支撑能力对接，包括新一代警综平台、警用地理位置综合服务系统和移动警务平台。

3. 标准及规范要求

3.1 标准规范

《新一代警综平台建设指南》（公安部）

《公安机关执法办案场所设置规范》（公通字〔2010〕56号）

《公安机关讯问犯罪嫌疑人录音录像工作规定》（公通字〔2014〕33号）

《公安大数据规范性技术文件汇编 第二部分：公安大数据处理》（GA/DSJ）

《公安大数据规范性技术文件汇编 第三部分：公安大数据安全》（GA/DSJ）

《公安大数据规范性技术文件汇编 第四部分：新一代公安信息网》（GA/DSJ）

《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）

《信息系统安全等级保护测评要求》（GB/T 28448-2019）

《信息安全技术网络安全等级保护定级指南》（GB/T22240-2020）

《公安数据元》（GA/T543.17-2018）

《信息安全技术信息系统密码应用基本要求》（GB/T 39786-2021）

《公共安全重点区域视频图像信息采集规范》（GB37300-2018）

《报警统计信息管理代码》（GA/T753.1~753.17-2008）

《常住人口管理信息规范》（GA214-2004）

《公安请求服务平台应用规范》（GA/T739-2007）

《共享数据项代码标准》（GA417.1-2003）

《数据交换格式标准编写要求》（GA/T1183-2014）

《数据项标准编写要求》（GA/T1053-2013）

《政务信息资源目录体系》（GBT_21063.5-2007）

《信息技术服务分类与代码》（GB/T 29264-2012）

《讯问同步录音录像系统技术要求》（GA/T882-2014）

《计算机信息系统保密管理暂行规定》（国保发〔1998〕1号）

《软件工程软件产品质量要求与评价（SQuaRE）SQuaRE指南》（GB/T 25000.1-2021）

《全卷宗规范》（DA/T 12-2012）

《纸质档案数字化规范》（DA/T 31-2017）

《电子档案管理基本术语》（DA/T 58-2014）

《录音录像档案数字化规范》（DA/T 62-2017）

公安部警察技术标准委员会《公安监管场所安全防范与信息管理系统技术要求》（GA/T1992-2022）

3.2其他编制依据

《国务院办公厅关于印发〈国家政务信息化项目建设管理办法〉的通知》（国办发〔2019〕57号）

《陕西省省级政务信息化项目实施方案编制指南（建设类）（试行）》（20230827印发）

《陕西省省级政务信息化项目投资编制指南（建设类）（试行）》（20230827印发）

4.建设范围

4.1采购清单

序号	产品名称	数量	单位	备注
一	应用系统			
1	政法协同办案系统	1	套	
1.1	政法协同	1	项	
1.2	案件办理	1	项	
1.3	执法办案管理中心	1	项	

1.4	智能笔录	1	项	
1.5	智能电子卷宗	1	项	
1.6	执法监督	1	项	
2	违法犯罪人员信息系统	1	套	
2.1	政法协同	1	项	
2.2	收押接待	1	项	
2.3	管理教育	1	项	
2.4	监控巡视	1	项	
2.5	医疗卫生	1	项	
2.6	所领导	1	项	
2.7	分析研判	1	项	
二	成品软件购置			
1	国产服务器操作系统	45	套	
2	国产数据库	16	套	
3	国产中间件	5	套	
4	数据治理工具	1	套	
三	数据资源建设			
1	数据治理服务	1	项	
四	数据迁移			
1	数据迁移服务	1	项	

4.2建设内容

4.2.1应用系统

陕西省公安机关执法办案综合管理平台项目建设，主要包含新建政法协同办案系统和升级改造违法犯罪人员信息系统（公安部金盾工程统一建设目录名称，以下统称“违法犯罪人员信息系统”）。

（1）政法协同办案系统（新建）

政法协同办案系统主要包含政法协同、案件办理、智能电子卷宗、执法办案管理中心、智能笔录、执法监督等模块。政法协同模块是本项目的核心，实现跨部门网上办案业务；案件办理、智能电子卷宗、执法办案管理中心、智能笔录模块是政法协同案件办理的业务支撑模块，为政法协同业务提供案、人、物、文书、证据材料、卷宗、笔录与音视频等数据；执法监督是为政法协同提供业务决策支撑，通过其他政法机关共享的数据（不/逮捕、不/起诉决定、判决、立案监督等）完善政法协同相关数据，从而提升系统的决策能力。

（2）违法犯罪人员信息系统（升级改造）

本期项目看守所侧是按照政法协同平台的安排建设协同流程及个流程节点，通过升级改造违法犯罪人员信息系统中其它流程和流程节点，实现违法犯罪人员信息系统在政法协同、收押接待、管理教育、监控巡视、医疗卫生、所领导、分析研判等功能。

1.4.2.2基础设施（成品软件）

本期项目成品软件采购需求如下：

成品软件需求表

序号	软件类型	数量	单位
----	------	----	----

1	国产服务器操作系统	45	套
2	国产数据库	16	套
3	国产中间件	5	套
4	数据治理工具	1	套

1.国产服务器操作系统

软件运行环境支持国产主流操作系统，需满足国产化环境适配。

2.国产数据库

国产主流数据库需满足国产化环境适配。

3.国产中间件

中间件支持国产主流中间件，需满足国产化环境适配。

4.数据治理工具

数据治理工具实现政法协同业务的主题库、专题库的数据治理。

4.2.3数据资源建设

数据资源体系建设包括数据标准规范、资源规划、数据接入、数据处理、数据治理。其中，数据治理服务包括数据调研，数据归集、数据清洗、数据标准化处理等内容，涉及人员、组织、物品、文书、笔录、卷宗、案件业务以及中心业务等类型数据。

4.2.4数据迁移

实现全省公安机关智慧法制平台和监管平台的历史数据库迁移到国产数据库中。

5.技术功能要求

5.1总体架构

5.1.1总体架构

投标人需提供本项目的总体架构设计及详细的设计方案。

5.1.2部署架构

投标人需提供本项目的部署架构设计及详细的设计方案。

5.1.3网络架构

投标人需提供本项目的网络架构设计及详细的设计方案。

5.1.4技术架构

投标人需提供本项目的技术架构设计及详细的设计方案。

5.1.5数据架构

投标人需提供本项目的数据架构设计及详细的设计方案。

5.1.6系统内外部交互

5.1.6.1系统外部关系

投标人需完成与陕西省政法跨部门大数据办案平台（总平台）数据资源共享交换平台的完整对接，需实现公安侧涵盖的政法协同流程节点与总平台的对接，实现刑事案件网上协同办理，案件、文书、人员、卷宗、涉案财物、音视频证据目录信息等各类办案信息均能从网上流通。

投标人需提供详细的对接方案。

5.1.6.2系统内部关系

投标人需完成与本次建设系统相关的已建/在建系统的对接，主要包括新一代警综平台、警用地理位置综合服务系统、移动警务平台等，详细对接要求如下：

需对接新一代警综平台，实现系统用户身份认证、组织机构、用户权限等验证服务。

需对接警用地理位置综合服务系统，获取发案详细地点、发案经纬度、地图显示等地理信息。

需对接移动警务平台，实现政法协同办案系统移动执法应用注册、上架、统一登录等。

投标人需完成与省级110平台、各警种业务系统、办案场所系统、部警综等平台的对接，详细对接要求如下：

需对接省级110平台接警单与处警单信息，生成警情信息；

需为各警种业务系统提供案件数据、文书数据以及业务数据；

需对接全省各级办案场所业务系统，实现各办案场所系统的数据汇聚；

需根据公安部数据规范要求，实现部警综、法综系统对接；

针对以上对接系统，投标人需提供详细的对接方案。

5.2应用系统

5.2.1应用系统概述

5.2.1.1政法协同办案系统

政法协同办案系统主要包含政法协同、案件办理、执法办案管理中心、智能笔录、智能电子卷宗、阳光执法和执法监督模块。政法协同模块是本项目的核心，实现跨部门网上办案业务；案件办理、智能电子卷宗、执法办案管理中心、智能笔录模块是为政法协同办理流程提供业务支撑，为政法协同业务提供案、人、物、文书、证据材料、卷宗、笔录与音视频等数据支撑；阳光执法、执法监督是为政法协同提供业务决策支撑，通过其他政法机关共享的数据（不/逮捕、不/起诉决定、判决、立案监督等）完善政法协同相关数据，从而提升系统的决策能力。

政法协同：主要功能包括一体化协同办案桌面、协同业务流程等功能，新建政法协同流程。

案件办理：主要功能包括警情管理、当场处罚、行政快办、行政案件、刑事案件、刑事复议复核、行政复议、国家赔偿、法综数据上报、知识详情服务、智能帮助服务、智能搜索服务、三个规定直报、送押送拘、远程提讯、印章管理、移动执法等功能。

智能电子卷宗：主要功能包括材料导入、卷宗配置、自动组卷、人工组卷、卷宗封面、电子书签、电子标记、阅卷日志等功能。

执法办案管理中心：主要功能包括案卷管理、涉案财物管理、办案区管理、音视频管理及办案区系统数据汇聚等业务功能。

智能笔录：主要功能包括笔录制作、笔录管理、远程提讯、权利义务告知书、笔录人员管理、辨认照片库、法律法规等功能。

执法监督：主要功能包括预警闭环管理、巡查问题闭环、执法考评、执法档案、执法白皮书等功能。

政法协同办案系统整合了执法办案的各个环节，提供了全方位的服务和支持，有助于提高执法效率、加强监督管理，实现政法协同和信息共享，为维护社会治安和法律权益提供了强大的技术支撑。

5.2.1.2违法犯罪人员信息系统

本期项目看守所侧是按照政法协同平台的安排建设协同流程及个流程节点，通过升级改造违法犯罪人员信息系统中其它流程和流程节点，实现违法犯罪人员信息系统在政法协同、收押接待、管理教育、监控巡视、医疗卫生、所领导、分析研判等功能。

政法协同：主要功能包括一审公诉、二审上诉、二审抗诉、审理期间交互、暂予监外执行、社区矫正解除矫正、变更羁押期限通知等与公检法部门的业务流程线上处理。

收押接待：主要功能包括公安入所、检察院入所、法院入所业务，收押接待包括送押监所需知、刑拘入所、逮捕入所、收押、拒收整个流程管理，规范加快监所收押业务办理进度

管理教育：主要功能包括安置帮教、社区矫正、权益和义务告知、重点管控分析等业务，旨在通过管教并举的形式教育感化被监管人员，提高监所被监管人员的管理水平。

监控巡视：主要功能包括巡视记录、行为规范等功能。

医疗卫生：主要功能包括五项体检、伤情检查、危重疾病、传染病、诊断和治疗文书材料等，规范加强监所医疗管理。

所领导：主要功能包括预警信息、法治规范监督等功能，帮助所领导监督监所业务办理情况。

分析研判：主要包括风险预警评估模型，由风险人员分析、风险监室分析、风险监所分析全维度进行监所风险评估。

5.2.2系统功能要求

5.2.2.1政法协同办案系统

（1）政法协同

本次系统建设需符合协同办案要求的**协同业务流程、协同音视频、一体化协同工作桌面**，对接并实现协同业务的发起和处理。

协同业务流程：本项目需新建政法协同的协同流程，包含逮捕、不捕异议、变更强制措施等流程，投标人需提供详细的流程设计方案。

协同音视频：本项目建设的音视频管理模块不存储媒体文件，仅保存结构化数据，各地数据本地保存，结构化数据统一汇聚至省厅管理。政法协同推送时，将下载地址与协同数据一起推送至大数据办案平台，由其获取并转发音视频文件至相关政法单位。

一体化协同办案桌面：建设内容需包含协同工作台、协同待办提醒、协同流程标准管理、协同数据统计、协同交互跟踪、协同业务处理。

协同对接：对接内容需包括机构用户同步接口、单点认证接口、流程发起处理、退回接口、流程数据同步接口、消息通知接口、消息接收接口、文件上传接口（可批量）。

案件办理

主要包括警情管理、当场处罚、行政快办、行政案件、刑事案件、刑事案件复议复核、行政案件复议、国家赔偿、知识详情服务、智能帮助服务、智能搜索服务、三个规定直报、送押送拘、远程提讯、印章管理、数据上报、移动办案。

▲为充分保障本项目行政快办功能模块的开发及交付，投标人需提供同类行政案件快速办理软件著作权证书（复印件或扫描件）。

执法办案管理中心

主要包括案卷管理、涉案财物、办案区、音视频管理、办案场所数据汇聚。

▲为充分保障本项目执法办案管理中心模块的开发及交付，投标人需提供同类执法办案管理中心管控平台软件著作权证书（复印件或扫描件）。

▲为充分保障本项目智能案卷管理功能模块的开发及交付，投标人需提供同类智能案卷管理软件著作权证书（复印件或扫描件）。

智能笔录

主要包括笔录服务器管理、笔录客户端管理、笔录方案模板管理、权利义务告知书、法律法规、笔录组件配置、笔录资源管理、辨认照片库、远程提审、笔录管理、笔录人员管理、笔录制作。

▲为充分保障本项目智能笔录功能模块的开发及交付，投标人需提供同类智能笔录软件著作权证书（复印件或扫描件）。

▲为充分保障本项目远程提审功能模块的开发及交付，投标人需提供同类远程提审系统软件著作权证书（复印件或扫描件）。

▲为充分保障本项目笔录制作功能模块的开发及交付，投标人需提供同类数字签名软件著作权证书（复印件或扫描件）。

智能电子卷宗

主要包括材料导入、卷宗配置、自动组卷、人工组卷、卷宗封面、电子书签、电子标记、电子批注、阅卷日志、智能阅卷。

▲为充分保障本项目智能电子卷宗功能模块的开发及交付，投标人需提供同类智能电子卷宗软件著作权证书（复印件或扫描件）。

执法监督

主要包括预警生成、预警闭环管理、执法考评管理、执法考评情况统计分析、综合查询、执法档案、执法白皮书。

▲为充分保障本项目执法监督模块的开发及交付，投标人需提供执法（管理）考评/评价/考核同类专利

▲为充分保障本项目执法监督模块的开发及交付，投标人需提供执法/办案预警同类专利。

5.2.2.2 违法犯罪人员信息系统

违法犯罪人员信息系统是陕西省公安监管部门、各市公安监管支队、全省公安监所的业务应用信息管理系统，同时按照规划通过新建政法协同办案系统对接。主要包括公安监管业务协同、数据协同、日志管理等基础功能模块，实现违法犯罪人员信息系统与全省政法三级检察机关、人民法院、司法行政、监狱、司法矫正等部门在对诉讼当事人采取强制措施至刑罚执行、减假暂、司法矫正等刑事诉讼活动全过程的信息交互、业务协同，并建立全流程接受人民检察院监督的业务协同智能应用体系，真正实现陕西省政法各部门刑事诉讼案件和公安机关刑事办理的网上流传、数据共享、业务协同，实现全省监管部门资源统一管理和统一调度，承担公安监管数据汇聚、融合、治理、存储、计算和深度应用的任务，支撑省厅监管部门、各市监管支队、公安监所的警务实战应用。

本项目建设包含政法协同、收押接待、管理教育、监控巡视、医疗卫生、所领导、分析研判。

（1）政法协同

一审公诉：庭审判前的准备。在开庭前，将起诉书副本送达被告。将开庭的时间通知人民检察院和看守所。

二审上诉：当事人不服一审法院判决或裁定时，有权在判决书送达之日起十五日内(裁定为十日)向上一级人民法院提起上诉。上诉原则上应提交书面上诉状，但也可以口头提出。

二审抗诉：对同级人民法院的第一审判决或裁定不服时，可以通过原审人民法院向上一级人民法院提出抗诉书。抗诉书应同时抄送上一级人民检察院。

审理期间交互：接收。接收再审信息、解析再审信息、再审信息增加、再审信息修改、再审信息更新、再审信息删除、再审信息查询、导出再审信息材料、再审信息查看、更新在押人员当前办案单位信息、更新在押人员当前办案人信息、更新在押人员当前关押期限信息。

暂予监外执行：暂予监外执行文书增加、暂予监外执行文书修改、暂予监外执行文书更新、暂予监外执行文书删除、暂予监外执行文书查询、导出暂予监外执行文书材料、暂予监外执行文书详情查

看

社区矫正解除矫正：接收。原服刑或接收、存放其档案的看守所接收通知办理释放手续。

变更羁押期限：接收变更羁押期限、解析变更羁押期限、变更羁押期限增加、变更羁押期限修改、变更羁押期限更新、变更羁押期限删除、变更羁押期限查询、导出变更羁押期限、移送变更羁押期限、更新在押人员当前办案单位信息、更新在押人员当前办案人信息、更新在押人员当前关押期限信息

（2）收押接待

主要包括送押监所须知、刑拘入所、逮捕入所、收押、拒收、拒收凭证、提讯、律师会见等功能。

（3）管理教育

主要包含：三固定、谈话教育、械具使用、禁闭管理、单独关押。

（4）监控巡视

主要包含：巡视记录、行为规范。

（5）医疗卫生

主要包含五项体检、伤情检查、危重疾病、传染病、诊断和治疗文书材。

（6）所领导

主要包含预警信息：未及时谈话、超时提讯、出所未归、提讯未归、羁押到期、公安未及时入所、检察院未及时入所、法院未及时入所监测预警；

法治规范监督：收押入所流程闭环监督、羁押期限预警监督、提讯流程规范监督、提解流程规范监督、出所流程规范监督、械具使用流程规范监督、管教谈话监督、医疗卫生工作监督。

（7）分析研判

主要包含风险人员分析：一级风险人员、二级风险人员、三级风险人员；

风险监控室分析：一级风险人员、二级风险人员、三级风险人员；风险监控所分析：一级风险人员、二级风险人员、三级风险人员。

5.3总体要求

5.3.1设计要求

设计思路清晰、整体方案完整，符合本项目的建设内容。方案总体架构和技术架构设计科学合理、层次清楚、特色鲜明、描述详细、无缺漏，符合软件测评、审计、密评、等保要求。

5.3.2软件要求

5.3.2.1开发原则

1、模块化

软件开发做到层次鲜明和模块化设计，以提高软件开发的进度及软件系统的信赖性和可维护性，模块逻辑上相对独立，大小要适中，高内聚、低耦合。

2、整体性

软件开发应遵循相关国家标准和行业标准，各模块的功能规范，数据采集统一，语言描述一致，内外部接口一致，信息资源共享，保证各模块协同工作。

3、扩展性

软件开发应对外界条件的变化有较强的适应能力和扩展能力，软件结构具有较好的灵活性和可重用性，能够实现功能重组、扩充，保持整体稳定性。

4、可靠性

软件开发应能完全满足大并发量、大用户量的应用需求，要保证软件系统的稳定性；要保证数据采集的质量；具备数据校验功能；有效处理错误输入。

5.3.3技术要求

要求符合公安部新一代警综应用平台建设指南中要求的微服务架构方式进行构建，实现系统中的多项服务需求。微服务之间松耦合，内部高内聚，每个微服务组件简单灵活，能够独立部署，并易于以后按需扩展。

技术架构要求可以有效地实现应用系统的模块化、可扩展性、高可用性等特性，提高开发效率和系统性能，满足项目需求。同时，还可以根据具体情况进行技术组件的选型和定制化开发，以满足项目的特定需求。

5.3.4性能要求

5.3.4.1政法协同办案系统性能要求

5.3.4.1政法协同办案系统性能要求

（1）用户并发数要求

系统支持平均登录并发要求：不小于800。

系统支持峰值登录并发要求：不小于1200。

（2）在线人数要求

系统支持最高同时在线人数：不小于1500

（3）响应性能要求

1.交互类业务平均响应时间 ≤ 2 秒，峰值平均响应时间 ≤ 4 秒。

2.查询业务简单查询平均响应时间 ≤ 2 秒，峰值平均响应时间 ≤ 4 秒；复杂查询平均响应时间 ≤ 3 秒，峰值平均响应时间 ≤ 5 秒。

（4）可用性指标要求

1）稳定性要求

对于本项目中的各个业务系统，要求采用高可靠的硬件配置确保平台的长期稳定运行，提供7×24小时不间断服务，系统可用性 $>99\%$ ，数据库需做好相应的备份和恢复策略。

2）可扩展性要求

本项目是全省公安行业基础性、综合性业务应用平台，对系统内部和外部的可扩展性要求非常高，除需要满足与现有业务系统的集成整合外，还要满足后续规划建设信息系统的数据交换和功能接入需要。并且，不仅要满足全省公安系统内各部门、各业务系统间的数据交换需求，还要满足公安与政法部门的数据交换需求。

3）可操作性要求

为使平台满足各类用户的应用需求，所有功能模块的操作终端应具有较强的可操作性。要求界面设计友好，简单易用，同时符合用户的业务操作习惯，最大限度的降低系统使用的复杂程度。

5.3.4.2违法犯罪人员信息系统性能要求

（1）用户并发数要求

1）系统支持平均登录并发要求：不小于150。

2）系统支持峰值登录并发要求：不小于200。

（2）在线人数要求

系统支持最高同时在线人数：不小于500

（3）响应性能要求

- 1) 交互类业务是指日常工作中在系统进行的业务处理，如录入，修改或删除一条记录、发布一条信息等操作。平均响应时间≤2秒，峰值平均响应时间≤4秒。
- 2) 查询业务简单查询平均响应时间≤2秒，峰值平均响应时间≤4秒；复杂查询平均响应时间≤3秒，峰值平均响应时间≤5秒。

(4) 可用性指标要求

1) 稳定性要求

对于本项目中的各个业务系统，要求采用高可靠的硬件配置确保平台的长期稳定运行，提供7×24小时不间断服务，系统可用性>99%，数据库需做好相应的备份和恢复策略。

2) 可扩展性要求

本项目是全省公安行业基础性、综合性业务应用平台，对系统内部和外部的可扩展性要求非常高，除需要满足与现有业务系统的集成整合外，还要满足后续规划建设信息系统的数据交换和功能接入需要。并且，不仅要满足全省公安系统内各部门、各业务系统间的数据交换需求，还要满足公安与政法部门的数据交换需求。

3) 可操作性要求

为使平台满足各类用户的应用需求，所有功能模块的操作终端应具有较强的可操作性。要求界面设计友好，简单易用，同时符合用户的业务操作习惯，最大限度的降低系统使用的复杂程度。

5.3.5 支撑平台标准

5.3.5.1 部署资源要求

本项目的所有业务系统均由三秦警务云（信创云）提供系统部署资源，以满足本次项目建，投标人需根据本次项目业务需求、业务系统功能需求、数据资源需求、网络安全需求、系统性能需求等分析情况，提供政法协同办案系统、违法犯罪人员信息系统、政法云公安端系统各自部署资源的测算依据，以满足本次项目建设需要。

5.3.5.2 成品软件要求

本项目需采购的成品软件资源如下：

成品软件需求表

序号	软件类型	数量	单位
1	国产服务器操作系统	45	套
2	国产数据库	16	套
3	国产中间件	5	套
4	数据治理工具	1	套

投标人需根据本项目的实际业务需求，提供政法协同办案系统、违法犯罪人员信息系统、政法云公安端成品软件的具体部署方案，以满足本次项目建设需要，并给出资源规划使用的依据。

5.3.6 规范性要求

5.3.6.1 命名规范

软件开发应遵循编程语言及技术架构的标准编程规范，对于方法、变量等方面的命名严格遵守编程规范，以描述性以及唯一性来命名，保证资源之间不冲突，同时源代码须给予详细注释，增加程序可读性。

5.3.6.2 数据库设计文档

软件开发必须详细的列举出软件所调用的数据库中的表及其各字段的含义和定义，表明各个表之间的关系。

5.3.6.3用户文档

用户文档应包括软件使用所需设置信息、产品所有功能说明、程序中用户可调用的所有功能说明、软件安装所需要的信息、软件维护所需要的信息等，要求描述准确，没有歧义，术语一致，与软件实际操作相符，清晰易读。

5.3.7数据要求

5.3.7.1数据资源建设要求

数据资源建设具体包括数据标准规范、数据集成服务、数据清洗服务、数据开发服务、数据融合服务、数据质量服务、数据共享服务等。

投标人需提供数据资源设计方案，包括数据标准规范、资源规划、数据接入、数据处理、数据治理，建立陕西省政法数据资源体系。

数据标准规范设计要求

投标人需依据公安部《全国执法办案数据汇聚技术规范》以及本期项目数据协同与规范化治理需求的标准规范，提供数据标准规范设计方案，保障项目数据治理的数据管理规范性和技术规范性。

数据资源规划设计要求

本系统数据来源于110接处警、智慧法制平台、本系统所生成、政法单位系统生成。其中，非结构化数据包括文书、证据材料、音视频等；结构化数据包括警、案、人、物、卷宗等信息。针对以上数据资源，投标人需提供数据资源规划设计方案。

3、数据接入要求

本项目需接入的数据主要包括“智慧法制”平台等业务数据以及政法协同办案系统的业务数据，投标人需对原有系统的数据进行迁移和汇聚，并建立统一的数据采集标准，对历史数据进行去重、补缺处理，全面汇聚执法监督相关业务数据资源。

4、数据处理要求

由于公安执法业务数据资源种类多样，投标人需要提供覆盖数据处理逻辑的集成设计、开发、调试、部署、运行、管理和监控各生命周期不同阶段的数据处理工具，对接入的数据内容进行探查、提取、清洗、转换、关联、比对、标识、融合等处理，并建立标准化的数据处理模式与流程。

5、数据治理服务要求

为了保障政法协同数据规范，同时满足公安部新一代警综平台、法综平台数据规范要求，需要对陕西省政法系统涉及相关数据进行数据治理服务。

5.3.7.2数据交换共享要求

投标人需提供数据交换共享方案，包括与外部（检察院、法院、司法）数据资源共享内容及交换方式、内部（公安侧与监管侧）数据资源共享内容及交换方式、数据资源目录和数据共享的算力和存储资源，并给出详细的测算依据。

5.3.7.3数据迁移要求

1、结构化数据迁移要求：

为了确保新系统能够完全兼容现有系统的业务需求，确保现有业务逻辑不被数据迁移所干扰，需对原系统的数据进行梳理，完成历史数据整合迁移，同时，实现系统切换时期的增量数据同步。投标人需提供详细的数据迁移方案。

2、非结构化数据迁移要求：

要求法制对卷宗、文书等非结构化数据完成迁移，监管对人员照片数据完成迁移，投标人需提供

详细的数据迁移方案。

5.3.8安全要求

本项目应遵循国家信息安全等级保护相关规定和技术要求，本次招标项目的信息安全要求如下：

1. 严格遵循国家信息安全等级保护相关管理规定和技术要求，系统平台应符合国家信息安全等级保护第三级相关要求；

2. 严格遵循国家保密相关管理规定和技术要求，系统平台应均应满足三级密评相关要求。

5.3.9部署要求

投标人需提供详细的系统部署方案，包括环境要求、安全、兼容性、存储等内容，其中，存储需满保证数据存储的全面性和稳定性，当发生事故时能快速有效恢复数据。

5.3.10项目管理要求

投标人必须成立项目组织、明确责任、严格按照信息化项目管理的有关规定进行项目管理，保证项目质量、确保项目如期完成。

5.3.10.1质量管理

投标人应建立严格的质量保证体系，制定项目开发建设质量控制方案和实施措施，并督促落实各环节质量控制内容和目标；保证总体规划设计、开发与实施、系统运行与验收各个阶段工作满足招标方对质量的要求。

投标人应根据整个开发的工作计划，对阶段性工作成果进行审查和测试，并向项目单位提交里程碑式工作成果。通过保证各阶段性成果的质量，最终保证整个系统集成、开发的质量。

投标人应按照监理单位对项目质量管理要求，提供项目阶段性质量测试报告。

投标人提供的应用软件应符合软件测评方案、审计、密评、等保等相关要求。

投标人应提供一套完整的问题管理平台，用于收集、流转、统计、反馈、管理项目建设、试运行、质保期间用户提出的各类问题、意见、建议。

投标人必须提供用于该项目的项目经理及组成开发小组、协调人、主管经理的人员名单，并且提供人员的基本情况和以往业绩，其中项目经理在项目开发过程中不能变更，开发人员的变化情况应控制在10%以内。

5.3.10.2进度管理

投标人需提供详细的项目进度管理计划表，并配套合理的进度管理措施。

5.3.10.3文档管理

需建立完善的文档管理体系，文档体系参照陕西省数据局相关标准，包括文件命名规范、目录规范、文件传递规则等。在规定时间内向招标人提交项目建设需求调研、设计、开发、测试、实施各个阶段的计划、方案、报告、质量标准、项目进展状态及文档。

项目结束后，中标方按照本标书要求把项目相关文档全部移交给招标人。

5.3.10.4其它要求

5.3.10.4.1运行维护系统要求

1、运维组织

（1）组织架构：运维团队应设立专门的管理平台运维小组，负责集群的日常运维、故障处理、性能优化等工作。小组内分工明确，包括集群管理员、网络管理员、存储管理员等。

（2）人员配备：运维人员需具备丰富的管理平台使用经验，熟悉集群部署、配置、升级等操作流程。同时，应具备良好的沟通能力和团队协作精神。

2、运维管理规范

（1）标准化流程：制定详细的管理平台运维流程，包括集群初始化、应用部署、资源调度、故

障恢复等。确保每一步操作都有明确的指导文档和最佳实践。

(2) 配置管理：采用集中式的配置管理方式，对集群配置进行统一存储和版本控制。确保配置变更可追溯、可审计。

(3) 变更管理：对任何影响集群稳定性和性能的变更操作，应经过严格的评审和测试流程，确保变更的安全性和有效性。

3、运维服务内容

投标人需提供以下运维服务内容

(1) 软件安装与配置：包操作系统、数据库、中间件等软件的安装与配置。

(2) 软件部署与更新：负责软件系统的安装、部署和更新，确保应用程序在各个环境中的正确性、稳定性和可靠性。

(3) 性能优化：对应用程序进行性能监控和优化，以提高系统的响应速度和用户体验。

(4) 系统运维：包括操作系统维护、数据库管理、中间件管理等内容。

(5) 故障处理与恢复：负责软件系统的故障排查、处理和恢复工作，确保系统尽快恢复正常运行。

(6) 版本管理与升级：通过版本管理工具对软件的相关版本进行管理，并在需要时进行软件的升级和补丁的安装。

4、运维服务提供方式

(1) 现场驻点：开发公司派驻5名维护人员在陕西省公安厅3年的现场驻点，在法定节假日期间提供现场维护。

(2) 定期巡检：定期对集群进行巡检，检查集群状态、配置、安全等方面的问题，并提前预防潜在风险。

(3) 培训与交流：全省每个地市公安机关至少现场培训一轮次，且定期举办全省技术培训和交流活动，提升用户的管理平台使用水平和问题解决能力。

5.3.10.4.2备份策略要求

投标人需按照等保三级的标准规范设计数据备份方案，遵循相关安全要求和技术标准，以确保数据的安全性、完整性和可用性。

本项目业务系统搭建于省信息化数据中心，依托三秦警务云（信创云--新建）现有“两地三中心容灾”能力，实现灾难发生时实时切换到同城灾备数据中心保持业务运行，或灾后从异地灾备数据中心恢复业务系统。

投标人需要设计出详细合理的系统和业务数据备份方案，以确保发生灾难时，可以安全、迅速、完整地恢复业务数据和信息，方案需要至少满足以下要求：

备份和灾难恢复功能全部测试通过；

分别制作应对策略，当发生黑客袭击、员工疏忽或者蓄意破坏、自然灾害时，当IT组件故障、尤其是服务器和存储系统故障时，以及当采取新技术而IT需求不断变化，如虚拟化技术等各种情况出现时，防止数据丢失。

对于各个关键系统，定期对日常业务相关的文件系统进行备份。保证1周为一个备份周期，每天定时在线增量备份关键文件系统，周末做关键文件系统的全备份，在线保留两周的数据。

5.3.11文档资料要求

5.3.11.1对文档资料的整体要求

1、技术文档应与系统相一致，技术文档应该全面、完整、详细；

2、技术文件应能够满足招标人对系统的使用、运行维护、应用开发的需要；

	<p>3、提供整个系统建设的技术管理文档，系统运行、维护管理体系对应的管理规范和管理规定的文档；</p> <p>4、技术文档应符合招标文件所述的功能和技术要求，提供在指定平台上可靠运行的并经测试合格的应用软件；</p> <p>5、提供的文档和资料均应以纸张和磁介质（或光盘）为载体，文件格式为OFD文档或其他可视化文件。</p> <p>5.3.11.2需要提交的资料</p> <p>1、需求调研：《需求分析说明书》、《项目计划书》等；</p> <p>2、设计阶段：《总体设计说明书》、《系统概要设计说明书》、《详细设计说明书》、《数据库设计说明书》、《接口数据规范》等；</p> <p>3、开发阶段：《用户操作手册》、《系统维护手册》等；</p> <p>4、测试阶段：《测试计划》、《测试报告》等；（含功能测试、性能测试）</p> <p>5、实施阶段：《实施报告》、《验收报告》、《培训计划》等；</p> <p>6、运行阶段：《系统运行维护管理规定》、《系统数据维护管理制度》等。</p> <p>5.3.12保密和知识产权要求</p> <p>5.3.12.1保密要求</p> <p>中标方应无条件对接触到的公安数据做好保密工作，不得对外泄漏有关审判工作信息，并承担相应的泄密责任。</p> <p>中标方提供的产品应该完全解决可能出现的相关安全问题，对可能出现的安全问题需提处详细的解决方案和具体措施。</p> <p>5.3.12.2知识产权</p> <p>采购方拥有本项目开发的应用软件的知识产权，项目验收时，中标方应提交涉及该项目所有的计算机程序及相关文档。</p>
--	--

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：服务

参数性质	序号	技术参数与性能指标
		<p>1.项目背景：</p> <p>为进一步响应中央政法委总体部署要求，深入贯彻落实省政法跨部门大数据办案平台项目建设专题会议精神，加快实现政法各部门信息资源共享，实现刑事案件网上协同办理，提升刑事案件跨部门办理质效。</p> <p>按照陕西省《数字政府建设“十四五”规划》，以及省委改革办关于新发展阶段推进创新型、引领型改革的工作部署，坚持以问题导向、需求导向、目标导向为原则，以政法协同办案流程、节点为依托，设计公安部门数据协同标准和规范，并满足信创要求，构建具有陕西特色的政法一体化协同办案体系。</p> <p>2.建设目标：</p> <p>2.1陕西省公安机关执法办案综合管理平台部署环境项目建设，通过分层解耦、异构兼容、充分利用现，扩容用户域“三秦警务云-信创域”，为“执法办案综合管理平台”和“违法犯罪人员信息系统”提</p>

供安全、稳定、易用的信创云运行环境。

2.2通过扩容国产化大数据平台组件，优化计算与存储资源，为数据的进一步融合、治理、共享提供支撑。

3.建设规模：

陕西省公安机关执法办案综合管理平台部署环境需求项目，建设规模包括基础设施服务（IaaS）、平台服务（PaaS）、安全保障体系。项目建成后，为执法办案综合管理平台和违法犯罪人员信息系统提供运行环境并实现全省民警对该业务系统的访问和使用。

3.1基础设施服务（IaaS）：用户域“三秦警务云-信创域”，建设20个信创云虚拟化服务器，共计1280CPU核心、10TB内存的计算能力；4台GPU服务器；1584TB（裸容量）信创云分布式存储、扩容集中式存储948TB容量；1套信创云备份系统；8台48口万兆交换机，6台万兆交换机，6台48口千兆交换机。

3.2平台服务（PaaS）：平台服务，包括扩容离线、内存计算、共计13节点与1套OCR识别软件。

3.3安全保障体系：2台国产化下一代防火墙，1台云平台安全一体机，2台便民应用安全接入服务系统保障信创云资源区的安全建设。

4.技术参数与性能指标：

4.1硬件产品购置

序号	设备名称	技术参数				数量	单位
		序号	指标分类	一级指标	二级指标	指标要求	
		1	产品类型	产品类型	产品属性	产品为2路机架式服务器，高度≤2U；	
		2	产品规格	CPU规格	★CPU信息	实配两颗国产高性能服务器级别CPU，每颗CPU核心数量：≥24核；线程数：≥24线程；基础频率：≥2.2GHz；	
		3	产品规格		★主板支持的CPU和内存情况	国产高性能服务器级别CPU内存型号：16G/32G/64G DDR4 ECC RDIMM	
		4	产品规格		主板内存槽数量	非板载内存的可扩展插槽数量应不少于16个	

5	产品规格	主板规格	主板存储接口	至少支持 SATA、SAS、M.2、U.2 等存储接口中的1种
6	产品规格		★PCIe 插槽接口	符合 PCIe3.0 或以上的高速串行计算机扩展总线标准，PCIe的接口速率与位宽需保证向下兼容
7	产品规格		主板PCIe插槽数量及规格	≥5个标准PCIe 4.0插槽,标卡槽位
8	产品规格	内存规格	内存数量	实配容量不小于8*16GB，所有物理内存品牌型号一致。
9	产品规格		内存规格	≥DDR4 3200MHz
10	产品规格	存储规格	硬盘实配容量	配备固态硬盘，实配固态硬盘单盘容量不小于480GB SATA SSD； 配备固态硬盘1，实配固态硬盘单盘容量不小于1.92TB SATA SSD；
11	产品规格		★硬盘实配数量	a) 配备固态硬盘，实配盘数应不小于2 b) 配备固态硬盘1，实配盘数应不小于2
12	产品规格		★硬盘插槽数量及规格	≥8个2.5寸热插拔硬盘槽位
13	产品规格	RAID卡规格	RAID卡支持的SAS接口数	≥8
14	产品规格	网络规格	★网口速率和数量	配备RJ45网口数量不少于4个，且网口速率不少于1GE 配备SFP+网口数量不少于4个，且网口速率不少于10GE

1	信创云管理服务器	15	产品规格	格	★网络接口	配置千兆网口≥4（2块双口千兆网卡或1块4口千兆网卡），网卡自带控制芯片配置≥2块10Gb以太网双口光口网卡（满配多模光模块），网卡自带控制芯片
		16	产品规格	外部接口规格	显示接口	≥1个VGA接口
		17	产品规格		USB 接口	配备USB3.0接口
		18	产品规格	电源规格	电源冗余模式	整机电源模块按 1+1 冗余或 N+1冗余配置
		19	产品规格		电源功率	电源模块功率应有一定冗余，满足服务器满载时的需求
		20	功能要求	网络功能	网络功能	支持网络连接、网络访问、数据交换和网络管控功能
		21	功能要求	CPU功能	计算处理	支持通用计算及虚拟化功能。处理器需集成整型计算单元、浮点计算单元、内存控制器、I/O 模块等，处理器与存储部件、网络部件、I/O部件等组成计算系统，提供数据处理、网络接入等计算相关功能
		22	功能要求		密码算法实现	CPU 芯片应符合GM/T 0008 的相关规定，或芯片密码模块应符合GB/T37092 或GM/T 0028 的相关规定
		23	功能要求	RAID卡功能	RAID卡RAID级别支持	RAID模式支持 RAID 0/1/10/5，存储型支持 RAID 0/1/5/6/10/50/60,实配同时支持直通和RAID模式
					3	台

24	功能要求		RAID卡 BBU单元	RAID 卡支持电池或电容备份单元
25	功能要求	电源功能	电源热插拔	整机电源模块应具备热插拔功能
26	功能要求	管理系统功能	★BMC 固件基础功能	1) 支持DHCP 设置网络功能； 2)支持静态IP 设置网络功能； 3)支持设备日志记录，包括但不限于登录日志、操作日志和报警日志等功能； 4)支持日志信息导出和记录删除功能； 5)支持通过管理接口向外输出准确的报警信息功能； 6)设备的BMC 管理软件应能够按报警的严重程度进行区分；
27	功能要求		★BIOS 固件基础功能	a) 支持查看固件版本、内存信息、主板信息、处理器信息和系统时间信息功能； b) 支持上电初始化界面显示CPU 信息、内存信息、固件版本和部分快捷键信息功能； c) 支持设置界面中英文显示切换功能； d) 支持查看PCIe 设备信息，SATA设备信息功能； e) 支持操作系统安装和引导功能，应向操作系统提供计算机主板信息和服务接口； f) 支持设置启动顺序，并按照设置的启动顺序启动功能； g) 支持安全启动功能；
28	功能要求		★操作 系统及 驱动的 升级	支持通过网络、闪存盘对操作系统、驱动进行升级
		操作系统及驱动功能		

29	功能要求		★操作系统功能	a) 支持访问控制、安全审计、网络接入鉴别等功能； b) 操作系统其他功能应满足操作系统政府采购需求标准中加*的指标要求
30	安全要求	关键部件安全要求	★关键部件安全要求	CPU 和操作系统等关键部件应当符合安全可靠测评要求
31	性能要求		单CPU 末级缓存容量	≥16MB
32	性能要求	内存性能	内存速率	≥3200MT/s
33	服务要求	服务响应	服务响应	a)提供电话、电子邮件、 远程连接等多种 形式服务； b) 提供5年原厂服务(存储介质不返还) ； 若硬件故障需提供备件4小时内到达现场 硬件保修和人工服务；免费软件升级 ； c) 提供设备安装、调试等原厂施工服务 ， 建立全国技术服务体系和服务团体， 符合专业服务体系标准要求，提供原厂 中文服务； d) 服务周期内提供产品的维修、换件和 升级服务，能在设备故障时提供同等备 机备件服务
34	服务要求		★培训服务	供应商提供培训材料、产品手册、培训 视频等培训相关内容

序号	指标分类	一级指标	二级指标	指标要求
1	产品类型	产品类型	产品属性	产品为2路机架式服务器，高度≤2U；
2	产品规格	CPU规格	★CPU信息	实配两颗国产高性能服务器级别CPU，每颗CPU核心数量：≥32核；线程数：≥32线程；基础频率：≥2.6GHz；
3	产品规格	主板规格	★主板支持的CPU和内存情况	国产高性能服务器级别CPU内存型号：16G/32G/64G DDR4 ECC RDIMM
4	产品规格		主板内存槽数量	非板载内存的可扩展插槽数量应不少于16个
5	产品规格		主板存储接口	至少支持 SATA、SAS、M.2、U.2等存储接口中的1种

6	产 品 规 格		★PCIe插槽 接口	符合 PCIe3.0 或以上的高速串行计 算机扩展总线标准，PCIe的接口速 率与位宽需保证向下兼容
7	产 品 规 格		主板PCIe插 槽数量及规 格	≥5个标准PCIe 4.0插槽,标卡槽位
8	产 品 规 格	内存规 格	内存数量	实配容量不小于16*32GB，所有物 理内存品牌型号一致。
9	产 品 规 格		内存规格	≥DDR4 3200MHz
10	产 品 规 格	存储规 格	硬磁盘实配 容量	配备固态硬盘，实配固态硬盘单盘容量 不小于480GB SATA SSD；
11	产 品 规 格		★硬盘实配 数量	a) 配备固态硬盘，实配盘数应不小于 2
12	产 品 规 格		★硬盘插槽 数量及规格	≥8个2.5寸热插拔硬盘槽位
13	产 品 规 格	RAID 卡规格	RAID卡支持 的SAS接口 数	≥8
14	产 品 规 格	网络规 格	★网口速率 和数量	配备RJ45网口数量不少于4个，且网 口速率不少于1GE 配备SFP+网口 数量不少于6个，且网口速率不少于 10GE

[illegible]

24	功能要求	卡功能	RAID 卡 BB U 单元	RAID 卡支持电池或电容备份单元
25	功能要求	电源功能	电源热插拔	整机电源模块应具备热插拔功能
26	功能要求	管理系统功能	★BMC 固件基础功能	1) 支持DHCP 设置网络功能； 2)支持静态IP 设置网络功能； 3)支持设备日志记录，包括但不限于登录日志、操作日志和报警日志等功能； 4)支持日志信息导出和记录删除功能； 5)支持通过管理接口向外输出准确的报警信息功能； 6)设备的BMC 管理软件应能够按报警的严重程度进行区分；
27	功能要求		★BIOS 固件基础功能	a) 支持查看固件版本、内存信息、主板信息、处理器信息和系统时间信息功能； b) 支持上电初始化界面显示CPU 信息、内存信息、固件版本和部分快捷键信息功能； c) 支持设置界面中英文显示切换功能； d) 支持查看PCIe 设备信息，SATA 设备信息功能； e) 支持操作系统安装和引导功能，应并向操作系统提供计算机主板信息和服务接口； f) 支持设置启动顺序，并按照设置的启动顺序启动功能； g) 支持安全启动功能；
28	功能要求	操作系统及驱	★操作系统及驱动的升级	支持通过网络、闪存盘对操作系统、驱动进行升级

29	功能要求	动功能	★操作系统功能	a) 支持访问控制、安全审计、网络接入鉴别等功能; b) 操作系统其他功能应满足操作系统政府采购需求标准中加*的指标要求
30	安全要求	关键部件安全要求	★关键部件安全要求	CPU 和操作系统等关键部件应当符合安全可靠测评要求
31	性能要求		单CPU 末级缓存容量	≥16MB
32	性能要求	内存性能	内存速率	≥3200MT/s
33	服务要求	服务响应	服务响应	a)提供电话、电子邮件、 远程连接等多种形式服务; b) 提供5年原厂服务(存储介质不返还); 若硬件故障需提供备件4小时内到达现场硬件保修和人工服务; 免费软件升级; c) 提供设备安装、调试等原厂施工服务, 建立全国技术服务体系和服务团体, 符合专业服务体系标准要求, 提供原厂中文服务; d) 服务周期内提供产品的维修、换件和升级服务, 能在设备故障时提供同等备机备件服务
34	服务要求		★培训服务	供应商提供培训材料、产品手册、培训视频等培训相关内容

序号	指标分类	一级指标	二级指标	指标要求
----	------	------	------	------

1	产 品 类 型	产品类 型	产品属性	产品为2路机架式服务器，高度≤4U ；
2	产 品 规 格	CPU规 格	★CPU信息	实配两颗国产高性能服务器级别CP U，每颗CPU核心数量：≥24核； 线程数：≥24线程；基础频率：≥2 .2GHz；
3	产 品 规 格	主板规 格	★主板支持 的CPU和内 存情况	国产高性能服务器级别CPU内存型 号：16G/32G/64G DDR4 ECC R DIMM
4	产 品 规 格		主板内存槽 数量	非板载内存的可扩展插槽数量应不 少于16个
5	产 品 规 格		主板存储接 口	至少支持 SATA、SAS、M.2、U.2 等存储接口中的1种
6	产 品 规 格		★PCIe插槽 接口	符合 PCIe3.0 或以上的高速串行计 算机扩展总线标准，PCIe的接口速 率与位宽需保证向下兼容
7	产 品 规 格	内存规 格	主板PCIe插 槽数量及规 格	≥5个标准PCIe 4.0插槽,标卡槽位
8	产 品 规 格		内存数量	实配容量不小于8*32GB，所有物 理内存品牌型号一致。
9	产 品 规 格		内存规格	≥DDR4 3200MHz

10	产 品 规 格	存储规 格	硬磁盘实配 容量	配备固态硬盘，实配固态硬盘单盘容量 不小于 480GB SATA SSD ； 配备 固态硬盘 1 ，实配固态硬盘单盘容量不小 于 1.6TB SATA SSD ；配置机械硬 盘 2 ，单盘容量不小于 12TB SATA
11	产 品 规 格		★硬盘实配 数量	a) 配备固态硬盘，实配盘数应不小于 2 b) 配备固态硬盘 1 ，实配盘数应不小 于 2 c) 配备机械硬盘 2 ，实配盘数应不 小于 22
12	产 品 规 格		★硬盘插槽 数量及规格	≥ 24 块 3.5 寸硬盘
13	产 品 规 格	RAID 卡规格	RAID卡支持 的SAS接口 数	≥ 8
14	产 品 规 格	网络规 格	★网口速率 和数量	配备 RJ45 网口数量不少于 4 个，且网 口速率不少于 1GE 配备 SFP+ 网口 数量不少于 4 个，且网口速率不少于 10GE
15	产 品 规 格		★网络接口	配置千兆网口≥ 4 （ 2 块双口千兆网 卡或 1 块 4 口千兆网卡），网卡自带 控制芯片 配置≥ 2 块 10Gb 以太网双 口光口网卡（满配多模光模块）， 网卡自带控制芯片
16	产 品 规 格	外部接 口规格	显示接口	≥ 1 个 VGA 接口
17	产 品 规 格		USB 接口	配备 USB3.0 接口
18	产 品 规 格	电源规	电源冗余模 式	整机电源模块按 1+1 冗余或 N+1 冗余配置

26	功能要求	管理系统功能	★BMC 固件基础功能	1) 支持DHCP 设置网络功能； 2)支持静态IP 设置网络功能； 3)支持设备日志记录，包括但不限于登录日志、操作日志和报警日志等功能； 4)支持日志信息导出和记录删除功能； 5)支持通过管理接口向外输出准确的报警信息功能； 6)设备的BMC 管理软件应能够按报警的严重程度进行区分；
27	功能要求		★BIOS 固件基础功能	a) 支持查看固件版本、内存信息、主板信息、处理器信息和系统时间信息功能； b) 支持上电初始化界面显示CPU 信息、内存信息、固件版本和部分快捷键信息功能； c) 支持设置界面中英文显示切换功能； d) 支持查看PCIe 设备信息，SATA 设备信息功能； e) 支持操作系统安装和引导功能，应并向操作系统提供计算机主板信息和服务接口； f) 支持设置启动顺序，并按照设置的启动顺序启动功能； g) 支持安全启动功能；
28	功能要求	操作系统及驱动功能	★操作系统及驱动的升级	支持通过网络、闪存盘对操作系统、驱动进行升级
29	功能要求	操作系统及驱动功能	★操作系统功能	a) 支持访问控制、安全审计、网络接入鉴别等功能； b) 操作系统其他功能应满足操作系统政府采购需求标准中加*的指标要求
30	安全要求	关键部件安全要求	★关键部件安全要求	CPU 和操作系统等关键部件应当符合安全可靠测评要求

31	性能要求		单CPU 末级 缓存容量	≥16MB
32	性能要求	内存性能	内存速率	≥3200MT/s
33	服务要求	服务响应	服务响应	<p>a)提供电话、电子邮件、 远程连接等多种形式服务；</p> <p>b) 提供5年原厂服务(存储介质不返还)；</p> <p>若硬件故障需提供备件4小时内到达现场硬件保修和人工服务；免费软件升级；</p> <p>c) 提供设备安装、调试等原厂施工服务，建立全国技术服务体系和服务团体，符合专业服务体系标准要求，提供原厂中文服务；</p> <p>d) 服务周期内提供产品的维修、换件和升级服务，能在设备故障时提供同等备机备件服务</p>
34	服务要求		★培训服务	供应商提供培训材料、产品手册、培训视频等培训相关内容

序号	指标分类	一级指标	二级指标	指标要求
1	产品类型	产品类型	产品属性	产品为2路机架式服务器，高度≤4U；

2	产 品 规 格	CPU规 格	★CPU信息	实配两颗国产高性能服务器级别CPU，每颗CPU核心数量：≥24核；线程数：≥24线程；基础频率：≥2.2GHz；
3	产 品 规 格	主板规 格	★主板支持的CPU 和内存情况	国产高性能服务器级别CPU内存型号：16G/32G/64G DDR4 ECC RDIMM
4	产 品 规 格		主板内存槽数量	非板载内存的可扩展插槽数量应不少于16个
5	产 品 规 格		主板存储接口	至少支持 SATA、SAS、M.2、U.2 等存储接口中的1种
6	产 品 规 格		★PCIe插槽接口	符合 PCIe3.0 或以上的高速串行计算机扩展总线标准，PCIe的接口速率与位宽需保证向下兼容
7	产 品 规 格		主板PCIe插槽数量及规格	≥5个标准PCIe 4.0插槽,标卡槽位
8	产 品 规 格	内存规 格	内存数量	实配容量不小于8*32GB，所有物理内存品牌型号一致。
9	产 品 规 格		内存规格	≥DDR4 3200MHz
10	产 品 规 格	存储规 格	硬磁盘实配容量	配备固态硬盘，实配固态硬盘单盘容量不小于480GB SATA SSD；配置机械硬盘1，单盘容量不小于12TB SATA
11	产 品 规 格		★硬盘实配数量	a) 配备固态硬盘，实配盘数应不小于2 b) 配备机械硬盘1，实配盘数应不小于22

12	产 品 规 格		★硬盘插槽 数量及规格	≥24块3.5寸硬盘
13	产 品 规 格	RAID 卡规格	RAID卡支持 的SAS接口 数	≥8
14	产 品 规 格	网络规 格	★网口速率 和数量	配备RJ45网口数量不少于4个，且网 口速率不少于1GE 配备SFP+网口 数量不少于4个，且网口速率不少于 10GE
15	产 品 规 格		★网络接口	配置千兆网口≥4（2块双口千兆网 卡或1块4口千兆网卡），网卡自带 控制芯片 配置≥2块10Gb以太网双 口光口网卡（满配多模光模块）， 网卡自带控制芯片
16	产 品 规 格	外部接 口规格	显示接口	≥1个VGA接口
17	产 品 规 格		USB 接口	配备USB3.0接口
18	产 品 规 格	电源规 格	电源冗余模 式	整机电源模块按 1+1 冗余或 N+1 冗余配置
19	产 品 规 格		电源功率	电源模块功率应有一定冗余，满足 服务器满载时的需求
20	功 能 要 求	网络功 能	网络功能	支持网络连接、网络访问、数据交 换和网络管控功能

4

信创云备份
存储服务器

1

台

21	功能要求	CPU功能	计算处理	支持通用计算及虚拟化功能。处理器需集成整型计算单元、浮点计算单元、内存控制器、I/O 模块等，处理器与存储部件、网络部件、I/O部件等组成计算系统，提供数据处理、网络接入等计算相关功能
22	功能要求		密码算法实现	CPU 芯片应符合GM/T 0008 的相关规定，或芯片密码模块应符合GB/T37092 或GM/T 0028 的相关规定
23	功能要求	RAID卡功能	RAID卡 RAID级别支持	RAID模式支持 RAID 0/1/10/5，存储型支持 RAID 0/1/5/6/10/50/60，实配同时支持直通和RAID模式
24	功能要求		RAID 卡 BB U 单元	RAID 卡支持电池或电容备份单元
25	功能要求	电源功能	电源热插拔	整机电源模块应具备热插拔功能
26	功能要求	管理系统功能	★BMC 固件基础功能	1) 支持DHCP 设置网络功能； 2)支持静态IP 设置网络功能； 3)支持设备日志记录，包括但不限于登录日志、操作日志和报警日志等功能； 4)支持日志信息导出和记录删除功能； 5)支持通过管理接口向外输出准确的报警信息功能； 6)设备的BMC 管理软件应能够按报警的严重程度进行区分；

27	功能要求		★BIOS 固件基础功能	<p>a) 支持查看固件版本、内存信息、主板信息、处理器信息和系统时间信息功能；</p> <p>b) 支持上电初始化界面显示CPU信息、内存信息、固件版本和部分快捷键信息功能；</p> <p>c) 支持设置界面中英文显示切换功能；</p> <p>d) 支持查看PCIe 设备信息，SATA设备信息功能；</p> <p>e) 支持操作系统安装和引导功能，应并向操作系统提供计算机主板信息和服务接口；</p> <p>f) 支持设置启动顺序，并按照设置的启动顺序启动功能；</p> <p>g) 支持安全启动功能；</p>
28	功能要求	操作系统及驱动功能	★操作系统及驱动的升级	支持通过网络、闪存盘对操作系统、驱动进行升级
29	功能要求		★操作系统功能	<p>a) 支持访问控制、安全审计、网络接入鉴别等功能；</p> <p>b) 操作系统其他功能应满足操作系统政府采购需求标准中加*的指标要求</p>
30	安全要求	关键部件安全要求	★关键部件安全要求	CPU 和操作系统等关键部件应当符合安全可靠测评要求
31	性能要求		单CPU 末级缓存容量	≥16MB
32	性能要求	内存性能	内存速率	≥3200MT/s

						a)提供电话、电子邮件、远程连接等多种形式服务; b) 提供5年原厂服务(存储介质不返还); 若硬件故障需提供备件4小时内到达现场硬件保修和人工服务;免费软件升级;		
		33	服 务	应 响	服务响应	c) 提供设备安装、调试等原厂施工服务，建立全国技术服务体系和服务网络要求符合专业服务体系标准要求，提供原厂中文服务; d) 服务周期内提供产品的维修、换件和升级服务，能在设备故障时提产品为2路机架式服务器，高度≤2U供同等备机备件服务 供应商提供培训材料、产品手册、实配两颗国产高性能服务器级别CPU培训视频等培训内容		
		序 号	要 指 求 标 分 类	一 级 指 标	二 级 指 标	d) 服务周期内提供产品的维修、换件和升级服务，能在设备故障时提产品为2路机架式服务器，高度≤2U供同等备机备件服务 供应商提供培训材料、产品手册、实配两颗国产高性能服务器级别CPU培训视频等培训内容		
		1	产 品 类 型	产 品 属 性				
		34 2	产 品 规 格	CPU规格	★培训服务 ★CPU信息	实配两颗国产高性能服务器级别CPU培训视频等培训内容		
		3	产 品 规格	主板规格	★主板支持的CPU和内 存情况	国产高性能服务器级别CPU内存型号：16G/32G/64G DDR4 ECC R DIMM		
		4	产 品 规格		主板内存槽数量	非板载内存的可扩展插槽数量应不少于16个		
		5	产 品 规格		主板存储接口	至少支持 SATA、SAS、M.2、U.2等存储接口中的1种		
		6	产 品 规格		★PCIe插槽接口	符合 PCIe3.0 或以上的高速串行计算机扩展总线标准，PCIe的接口速率与位宽需保证向下兼容		
		7	产 品 规格		主板PCIe插槽数量及规格	≥5个标准PCIe 4.0插槽,标卡槽位		

8	产 品 规 格	内存规 格	★内存数量	实配容量不小于8*32GB，所有物理内存品牌型号一致。
9	产 品 规 格		★内存规格	≥DDR4 3200MHz
10	产 品 规 格	存储规 格	硬磁盘实配容量	配备SAS盘，实配SAS盘单盘容量不小于600GB； 配备SAS盘1，实配SAS盘单盘容量不小于1.8TB；
11	产 品 规 格		★硬盘实配数量	a) 配备SAS盘，实配盘数应不小于2 b) 配备SAS盘1，实配盘数应不小于24
12	产 品 规 格		★硬盘插槽数量及规格	≥29个2.5寸热插拔硬盘槽位
13	产 品 规 格	RAID 卡规格	RAID卡支持的SAS接口数	≥8
14	产 品 规 格	网络规 格	★网口速率和数量	配备RJ45网口数量不少于4个，且网口速率不少于1GE 配备SFP+网口数量不少于4个，且网口速率不少于10GE
15	产 品 规 格		★网络接口	配置千兆网口≥4（2块双口千兆网卡或1块4口千兆网卡），网卡自带控制芯片 配置≥2块10Gb以太网双口光口网卡（满配多模光模块），网卡自带控制芯片
16	产 品 规 格	外部接 口规格	显示接口	≥1个VGA接口

26	功能要求	管理系统功能	★BMC 固件基础功能	1) 支持DHCP 设置网络功能； 2)支持静态IP 设置网络功能； 3)支持设备日志记录，包括但不限于登录日志、操作日志和报警日志等功能； 4)支持日志信息导出和记录删除功能； 5)支持通过管理接口向外输出准确的报警信息功能； 6)设备的BMC 管理软件应能够按报警的严重程度进行区分；
27	功能要求		★BIOS 固件基础功能	a) 支持查看固件版本、内存信息、主板信息、处理器信息和系统时间信息功能； b) 支持上电初始化界面显示CPU 信息、内存信息、固件版本和部分快捷键信息功能； c) 支持设置界面中英文显示切换功能； d) 支持查看PCIe 设备信息，SATA 设备信息功能； e) 支持操作系统安装和引导功能，应并向操作系统提供计算机主板信息和服务接口； f) 支持设置启动顺序，并按照设置的启动顺序启动功能； g) 支持安全启动功能；
28	功能要求	操作系统及驱动功能	★操作系统及驱动的升级	支持通过网络、闪存盘对操作系统、驱动进行升级
29	功能要求		★操作系统功能	a) 支持访问控制、安全审计、网络接入鉴别等功能； b) 操作系统其他功能应满足操作系统政府采购需求标准中加*的指标要求
30	安全要求	关键部件安全要求	★关键部件安全要求	CPU 和操作系统等关键部件应当符合安全可靠测评要求

31	性能要求		单CPU 末级 缓存容量	≥16MB
32	性能要求	内存性能	内存速率	≥3200MT/s
33	服务要求	服务响应	服务响应	<p>a)提供电话、电子邮件、 远程连接等多种形式服务；</p> <p>b) 提供5年原厂服务(存储介质不返还)；</p> <p>若硬件故障需提供备件4小时内到达现场硬件保修和人工服务；免费软件升级；</p> <p>c) 提供设备安装、调试等原厂施工服务，建立全国技术服务体系和服务团体，符合专业服务体系标准要求，提供原厂中文服务；</p> <p>d) 服务周期内提供产品的维修、换件和升级服务，能在设备故障时提供同等备机备件服务</p>
34	服务要求		★培训服务	<p>供应商提供培训材料、产品手册、培训视频等培训相关内容</p>

6	存储扩容	<p>采购的设备应满足整体云解决方案纳管，所扩容的磁盘柜及硬盘能够被现有存储控制器进行统一管理和存储资源池化；</p> <p>1.配置≥3个2U25盘位机架式磁盘扩展单元，单个磁盘柜支持25个2.5寸磁盘驱动器，支持SSD、SAS 等不同类型硬盘在同一个磁盘柜混插、热拔插和在线更换故障硬盘；</p> <p>2.配置≥75块2.4TB 10K转SAS硬盘；</p> <p>3.配置≥4个4U24盘位机架式磁盘扩展单元，单个磁盘柜支持24个3.5寸磁盘驱动器，支持SSD、SAS、NL-SAS、SATA 等不同类型硬盘在同一个磁盘柜混插、热拔插和在线更换故障硬盘；</p> <p>4.配置≥96块8TB7.2K转NL-SAS硬盘；</p> <p>5.单RAID5硬盘组的两块及以上硬盘同时发生介质错误，业务不中断、数据不丢失；</p> <p>6.单RAID硬盘组任意3块及以上硬盘发生整盘永久性故障，数据不丢失，业务不中断；</p> <p>7.单LUN任意1块硬盘发生整盘永久性故障，业务不中断，单LUN无IO跌零；</p> <p>8.支持RAID快速重建功能，在RAID5中，单块硬盘发生闪断，重建时间不超过10分钟；在RAID5中，单块硬盘大面积介质故障，热备盘重建时间不超过20分钟。支持0、1、3、5、6、10、50、60等多种RAID方式；</p> <p>9.配置智能管理系统，用于设备的自动运维，可根据预设定时任务，自动巡检指定设备的控制器状态、CPU使用率、硬盘状态、电源状态、RAID/LUN状态等信息；智能检查最小周期≤1小时；检查结果可以通过邮件等方式发送给指定接收人；</p> <p>10.配置系统监控、性能监控分析、日志及邮件告警功能；配置自动精简、服务质量控制（QoS）；</p> <p>11.提供扩容所需配套SAS线缆、电源线、滑轨等附件；</p> <p>▲12.提供五年原厂质保服务，提供原厂存储空间扩容实施服务及扩容相关的配套服务，质保期内，存储介质不返还。</p>	1	套
---	------	--	---	---

7	国产化下一代防火墙	<p>1.采用国产芯片设备</p> <p>2.吞吐量≥30Gbps，并发连接数≥2000万，新建连接数≥500000cps。</p> <p>▲3.配置≥8个千兆电口，≥4个千兆光口（满配万兆多模光模块），≥10个10G光口（配置2个10GE多模光模块），配置≥960G SSD硬盘。（提供证明材料，加盖厂商公章）</p> <p>4.支持静态路由、策略路由、RIP、OSPF、BGP等路由协议</p> <p>5.支持路由模式、透明模式、混合模式部署。</p> <p>6.支持安全区域划分，访问控制列表，配置对象及策略，动态包过滤，黑名单，MAC 和 IP 绑定功能，基于MAC的访问控制列表，802.1q VLAN 透传等功能。</p> <p>7.支持基于域名的安全策略模糊匹配。（提供证明材料，加盖厂商公章）</p> <p>8.支持基于源安全域、目的安全域、源IP/MAC地址、目的IP地址、用户、应用、终端、服务、VRF和时间段进行策略冗余分析，冲突策略分析以及命中率统计。</p> <p>9.支持IPv6路由协议、IPv6对象及策略、IPv6状态防火墙、IPv6攻击防范、IPv6 GRE/IPsec VPN、IPv6日志审计、IPv6会话热备等功能。</p> <p>10.支持对检测到的攻击行为的前后报文进行自动化抓包功能，方便用户对攻击行为进行取证。（提供证明材料，加盖厂商公章）</p> <p>11.支持2台设备堆叠成一台设备使用，实现统一管理，统一配置，所投设备支持高可靠性部署。（提供证明材料，加盖厂商公章）</p> <p>12.僵尸网络分析，攻击链推导及资产安全风险等级的可视化呈现；基于应用的数据分析</p> <p>13.服务：≥5年质保，配置≥5年IPS,AV,WAF特征库升级。</p>	2	台
8	云平台安全一体机	<p>1.软硬一体式设备，国产处理器，提供≥4个千兆电口，≥2个千兆光口，≥1个管理口，内存≥96G，存储≥4T，支持RAID1，双模块化电源</p> <p>2. 设备具备综合日志审计功能（≥50个日志源）、运维审计（≥50个资产数量、≥2个双因素认证动态口令卡）功能；</p> <p>3. 日志审计模块支持按照日志类型进行查询，支持操作日志、审计日志、流量日志、威胁日志、主机日志等11大类进行分类；支持多条件查询，包含开始时间、结束时间、动作类型、设备名称、日志等级、用户名、源IP、目的IP、协议等条件进行过滤查询展示；支持全文检索原始日志，检索字段变色高亮；支持任意信息、任意时间进行内容查询匹配，支持可选包含/不包含匹配方式</p> <p>4.运维审计功能最大图形并发连接数不少于150，最大字符并发连接数不少于300；支持域账号的自动化同步，可将未纳管的域账号自动添加到系统中并自动赋予指定角色，无需管理员干预；支持 动态权限管控，管理员可基于用户属性、设备属性、系统账号属性来创建弹性动态权限规则，只要满足相关属性的用户、设备、账号即会被自动赋予对应访问权限。</p>	1	台

9	48口万兆交换机	<p>1.交换容量$\geq 4.8\text{Tbps}$，包转发率$\geq 2000\text{Mpps}$。（以最低参数为准，提供证明材料，加盖厂商公章）</p> <p>▲2.配置≥ 48个SFP+口，≥ 6个QSFP28口（部分支持拆分10G/25G），$\geq 48 * \text{SFP+}$ 万兆多模光模块;$\geq 4 * \text{QSFP+}$ 40G 2KM单模光模块，≥ 2根堆叠线缆。</p> <p>3.支持并配置≥ 2个交流电源。</p> <p>4.支持快速环网保护协议，链路切换时间小于50ms。</p> <p>5.支持IPv6静态路由、RIPng、OSPFv3及加密、ISISv6及加密、BGP4+及加密。</p> <p>6.支持硬件BFD, 最小检测间隔3ms。</p> <p>7.支持对光模块进行健康度检查。</p> <p>8.设备采用国产芯片，≥ 5年质保。</p>	8	台
10	万兆交换机	<p>1.交换容量$\geq 4.8\text{Tbps}$，包转发率$\geq 2000 \text{ Mpps}$。（以最低参数为准，提供证明材料，加盖厂商公章）</p> <p>2.配置≥ 48个SFP+口，≥ 4个QSFP28口，≥ 2个QSFP+口，$\geq 24 * \text{SFP+}$ 万兆多模光模块;$\geq 2 * \text{QSFP+}$ 40G 多模光模块。</p> <p>3.配置≥ 2个交流电源。</p> <p>4. MAC表项 $\geq 256\text{K}$，ARP表项$\geq 64\text{K}$。（提供证明材料，加盖厂商公章）</p> <p>5.支持堆叠多虚一技术，实现单一界面管理多台设备。</p> <p>6.内置图形化网管</p> <p>7.设备采用国产芯片，≥ 5年质保。</p>	6	台
11	48口千兆交换机	<p>1.交换容量$\geq 670\text{Gbps}$，以官网所列最低参数为准，包转发率$\geq 200\text{Mpps}$。（以最低参数为准，提供证明材料，加盖厂商公章）</p> <p>2.配置≥ 48个10/100/1000Base-T自适应以太网接口，≥ 4个万兆SFP+接口，$\geq 4 * \text{SFP+}$ 万兆多模光模块。</p> <p>3.内置冗余多风扇，内置冗余双电源。</p> <p>4.支持堆叠多虚一技术，实现单一界面管理多台设备。</p> <p>5.支持SNMP V1/V2/V3、Telnet、RMON、SSH功能。</p> <p>6.支持动态ARP检测，防止中间人攻击和ARP拒绝服务</p> <p>7.设备采用国产芯片，≥ 5年质保。</p>	6	台

			<div>硬件指标：标准机架式设备，网络接口≥4个千兆电口，内置PCI-E密码卡≥1张。</div> <div>性能指标：吞吐量≥720Mbps，网络延时<25ms，单台设备支持≥2000应用代理设备接入，最大并发连接数≥1600，每秒可建立VPN连接数≥1000个。</div> <div>产品功能：<div>1.使用数字证书认证方式确保接入用户的合法性。</div><div>2.系统基于SSL协议，通过PCI-E密码卡的密码能力构建安全传输通道，为应用数据安全传输提供密码服务，支持国密算法SM1/2/3/4。</div><div>3.提供用户接入控制、资源访问控制，保证内网数据的安全。</div><div>4.提供防火墙功能，通过在管理平台配置对进入数据进行过滤，从而控制外部用户对内网的访问。</div><div>▲5.实现与陕西省公安厅新一代移动警务平台集中安全管理系统无缝对接，能够实时上报服务运行状态、服务报警信息，定时上报数据流量信息。</div></div>	2	台																															
		<table><tr><td>序号</td><td>指标分类</td><td>一级指标</td><td>二级指标</td><td>指标要求</td></tr><tr><td>1</td><td>产品类型</td><td>产品类型</td><td>产品属性</td><td>产品为2路机架式服务器，高度≤4U；</td></tr><tr><td>2</td><td>产品规格</td><td>CPU规格</td><td>★CPU信息</td><td>实配两颗国产高性能服务器级别CPU，每颗CPU核心数量：≥24核；线程数：≥24线程；基础频率：≥2.2GHz；</td></tr><tr><td>3</td><td rowspan="2">产品规格</td><td rowspan="5">主板规格</td><td>★主板支持的CPU和内存情况</td><td>国产高性能服务器级别CPU</td></tr><tr><td>4</td><td>内存型号：16G/32G/64G DDR4 ECC RDIMM</td></tr><tr><td>5</td><td>主板内存槽数量</td><td>非板载内存的可扩展插槽数量应不少于16个</td></tr><tr><td>6</td><td>主板存储接口</td><td>至少支持 SATA、SAS、M.2、U.2等存储接口中的1种</td></tr><tr><td></td><td></td><td></td><td></td></tr></table>	序号	指标分类	一级指标	二级指标	指标要求	1	产品类型	产品类型	产品属性	产品为2路机架式服务器，高度≤4U；	2	产品规格	CPU规格	★CPU信息	实配两颗国产高性能服务器级别CPU，每颗CPU核心数量：≥24核；线程数：≥24线程；基础频率：≥2.2GHz；	3	产品规格	主板规格	★主板支持的CPU和内存情况	国产高性能服务器级别CPU	4	内存型号：16G/32G/64G DDR4 ECC RDIMM	5	主板内存槽数量	非板载内存的可扩展插槽数量应不少于16个	6	主板存储接口	至少支持 SATA、SAS、M.2、U.2等存储接口中的1种						
序号	指标分类	一级指标	二级指标	指标要求																																
1	产品类型	产品类型	产品属性	产品为2路机架式服务器，高度≤4U；																																
2	产品规格	CPU规格	★CPU信息	实配两颗国产高性能服务器级别CPU，每颗CPU核心数量：≥24核；线程数：≥24线程；基础频率：≥2.2GHz；																																
3	产品规格	主板规格	★主板支持的CPU和内存情况	国产高性能服务器级别CPU																																
4			内存型号：16G/32G/64G DDR4 ECC RDIMM																																	
5	主板内存槽数量		非板载内存的可扩展插槽数量应不少于16个																																	
6	主板存储接口		至少支持 SATA、SAS、M.2、U.2等存储接口中的1种																																	

7	产品规格		★PCIe插槽接口	符合 PCIe3.0 或以上的高速串行计算机扩展总线标准，PCIe的接口速率与位宽需保证向下兼容
8	产品规格		主板PCIe插槽数量及规格	≥5个标准PCIe 4.0插槽,标卡槽位
9	产品规格	内存规格	★内存数量	实配容量不小于16*32GB，所有物理内存品牌型号一致；
10	产品规格		★内存规格	≥DDR4 3200MHz
11	产品规格	存储规格	硬磁盘实配容量	配备SAS盘，实配SAS盘单盘容量不小于600GB； 配备SAS盘1，实配SAS盘单盘容量不小于1.8TB；
12	产品规格		★硬盘实配数量	a) 配备SAS盘，实配盘数应不小于2
13	产品规格			b) 配备SAS盘1，实配盘数应不小于24
14	产品规格		★硬盘插槽数量及规格	≥29个2.5寸热插拔硬盘槽位
15	产品规格	GPU规格	GPU规格	≥4张国产GPU卡，单卡显存≥48G，单卡推理算力≥50TFLOPS@FP16；
16	产品规格	RAID卡规格	RAID卡支持的SAS接口数	≥8
17	产品规格	网络规格	★网口速率和数量	配备RJ45网口数量不少于4个，且网口速率不少于1GE 配备SFP+网口数量不少于4个，且网口速率不少于10GE

27	功能要求		RAID 卡 BB U 单元	RAID 卡支持电池或电容备份单元
28	功能要求	电源功能	电源热插拔	整机电源模块应具备热插拔功能
29	功能要求	管理系统功能	★BMC 固件基础功能	1) 支持DHCP 设置网络功能； 2)支持静态IP 设置网络功能； 3)支持设备日志记录，包括但不限于登录日志、操作日志和报警日志等功能； 4)支持日志信息导出和记录删除功能； 5)支持通过管理接口向外输出准确的报警信息功能； 6)设备的BMC 管理软件应能够按报警的严重程度进行区分；
30	功能要求		★BIOS 固件基础功能	a) 支持查看固件版本、内存信息、主板信息、处理器信息和系统时间信息功能； b) 支持上电初始化界面显示CPU 信息、内存信息、固件版本和部分快捷键信息功能； c) 支持设置界面中英文显示切换功能； d) 支持查看PCIe 设备信息，SATA 设备信息功能； e) 支持操作系统安装和引导功能，应并向操作系统提供计算机主板信息和服务接口； f) 支持设置启动顺序，并按照设置的启动顺序启动功能； g) 支持安全启动功能；
31	功能要求		★操作系统及驱动的升级	支持通过网络、闪存盘对操作系统、驱动进行升级
		操作系统及驱		

32	功能要求	动功能	★操作系统功能	a) 支持访问控制、安全审计、网络接入鉴别等功能; b) 操作系统其他功能应满足操作系统政府采购需求标准中加*的指标要求
33	安全要求	关键部件安全要求	★关键部件安全要求	CPU 和操作系统等关键部件应当符合安全可靠测评要求
34	性能要求		单CPU 末级缓存容量	≥16MB
35	性能要求	内存性能	内存速率	≥3200MT/s
36	服务要求	服务响应	服务响应	a)提供电话、电子邮件、 远程连接等多种形式服务; b) 提供5年原厂服务(存储介质不返还); 若硬件故障需提供备件4小时内到达现场硬件保修和人工服务; 免费软件升级; c) 提供设备安装、调试等原厂施工服务, 建立全国技术服务体系和服务团体, 符合专业服务体系标准要求, 提供原厂中文服务; d) 服务周期内提供产品的维修、换件和升级服务, 能在设备故障时提供同等备机备件服务
37	服务要求		★培训服务	供应商提供培训材料、产品手册、培训视频等培训相关内容

--	--	--	--	--

4.2软件产品购置

序号	软件名称	技术参数	数量	单位
1	信创云计算软件	<p>本次项目各组件的软件授权如下：</p> <p>≥50个物理CPU接入授权；≥1个文件存储服务授权；≥1个块存储服务授权；</p> <p>≥1个对象存储服务授权；≥4个GPU服务授权；≥1个备份服务授权；</p> <p>云平台安全组件包含：</p> <p>≥1个日志审计组件(≥64个日志源)；≥1个漏洞扫描系统组件(≥128个可扫描IP地址数)；≥2个运维审计系统组件(≥50个可管理资产)；≥2个WEB应用防火墙组件(≥400M)；≥2个VFW防火墙组件；</p> <p>1.投标产品国产自研产品，以保证功能的可靠性和安全性，要求云计算产品的计算虚拟化软件、存储虚拟化软件、网络虚拟化软件同一品牌，提供国家版权局颁发的《计算机软件著作权登记证书》证明。</p> <p>▲2.为保障平台的解耦和可扩展，云管理平台管理节点和OpenStack控制组件须支持集群部署，并能够支持部署在物理机或虚拟机上，并在部署前自动检测主机性能以识别主机性能是否存在风险。提供平滑升级扩展、高可靠容错机制，各云服务组件之间松耦合，支持不同的服务组件如IaaS、PaaS大数据、数据库、安全等独立部署，支持不同的服务组件单独启用或停用，单云服务组件升级对其他云服务和云管理平台无影响。（提供证明材料，加盖厂商公章）</p> <p>3.云管理平台提供用户自助服务界面，用户能够通过自助服务门户完成云资源申请、使用、修改、销毁等操作。服务门户能够为用户纳管云主机、云硬盘、VPC、云防火墙、云负载均衡、云容器引擎、应用管理、云数据库、中间件、大数据、微服务引擎。</p> <p>▲4.云管理平台支持配置告警规则，支持告警级别等信息，告警级别支持紧急、严重、一般，可根据现场情况，选择不同级别的告警信息通知，支持邮件、短信的通知方式。为保证规则生效，对接短信平台后，可发送测试短信，确认短信功能与云管理平台已成功联动。（提供响应承诺，加盖厂商公章）</p> <p>5.云管理平台支持多组织划分，为不同的组织分配资源配额，配额包括CPU、内存、云主机、路由器、VPN、网卡、防火墙、负载均衡、安全组、公网IP、WAF、日志审计、数据库审计、态势感知、DDOS防护个数等，组织管理员可以根据组织内部架构，划分子组织。（提供证明材料，加盖厂商公章）</p> <p>6.云管理平台支持大屏展示功能，展示云管平台IaaS层计算、网络、存储、组织用户等资源统计信息和资源分配情况、告警信息及PaaS层应用状态统计信息等内容，支持自定义大屏。</p> <p>7.云管理平台支持设定用户账号的安全策略。管理员可进行账号锁定/解锁，设定账号密码策略，如密码长度、密码复杂度、密码有效期、连续登录失败锁定，同一账号的接入点限制与ACL等策略。</p>	1	套

	<p>8.可以通过自助服务门户批量申请云主机。申请云主机时可以定义所需操作系统类型、镜像、CPU规格、内存规格、硬盘规格，可自定义IP及安全组，可以为云主机选择自定义密码、随机密码、密钥对或镜像默认密码登录。</p> <p>9.云管理平台可支持云硬盘服务，支持新建、销毁、修改所有者、在线扩展硬盘容量、快照、备份、克隆等操作，支持云硬盘自动快照策略。</p> <p>▲10.云管理平台支持对象存储服务，新建、编辑、扩容、删除对象存储桶；支持在已创建的存储桶中创建、删除文件夹；支持已创建的存储桶中文件的上传、下载、复制、编辑和删除。支持对上传的文件进行加密。（提供证明材料，加盖厂商公章）</p> <p>11.云管理平台可以提供云主机的安全防护能力，可以对登录用户所属组织下的云虚拟主机提供深度防护服务。</p> <p>12.云管理平台支持对资源扩展和收缩策略的灵活配置，能够根据虚拟机CPU、内存、连接数等参数动态的增加虚拟机或删除虚拟机以满足“业务量大时使用多个虚拟机提供服务、业务量少时使用少量虚拟机提供服务”的业务需求。</p> <p>13.支持云主机回收站，为了防止误删云主机，用户通过该功能可以将云主机移入回收站，而非直接销毁。在云主机回收保存期内用户可以从回收站中还原云主机，超过保存期后云主机将被自动销毁。</p> <p>▲14.漏洞扫描组件支持一键下发系统扫描、Web扫描、弱口令扫描任务，弱口令扫描能自动发现开放服务并自动开展弱口令扫描。（提供响应承诺，加盖厂商公章）</p> <p>15.WEB应用防火墙组件支持SQL注入、XSS跨站攻击的语义分析检测，同时支持语义分析算法和特征检测算法的切换</p> <p>16.运维审计系统组件支持从云管理平台自动同步所在租户VPC网络内的主机资产信息（名称、IP、类型、）和用户账号信息（用户名、信息、邮箱），通过勾选实现自动导入，从而提高配置效率。（提供响应承诺，加盖厂商公章）</p> <p>17.提供5年的软件质保，在质保期内提供免费升级服务。</p>	
--	--	--

2	信创云虚拟化软件	<p>≥50颗物理CPU授权</p> <p>1.虚拟化产品支持 安装在通用的国产架构服务器，支持国产主流CPU服务器，支持服务器集群统一管理。</p> <p>2.虚拟化平台提供统一的虚拟化管理界面，支持管理所有虚拟化计算节点，在同一界面上提供虚拟机启动、休眠、恢复、重启、安全关闭、关闭电源、迁移、备份、快照、克隆、克隆为模板、修改等生命周期管理功能。</p> <p>3.支持宿主机自治功能，在虚拟化管理平台故障时，可以通过主机自治平台对所在宿主机和虚拟机进行管理运维，提供虚拟机启动、配置、关闭、重启、休眠、删除等生命周期管理，提供虚拟机及主机性能监控、告警管理等，保障业务稳定运行。</p> <p>▲4.虚拟化平台应提供虚拟交换机的集中化展示虚拟交换机端口使用情况，通过点击虚拟交换机端口，可以快速查看端口详细信息和端口流量实时监控，提供可视化的监控界面降低运维难度，快速掌握网络流量情况。（提供响应承诺，加盖厂商公章）</p> <p>5.虚拟机之间可以做到隔离保护，其中每一个虚拟机发生故障都不会影响同一个物理机上的其它虚拟机运行，每个虚拟机上的用户权限只限于本虚拟机之内，以保障系统平台的安全性。</p> <p>6.支持虚拟机规格的在线和离线调整，包括CPU、内存、硬盘、网卡等资源，在虚拟机操作系统本身支持的前提下，热添加的CPU/内存可以即时生效。</p> <p>7.支持虚拟机一致性快照，快照时将缓存数据落盘，保证虚拟机磁盘数据的一致性，在软件安装测试、升级等故障恢复场景，快速恢复到快照前的环境，同时支持开放快照接口与第三方备份对接，保证虚拟机备份的数据完整性。</p> <p>8.虚拟机支持在线克隆为模板，模板制作过程中对业务运行无影响，同时虚拟机模板支持完整性验证与来源追溯，避免虚拟机模板文件被篡改的可能性，并追踪虚拟机模板的来源以及虚拟机模板部署的记录。</p> <p>9.支持批量修改虚拟机的配置参数，包括：CPU调度优先级、CPU个数、内存大小、I/O优先级、启动优先级、是否自动迁移、tools自动升级等。</p> <p>10.虚拟机支持市场上主流的国内操作系统，包括统信、银河麒麟等。</p> <p>11.支持主流国产操作系统虚拟机无代理底层防病毒能力，包括统信、银河麒麟等，不需要在虚拟机部署安全防护代理，对虚拟机数量无限制。</p> <p>▲12.支持在同一管理平台对虚拟化宿主机和虚拟机统一安全防护，支持宿主机和虚拟机同时开启病毒防护，无需改变网络架构，及时识别并有效阻断对宿主机和虚拟机发起的入侵攻击和病毒破坏行为。（提供证明材料，加盖厂商公章）</p> <p>13.提供5年的软件质保，在质保期内提供免费升级服务。</p>	1	套
---	----------	--	---	---

		<p>1.本次配置≥1.6PB的软件裸容量授权，包含所有功能特性，不额外收费。</p> <p>▲2.单节点池可同时部署文件、对象或块存储类型服务。（提供证明材料，加盖厂商公章）</p> <p>3. Scale-out横向扩展的分布式架构，节点间完全对称，无独立的元数据物理服务器或索引服务器；元数据、数据均采用集群方式部署，满足任何一个节点出现故障，不影响数据的正常访问功能。</p> <p>4.支持存储加密，数据通过标准的商密和国密算法以密文落盘进行存储，裸盘直接读取的文件为密文。（提供证明材料，加盖厂商公章）</p> <p>5.支持多副本保护机制，可选择2~8副本，允许在线调整设置副本数量，支持纠删码特性，支持N+1到N+4的纠删码保护，最大支持任意4个节点故障而数据不丢失、系统不停机。</p> <p>6.支持块、文件、对象存储的pool级重删。开启重删后，对存储池内写入数据进行比较，重复数据仅保留一份，删除其他的重复数据，节省存储空间。</p> <p>▲7.支持精简配置，可以根据应用实际写需要时才弹性分配相应的物理存储空间。（提供证明材料，加盖厂商公章）</p> <p>8.块存储支持iscsi虚IP高可用，具有动态绑定、故障时可“漂移”的特性，进行负载均衡和故障时自动切换ip，业务端无感知。</p> <p>▲9.支持分布式集群拉远双活功能，以实现两站点（即数据中心）两个存储数据双活，主机能够并发读写同一双活卷，任何一边站点设备宕机均不影响上层业务系统运行。（提供证明材料，加盖厂商公章）</p> <p>10.支持NFS/S3协议转换，如对于新建对象存储，可以支撑老旧业务使用NFS访问。</p> <p>11.提供多租户管理能力，不同租户之间的数据逻辑隔离，便于资源划分；支持对租户的配额设置。</p> <p>12.支持对主机的各个维度信息进行监控展示，包括IOPS/OPS、带宽、硬盘容量、CPU/内存使用率、硬盘时延、硬盘负载、网卡、系统平均负载等信息，支持自定义时间一键导出监控报表。</p> <p>13.提供5年的软件质保，在质保期内提供免费升级服务。</p>		
3	信创云分布式存储软件		1	套

4	信创云备份软件	<p>1.本次提供备份、数据库复制、统一容量授权220TB，对数据库复制和实时备份无需再单独购买额外授权。</p> <p>2.备份系统的管理平台支持B/S架构，通过浏览器访问备份平台对定时备份、数据库复制等相关功能进行统一管理。</p> <p>3.备份系统可部署在通用的国产架构服务器上，支持海光、鲲鹏、飞腾、龙芯、兆芯等国产化服务器。</p> <p>4.支持将块存储、文件存储、对象存储、光盘等作为备份数据的存储介质。</p> <p>5.支持源端/目的端重删，并行重删技术，提升备份数据的去重率，满足海量数据的去重需求。</p> <p>6.支持对备份数据进行加密传输和存储，支持主流国产商用密码算法，提升传输过程以及存储的安全性。</p> <p>▲7.备份任务异常停止后，备份系统可自动将备份任务重启，重启参数支持次数和时间设置，确保备份任务的高可靠性，从而保障备份业务的自动连续性。（提供证明材料，加盖厂商公章）</p> <p>8.支持对虚拟化平台虚拟机文件细粒度的恢复，在恢复时可指定虚拟机中的某个文件夹或文件。（提供证明材料，加盖厂商公章）</p> <p>9.提供数据库事务级的实时复制功能，通过同步日志技术实现生产端和备份端的事务级数据一致性，可通过一键切换进行数据库接管。</p> <p>10.支持银河麒麟、统信UOS等国产操作系统。</p> <p>11.支持达梦、人大金仓、南大通用、华为高斯、优炫、瀚高等国产数据库。</p> <p>12.支持对主流虚拟化平台的无代理备份，可以以资源池、集群、主机为单位进行虚拟机的备份保护，无需在虚拟机内部安装任何代理软件。</p> <p>13.提供5年的软件质保，在质保期内提供免费升级服务。</p>	1	套
---	---------	--	---	---

			5	国产化大数据服务组件	<p>≥13个节点授权</p> <p>1.支持海光、鲲鹏、飞腾等主流国产化服务器，提供响应承诺，加盖厂商公章</p> <p>2. 管理节点在内的组件节点及所有业务组件中心管理节点实现HA包括但不限于HDFS NameNode HA、YARN Resource Manager HA、Hive HA、HBase Master HA、ElasticSearch HA。</p> <p>▲3.管理平台支持基于角色的权限控制，运维管理员、安全管理员和审计管理员三员分立，不同用户具有部分管理权限。（提供证明材料，加盖厂商公章）</p> <p>4.提供分布式文件系统HDFS、HBase数据库、Redis内存数据库和Hive离线数据仓库。</p> <p>5.提供MapReduce、Spark、Storm、Flink等多种计算框架，离线计算、内存计算和流式计算并存，满足高吞吐、大数据量和低时延实时处理等多方面的数据计算要求。</p> <p>6.可以根据不同的业务部门，以及各自部门的业务需求，向多个部门提供资源隔离的多租户服务。</p> <p>7.为保障的多租户的资源隔离，要求大数据平台提供共享资源模式，支持HDFS、Hive、HBase、Kafka、Yarn、ES等组件。</p> <p>8.支持用户权限认证，对存放在HDFS/HBase中的数据根据认证用户进行读/写访问控制；并支持支持ACL和Policy方式授权机制；</p> <p>9.支持web化的基于角色的统一权限管控，包括HDFS、YARN、HBase、Hive、Kafka、ES和Solr等组件。</p> <p>10.支持对集群所有主机进行全方位的统一管理：查看主机的资源使用分布统计图，如CPU/磁盘/内存/网络接收发送使用率等；查看主机列表信息：主机状态、IP、CPU、内存、磁盘使用率。</p> <p>11.支持一键进行集群健康检查和主机健康检查，并能导出健康检查报告，及时发现集群潜在风险。</p> <p>12.支持计划性迁移即容灾演练，支持启停保护组以及故障恢复。</p> <p>13.提供5年的软件质保，在质保期内提供免费升级服务。</p> <p>▲14.为保障产品稳定性，降低运维难度，要求大数据软件与云计算软件同一品牌。</p>	1	套
			6	OCR识别软件	<p>1.识别类型：印刷体；</p> <p>2.输入图像格式：支持 jpg、png、tiff、bmp 等常见图像格式；</p> <p>3.图像颜色：支持彩色、灰度、黑白</p> <p>4.图像分辨率：待识别的单个字符高度大于 20 像素，字号支持小六号到初号；</p> <p>5.中文字符集：大字符集；</p> <p>6.文档方向：文档方向 支持文档的四个方向判断，输出四个方向角度信息（0°、90°、180°、270°）；</p> <p>7.识别精度：字符准确率 99%以上（背景干净，字迹清晰）；</p>	1	套
采购包3：					8.识别速度：≤1.5s 左右/400-600 字；		
供应商报价不允许超过标的金额					9.支持1200个以上并发访问。		
（招单价的）供应商报价不允许超过标的单价							

参数性质	序号	技术参数与性能指标
		<p style="text-align: center;">(一)软件平台部分</p> <p>一、建设背景</p> <p>陕西省公安机关执法办案综合管理平台建设项目应按照《关于分批次组织开展全国执法办案数据治理和汇聚上报工作的通知》、《公安机关接报案与立案工作规定》、《公安机关执法细则》等相关工作规定，全面整合执法办案和监督管理数据资源，规范相关业务标准，联通部省数据汇聚渠道，加强执法大数据智能应用服务，为下一步部平台数据反哺、数据应用提供有力数据支撑。调整完善执法办案业务流程，拓展执法监督业务，建设全省统一管理执法办案管理中心应用，助推我省法治公安建设质量变革、效率变革、动力变革。</p> <p>二、建设内容</p> <p>本项目建设相关系统部署在陕西省公安厅“三秦警务云（信创云--新建）”平台，项目涵盖的业务对象为陕西省公安厅。一旦该系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，还会对社会秩序和公共利益造成损害。</p> <p>根据《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）和《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020），本项目信息系统均应满足等保2.0三级相关要求。</p> <p>本次不进行等级保护软硬件基础设施建设，进行系统等级保护设计，设计按等级保护三级进行。</p> <p>三、项目要求</p> <p>1.等级保护测评方案</p> <p>1.1等级测评工作目的</p> <p>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。</p> <p>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。</p> <p>1.2开展等级测评的时机</p> <p>（一）安全建设整改前</p> <p>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。</p> <p>（二）安全建设整改后</p> <p>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。</p> <p>（三）定期开展等级测评</p> <p>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。</p>

《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)整个系统的网络拓扑结构；
- 2)能够完成被测定级对象不同业务使命的业务应用系统；
- 3)业务备份系统；
- 4)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；
- 5)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
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，检查机房及其除湿设备等过程，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
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。
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	
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。
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。渗透测试不只是一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7名人员。项目组内须明确项目经理、质量监督、测评实施、渗透实施等角色分工，组内成员高级测评师不少于1人，中级测评师不少于2人，初级测评师不少于2人，渗透测试人员不少于2人。

(二)硬件部分

一、招标要求

1.测评系统：陕西省公安机关执法办案综合管理平台部署环境("三秦警务云-信创域"云平台)

2.人员要求：本项目高级测评师不得少于1人，中级测评师不得少于2人，初级测评师不得少于2人。

3.项目成果：

《XXXXXX等级保护测评项目系统测评方案》

《XXXXXX等级保护测评项目系统等级保护整改建议书》

《XXXXXX等级保护测评项目系统等级保护测评报告》

二、技术要求

1.项目概况:

为保障陕西省公安机关执法办案综合管理平台部署环境("三秦警务云-信创域"云平台)的重要网络安全运行,落实《中华人民共和国网络安全法》《信息安全等级保护管理办法》等国家法律法规要求,结合我单位的实际情况,现对1个信息系统开展等级保护测评服务工作。

2.服务总体要求:

测评服务要求:依据《基本要求》(GB/T 22239-2019)、《测评要求》(GB/T 28448-2019)和《测评过程指南》(GB/T 28449-2018)等国家关于网络安全等级保护2.0的相关标准和规范要求,为陕西省公安机关执法办案综合管理平台部署环境("三秦警务云-信创域"云平台)提供相应级别信息系统等级保护测评实施工作,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、安全运维管理测评。

渗透测试服务要求:服务商的渗透测试工程师要模拟恶意黑客的攻击方法,来对我单位计算机网络的安全性进行检测评估。对系统和网络进行非破坏性质的攻击性测试,尝试侵入系统,获取系统控制权并将入侵的过程和细节产生报告,由此证实系统所存在的安全威胁和风险,及时提示开发人员修复安全漏洞,提醒安全管理员完善安全策略,提升系统安全防护能力,为保证本次项目渗透的质量,参与本项目的项目经理需要参与过测评机构能力验证(应用安全渗透测试),且结果为满意。

安全需求分析及设计服务要求:为保障陕西省公安机关执法办案综合管理平台重要信息系统的安全防护能力,服务商需对其信息系统提供安全需求分析,并且能对陕西省公安机关执法办案综合管理平台部署环境("三秦警务云-信创域"云平台)的信息系统做安全方案设计,提出有针对性的安全规划方案。

应急响应及应急处理要求:服务商在测评项目结束后,要提供至少一年的信息安全应急处理保障。一旦被测系统出现紧急重大安全事件,收到陕西省公安厅的服务请求,测评单位工程师在3小时内到达用户现场,提供服务。

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

安全培训服务:服务商需提供网络安全培训服务2次,培训内容包括网络安全意识、网络安全技术、网络安全政策法规等。

重保服务:根据陕西省公安厅的实际需要,在重大节日活动、重要会议召开前等关键时间点提供专业漏洞扫描服务不少于6次。

服务商须服从陕西省公安厅的统一协调,且必须在项目实施期间由服务商派驻有丰富实施经验的信息安全等级保护测评中级及以上测评师为项目实施团队主要负责人和核心成员,全程参与项目实施。

服务商须提供完善的测评实施方案和计划、测评方案,经我单位审核通过后实施,并完成我单位对安全管理制度的补充完善和整理工作,配合对我单位信息系统进行整改测评服务。

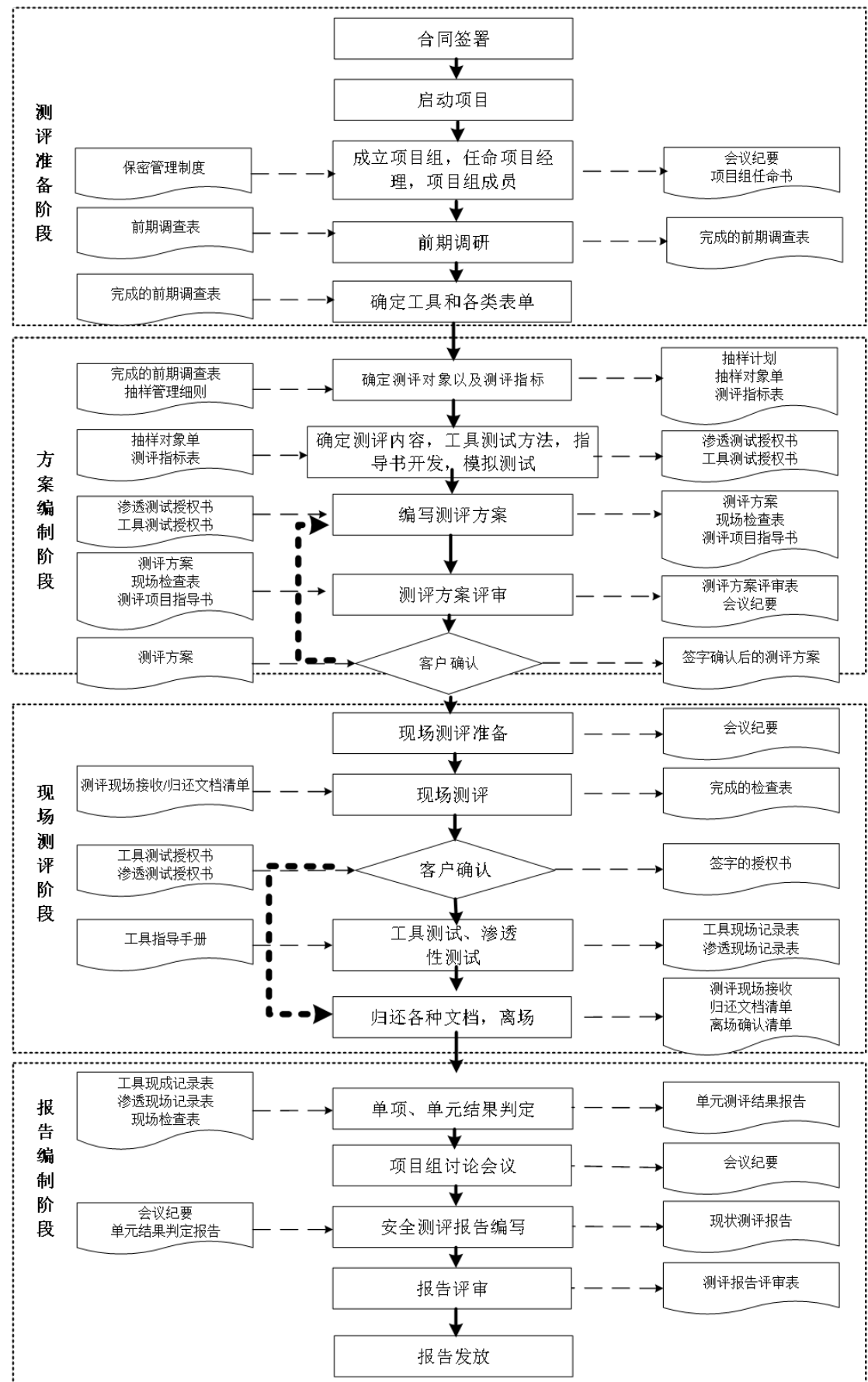
服务商须与我单位签订项目合同、保密协议和现场评测授权书、风险预判告知书,核实驻场测评师资质与投标时对本项目配备的测评师是否一致。确因工作调配需更换测评师,需提前10个工作日向我信息部门负责人书面报备,并提供更换测评师资质证明。

测评结束后,服务方需免费提供整改咨询服务和免费质保服务,并提供为期一年的售后服务,就本项目成果中的具体内容提供解释,提供信息系统等级保护相关工作的技术支持和咨询服务,以帮助陕西省公安厅提高安全防护能力。

网络与信息安全信息通报服务要求:服务商需要在测评结束后,提供至少的一年网络信息安全通报服务,要与我单位建立完善的通报和沟通机制,及时按照国家标准提供对应服务。

3.实施流程及工作内容要求

信息安全等级保护测评工作的流程如下图所示，在开展信息安全等级保护测评工作过程中要求严格遵循如下流程：



①测评准备活动

本活动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评系统的详细情况，准备测评工

具，为编制测评方案做好准备。

②方案编制活动

本活动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评信息系统相适应的测评对象、测评指标及测评内容等，并根据需要开发测评指导书，形成测评方案。

③现场测评活动

本活动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，严格执行测评指导书，分步实施所有测评项目，包括单位测评和整体测评两个方面，以了解系统的真实保护情况，获取足够证据，发现系统存在的安全问题。

④分析与报告编制活动

本活动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行标的有关要求，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评系统面临的风险，提出整改意见并配合被测评单位完成整改，从而给出等级测评结论，形成测评报告文本。

测评指标：

二级要求指标：

安全层面	安全控制点	测评指标（2.0）
安全物理环境	物理位置选择	a)机房场地应选择在具有防震、防风和防雨等能力的建筑内；
		b)机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。
	物理访问控制	a)机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。
	防盗窃和防破坏	a)应将设备或主要部件进行固定，并设置明显的不易除去的标记；
		b)应将通信线缆铺设在隐蔽处。
	防雷击	a)应将各类机柜、设施和设备等通过接地系统安全接地。
	防火	a)机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；
		b)机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。
	防水防潮	a)应采取措施防止雨水通过机房窗口、屋顶和墙壁渗透；
		b)应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。
	防静电	a)应采用防静电地板并采用必要的接地防静电措施。
	温湿度控制	a)应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。

			电力供应	a)应在机房供电线路上配置稳压器和过电压防护设备；
				b)应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。
			电磁防护	a)电源线和通信线缆应隔离铺设，避免互相干扰。
安全通信网络		网络架构		a)应划分不同的网络区域，并按照方便管理和控制的原则为各个网络区域分配地址；
				b)应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。
		通信传输		a)应采用校验技术保证通信过程中数据的完整性。
		可信验证		a)可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，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
安全区域边界			边界防护	a)应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。
			访问控制	a)应在网络边界或区域之间访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；
				b)应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；
				c)应对源地址、目标地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；
				d)应根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。
			入侵防范	a)应在关键网络节点处监视网络攻击行为。
			恶意代码防范	a)应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。
			安全审计	a)应在网络边界，重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
				b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
				c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。
			可信验证	a)可基于可信根对边界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，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

安全计算环境	身份鉴别	a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；
		b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登陆次数和当登录连接超时自动退出等相关措施；
		c)当进行远程管理时，应采取必要的措施防止鉴别信息在网络传输过程中被窃听。
	访问控制	a)应对登录的用户分配账户和权限；
		b)应重命名或删除默认账户，修改默认账户的默认口令；
		c)应及时删除或停用多余的、过期的账户，避免共享账户的存在；
		d)应授予管理用户所需的最小权限，实现管理用户的权限分离。
	安全审计	a)应提供安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
		b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
		c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。
	入侵防范	a)应遵循最小安装的原则，仅安装需要的组件和应用程序；
		b)应关闭不需要的系统服务、默认共享和高危端口；
		c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；
		d)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求。
		e)应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。
	恶意代码防范	a)应安装方恶意代码软件或配置具有相应功能的软件，并及时更新防恶意代码软件版本和恶意代码库。
	可信验证	a)可基于可信根对计算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，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
	数据完整性	a)应采用校验技术保证重要数据在传输过程中的完整性。
	数据备份和恢复	a)应提供重要数据的本地数据备份与恢复功能；

			b)应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
		剩余信息保护	a)应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。
		个人信息保护	a)应仅采集和保存业务必需的用户个人信息；
			b)应禁止未授权访问和非法使用用户个人信息。
	安全管理中心	系统管理	a)应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；
			b)应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。
		审计管理	a)应对安全审计员进行身份鉴别，只允许通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；
			b)应通过安全审计员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询。
	安全管理制度	安全策略	a)应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。
		管理制度	a)应对安全管理活动中的主要管理内容建立安全管理制度；
			b)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。
		制定和发布	a)应指定或授权专门的部门或人员负责安全管理制度的制定；
			d)安全管理制度应通过正式、有效的方式发布，并进行版本控制。
		评审和修订	a)应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足需要改进的安全管理制度进行修订。
		岗位设置	a)应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；
			b)应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各工作岗位的职责。
		人员配备	a)应配备一定数量的系统管理员、审计管理员、安全管理员等。

安全管理机构	授权和审批	a) 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；
		b) 应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程。
	沟通和合作	a) 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理信息安全问题；
		b) 应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；
		c) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。
	审核和检查	a) 应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。
	人员录用	a) 应指定或授权专门的部门或人员负责人员录用；
		b) 应对被录用人的身份、安全背景、专业资格或资质等进行审查。
	人员离岗	a) 应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。
	安全意识教育和培训	a) 应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。
安全管理人员	外部人员访问管理	a) 应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；
		b) 应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户，分配权限，并登记备案；
		c) 外部人员离场后应及时清除其所有的访问权限。
	定级和备案	a) 应以书面的形式说明保护对象的安全保护等级及确定安全保护等级的方法和理由；
		b) 应组织相关部门和有关安全技术专家对信息系统定级结果的合理性和正确性进行论证和审定；
		c) 应保证定级结果经过相关部门的批准；
		d) 应将备案材料报主管部门和公安机关备案。
	安全方案设计	a) 应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；
		b) 应根据保护对象的安全保护等级进行安全方案设计；
		c) 应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。

安全建设管理

产品采购和使用	a) 应确保网络安全产品的采购和使用符合国家的有关规定;
	b) 应确保密码产品与服务的采购和使用符合国家密码主管部门的要求。
自行软件开发	a) 应将开发环境与实际运行环境物理分开, 测试数据和测试结果受到控制;
	b) 应在软件开发过程中对安全性进行测试, 在软件安装前对可能存在的恶意代码进行检测。
外包软件开发	a) 应在软件交付前检测其中可能存在的恶意代码;
	b) 应保证开发单位提供软件设计文档和使用指南。
工程实施	a) 应指定或授权专门的部门或人员负责工程实施过程的管理;
	b) 应制定安全工程实施方案控制工程实施过程。
测试验收	a) 应制订测试验收方案, 并依据测试验收方案实施测试验收, 形成测试验收报告;
	b) 应进行上线前的安全性测试, 并出具安全测试报告。
系统交付	a) 应制定交付清单, 并根据交付清单对所交接的设备、软件和文档等进行清点;
	b) 应对负责系统运行维护的技术人员进行相应的技能培训;
	c) 应提供系统建设过程文档和运行维护文档。
等级测评	a) 应定期进行等级测评, 发现不符合相应等级保护标准要求的及时整改;
	b) 在发生重大变更或级别发生时进行等级测评;
	c) 应确保测评机构的选择符合国家相关规定。
服务供应商管理	a) 应确保服务供应商的选择符合国家的有关标准;
	b) 应与选定的服务供应商签订相关协议, 明确整个服务供应链各方需履行的网络安全相关义务。
环境管理	a) 应指定专门的部门或人员负责机房安全, 对机房出入进行管理, 定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理;
	b) 应对机房的安全管理作出规定, 包括物理访问, 物品进出和环境安全等;
	c) 应不在重要区域接待来访人员, 不随意放置包含敏感信息的纸质文件和移动介质等。
资产管理	a) 应编制并保存与保护对象相关的资产清单, 包括资产责任部门、重要程度和所处位置等内容。

安全运维管理

介质管理	a) 应确保介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理并根据存档介质的目录清单定期盘点；
	b) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，对介质归档和查询等进行登记记录。
设备维护管理	a) 应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；
	b) 应对配套设施、软硬件维护管理作出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。
漏洞和风险管理	a) 应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或评估可能的影响后进行修补。
网络和系统安全管理	a) 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；
	b) 应指定专门的部门或人员进行账户管理，对账户申请，建立账户、删除账户等进行控制；
	c) 应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；
	d) 应制定重要设备的配置和操作手册，依据操作手册对设备进行安全配置和优化配置等；
	e) 应详细记录运维操作日志，包括日常巡检工作，运行维护记录、参数的设置和修改的内容。
恶意代码防范管理	a) 应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；
	b) 应对防恶意代码防范要求作出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；
	c) 应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。
配置管理	a) 应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。
密码管理	a) 应遵循密码相关的国家标准和行业标准；
	b) 应使用国家密码管理局认证核准的密码技术和产品。
变更管理	a) 应明确变更需求，变更前根据变更需求制定变更方案、变更方案经过评审、审批后方可实施。

备份与恢复管理	a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等;
	b) 应规定备份信息的备份方式、备份频度、存储介质和保存期等;
	c) 应根据数据的重要性的和数据对系统运行的影响, 制定数据的备份策略和恢复策略, 备份程序和恢复程序。
安全事件处置	a) 应及时向安全管理部门报告所发现的安全弱点和可疑事件;
	b) 应制定安全事件报告和处置管理制度, 明确不同安全事件的报告、处置和响应流程, 规定安全事件的现场处理、事件报告和后期恢复的管理职责等;
	c) 应在安全事件和响应处理过程中, 分析和鉴定事件产生的原因, 收集证据, 记录处理过程, 总结经验教训。
应急预案管理	a) 应制定重要事件的应急预案, 包括应急处理流程、系统恢复流程等内容;
	b) 应定期对系统相关的人员进行应急预案培训, 并进行应急预案的演练。
外包运维管理	a) 应确保外包运维服务商的选择符合国家有关规定;
	b) 应与选定的外包运维服务商签订相关的协议, 明确约定外包运维的范围、工作内容。

三级要求指标:

安全层面	安全控制点	测评指标 (2.0)
	物理位置选择	a) 机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内;
		b) 机房场地应避免设在建筑物的高层或地下室, 否则应加强防水和防潮措施。
	物理访问控制	a) 机房出入口应配置电子门禁系统, 控制、鉴别和记录进入的人员。
	防盗窃和防破坏	a) 应将设备或主要部件进行固定, 并设置明显的不易除去的标识;
		b) 应将通信线缆铺设在隐蔽安全处;
		c) 应设置机房防盗报警系统或设置有专人值守的视频监控系统。
	防雷击	a) 应将各类机柜、设施和设备等通过接地系统安全接地;

				安全物理环境		b)应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。
					防火	a)机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；
						b)机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；
						c)应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。
					防水防潮	a)应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；
						b)应采取措施防止机房内水蒸气结露和地下积水的转移与渗透；
						c)应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。
					防静电	a)应采用防静电地板或地面并采用必要的接地防静电措施；
						b)应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。
					温湿度控制	a)应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。
					电力供应	a)应在机房供电线路上配置稳压器和过电压防护设备；
						b)应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求；
						c)应设置冗余或并行的电力电缆线路为计算机系统供电。
					电磁防护	a)电源线和通信线缆应隔离铺设，避免互相干扰；
						b)应对关键设备实施电磁屏蔽。
				安全通信网络	网络架构	a)应保证网络设备的业务处理能力满足业务高峰期需要；
						b)应保证网络各个部分的带宽满足业务高峰期需要；
						c)应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；
						d)应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段；
						e)应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。
					通信传输	a)应采用校验技术或密码技术保证通信过程中数据的完整性；
						b)应采用密码技术保证通信过程中数据的保密性。

					可信验证	a)可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，在监测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
					安全区域边界	a)应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信；
						b)应能够对非授权设备私自联到内部网络的行为进行检测或限制；
						c)应能够对内部用户非授权联到外部网络的行为进行检查或限制；
						d)应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。
						a)应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；
						b)应删除多余或无效的控制规则，优化访问控制列表，并保证访问控制规则数量最小化；
						c)应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；
						d)应根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力；
						e)应对进出网络的数据流实现基于应用协议和应用内容的访问控制。
						a)应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；
						b)应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为；
						c)应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；
						d)当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。
						a)应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新；
						b)应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。
						a)应在网络边界，重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

				安全审计	b)审计记录应包括事件的日期、用户、事件类型、事件是否成功及其他与审计相关的信息；
					c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
					d)应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。
				可信验证	a)可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护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，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
				身份鉴别	a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；
					b)应启用登陆失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时时自动退出等相关措施；
					c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；
					d)应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术实现。
				访问控制	a) 应对登录的用户分配账户和权限；
					b) 应重命名或删除默认账户，修改默认账户的默认口令；
					c) 应及时删除或停用多余的，过期的账户，避免共享账户的存在；
					d) 应授予管理用户所需的最小权限，实现管理用户的权限分离；
					e) 应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；
					f)访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；
					g)应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。
				安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
					b) 审计记录应包括事件的日期、时间、事件类型、事件是否成功及其他与审计相关的工作；

安全计算环境		c) 应对审计记录进行保护，定期备份、避免受到未预期的删除、修改或覆盖等；
		d) 应对审计进程进行保护，防止未经授权的中断。
	入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；
		b) 应关闭不需要的系统服务、默认共享和高危端口；
		c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；
		d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求。
		e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；
		f) 应能检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。
	恶意代码防范	a) 应采用免受恶意代码攻击的技术措施，或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。
	可信验证	a) 可基于可信根对计算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，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
	数据完整性	a) 应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于数据鉴别、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；
		b) 应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于数据鉴别、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。
	数据保密性	a) 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于数据鉴别、重要业务数据和重要个人信息等；
		b) 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于数据鉴别、重要业务数据和重要个人信息等。
		a) 应提供重要数据的本地数据备份与恢复功能；

				数据备份和恢复	b) 应提供异地实时备份功能，利用通信网络将重要数据实时备份至备用场地；
					c) 应提供重要数据处理系统的冗余，保证系统的高可用性。
				剩余信息保护	a)应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；
					b)应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。
				个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；
					b) 应禁止未授权访问和非法使用用户个人信息。
	安全管理中心	系统管理	a)应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；		
			b) 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份，系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。		
		审计管理	a) 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；		
			b)应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询。		
		安全管理	a) 应对安全管理员进行身份鉴别，只允许通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计；		
			b)应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体，客体进行统一安全标识，对主体进行授权，配置安全可信验证策略等。		
		集中管控	a) 应划分特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；		
			b)应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；		
			c) 应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；		
			d)应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求；		
			e) 应对安全策略、安全代码、补丁升级等安全事项进行集中管理；		

			f) 应能对网络中发生的各类安全事件进行识别报警和分析。
	安全管理制度	安全策略	a) 应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。
		管理制度	a) 应对安全管理活动中的各类管理内容建立安全管理制度；
			b) 应对要求管理人员或操作人员执行的日常管理操作建立操作规程；
			c) 应形成由安全策略，管理制度，操作规程，记录表单等构成安全管理制度体系。
		制定和发布	a) 应指定或授权专门的部门或人员负责安全管理制度的制定；
			d) 安全管理制度应通过正式、有效的方式发布，并进行版本控制。
		评审和修订	a) 应定期对安全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。
	安全管理机构	岗位设置	a) 应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权；
			b) 应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；
			c) 应设立系统管理员、审计管理员、安全管理员等岗位，并定义部门及各个工作岗位的职责。
		人员配备	a) 应配备一定数量的系统管理员、审计管理员、安全管理员等；
			b) 应配备专职的安全管理员，不可兼任。
		授权和审批	a) 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；
			b) 应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；
			c) 应定期审查审批事项，及时更新授权和审批的项目、审批部门和审批人等信息。
		沟通和合作	a) 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题。；
			b) 应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；

				c) 应建立外联单位联系列表, 包括外联单位名称、合作内容、联系人和联系方式等信息。
			审核和检查	a) 应定期进行常规安全检查, 检查内容包括系统日常运行、系统漏洞和数据备份等情况; b) 应定期进行全面安全检查, 检查内容包括现有安全技术措施的有效性、安全配置和安全策略的一致性, 安全管理制度的执行情况等; c) 应制定安全检查表格实施安全检查, 汇总安全检查数据, 形成安全检查报告, 并对安全检查结果进行通报。
		安全管理人员	人员录用	a) 应指定或授权专门的部门或人员负责人员录用; b) 应对被录用人的身份、安全背景、专业资格或资质等进行审查, 对其所有的技术技能进行考核; c) 应与被录用人员签署保密协议, 与关键岗位人员签署岗位责任协议。
			人员离岗	a) 应及时终止离岗人员的所有访问权限, 取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备; b) 应办理严格的调离手续, 并承诺调离后的保密义务方可离开。
			安全意识教育和培训	a) 应对各类人员进行安全意识教育和岗位技能培训, 并告知相关的安全责任和惩戒措施; b) 应针对不同岗位制定不同的培训计划, 对安全基础知识, 岗位操作规程等进行培训; c) 应定期对不同岗位的人员进行技能考核。
			外部人员访问管理	a) 应在外部人员物理访问受控区域前提出书面申请, 批准后由专人全程陪同, 并登记备案; b) 应在外部人员接入受控网络访问系统前提出书面申请, 批准后由专人开设账户, 分配权限, 并登记备案; c) 外部人员离场后应及时清除其所有的访问权限; d) 获得系统访问授权的外部人员签署保密协议, 不得进行非授权操作, 不得复制和泄露敏感信息。
			定级和备案	a) 应以书面的形式说明保护对象的安全保护等级及确定安全保护等级的方法和理由; b) 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定; c) 应保证定级结果经过相关部门的批准; d) 应将备案材料报主管部门和相应公安机关备案

安全建设管理	安全方案设计	a) 应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；
		b) 应根据保护对象的安全保护等级及与其他级别对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容、并形成配套文件；
		c) 应组织相关部门和有关安全技术专家对整体安全规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。
	产品采购和使用	a) 应确保网络安全产品采购和使用符合国家的有关规定；
		b) 应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求；
		c) 应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新产品候选名单。
	自行软件开发	a) 应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；
		b) 应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；
		c) 应制定代码编写安全规范，要求开发人员参照规范编写代码；
		d) 应具备软件设计的相关文档和使用指南，并对文档使用进行控制；
		e) 应保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测；
		f) 应对程序资源库的修改、更新，发布进行授权和批准，并严格进行版本控制；
		g) 应保证开发人员为专职人员，开发人员的开发活动受到控制，监视和审查。
	外包软件开发	a) 应在软件交付前检测其中可能存在的恶意代码；
		b) 应保证开发单位提供软件设计文档和使用指南；
		c) 应保证开发单位提供软件源代码，并审查软件中可能存在的后面和隐蔽信道。
	工程实施	a) 应指定或授权专门的部门或人员负责工程实施过程的管理；
		b) 应制定安全工程实施方案控制实施过程；
		c) 应通过第三方工程监理控制项目的实施过程。
	测试验收	a) 应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；

					b) 应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性安全测试内容。
				系统交付	a) 应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；
					b) 应对负责系统运行维护的技术人员进行相应的技能培训；
					c) 应提供建设过程文档和运行维护文档。
				等级测评	a) 应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；
					b) 在发生重大变化或级别发生时进行等级测评；
					c) 应确保测评机构的选择符合国家相关规定。
				服务供应商管理	a) 应确保服务供应商的选择符合国家的有关规定；
					b) 应与选定的服务商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务；
					c) 应定期监督、评审和审核服务供应商提供的服务，并对其变更服务进行控制。
				环境管理	a) 应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；
					b) 应建立机房安全管理制度，对有关物理访问，物品带进带出和环境安全等方面的管理作出规定；
					c) 应不在重要区域接待来访人员，不随意放置包含敏感信息的纸质文件和移动介质。
				资产管理	a) 应编制并保存与信息系统相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；
					b) 应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；
					c) 应对信息分类与标识方法做出规定，并对信息的使用，传输和存储等进行规范化管理。
				介质管理	a) 应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理并根据存档介质的目录清单定期盘点；
					b) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质归档和查询等进行登记记录。
					a) 应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；

安全运维管理	设备维护管理	b) 应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等；
		c) 信息处理设备应经过审批才能带离机房或办公地点，含有储存介质的设备带出工作环境时其重要数据应加密；
		d) 含有存储介质的设备在报废或重用前，应进行完全清除或完全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。
	漏洞和风险管理	a) 应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或评估可能的影响后进行修补；
		b)应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。
	网络和系统安全管理	a) 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；
		b) 应指定专门的部门或人员进行账户管理，对申请账户，建立账户、删除账户等进行控制；
		c) 应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；
		d) 应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；
		e) 应详细记录运维操作日志，包括日常巡检工作，运行维护记录、参数的设置和修改的内容；
		f) 应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为；
		g) 应严格控制变更性运维，经过审批后才可改变连接，安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步配置更新配置信息库；
		H) 应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据；
i) 应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道；		
j) 应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略行为。		

恶意代码防范管理	a) 应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；
	b) 应定期验证防范恶意代码攻击的技术措施的有效性。
配置管理	a) 应记录和保存基本配置信息，包括网络拓扑结构、各类设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等；
	b) 应将基本信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。
密码管理	a) 应遵循密码相关国家标准和行业标准；
	b) 应使用国家密码管理主管部门认证核准的密码技术和产品。
变更管理	a) 应明确变更需求，变更前根据变更需求制定变更方案、变更方案经过评审、审批后方可实施；
	b) 应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程；
	c) 应建立终止变更并从失败的变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。
备份与恢复管理	a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等；
	b) 应规定备份信息的备份方式、备份频度、存储介质和保存期等；
	c) 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略，备份程序和恢复程序等。
安全事件处置	a) 应及时向安全管理部门报告所发现的安全弱点和可疑事件；
	b) 应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；
	c) 应在安全事件和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训；
	d) 对造成系统中断和造成信息泄露的重大安全事件应采用不同的处理程序和报告程序。
	a) 应规定统一的应急预案框架，包括启动预案的条件，应急组织构成，应急资源保障，事后教育和培训内容；

			应急预案管理	b) 应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；
				c) 应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练；
				d)应定期对原有的应急预案重新评估，修订完善。
			外包运维管理	a) 应确保外包运维服务商的选择符合国家有关规定；
				b) 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容；
				d) 应保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力在签订的协议中明确；
				d) 应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、储存要求，对IT基础设施中断服务的应急保障要求等。
			总计：211	

三、项目管理要求

1.项目管理总体要求

服务商应在被陕西省公安厅统一组织协调下，开展好前期调研、现场实施和报告撰写等工作。测评机构所提供的项目经理和实施人员应是具有丰富经验和专业技能的技术骨干，应有同类项目经验。在测评机构以往参与的项目中，应具有项目实施、熟悉项目需求和团队建设方面的优势。测评机构应在项目全过程中严格遵循各项管理制度的要求，确保项目顺利开展。

本项目测评驻场人员要求：承担本次测评工作的供应商至少有1名高级测评师，2名中级测评师,3名初级测评师。本次等保测评服务不得转包或者分包，所有驻场测评师必须是测评机构自己的正式在职员工,所有驻场测评师必须持证上岗，投标文件中应提供项目组驻场人员名单以及社保主管部门出具的响应单位为其缴纳社保的证明、驻场人员信息安全等级测评师证书复印件，未经采购方同意，项目组成员不得更改。

2.项目管理保密要求

测评机构应与被测评单位签订正式保密协议，并在工作中坚持保密原则，确保应答人及其员工严格规范执行各项保密制度，杜绝任何泄密事件的发生。测评机构需明确将采取的保密措施，对员工的保密管理措施，以及一旦发生泄密事件将采取的措施、需承担的责任。

采购包4:

3.项目风险控制

测评机构应能够对信息安全等级测评项目过程进行充分的风险考虑, 并制定相应的风险规避措施和控制方法。在项目实施过程中, 应做好计划与安排, 不影响被测评单位正常业务工作的开展。

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: 服务

参数性质	序号	技术参数与性能指标
		<p>(一)软件平台部分</p> <p>一、建设背景</p> <p>陕西省公安机关执法办案综合管理平台建设项目应按照《关于分批次组织开展全国执法办案数据治理和汇聚上报工作的通知》、《公安机关接报案与立案工作规定》、《公安机关执法细则》等相关</p>

工作规定，全面整合执法办案和监督管理数据资源，规范相关业务标准，联通部省数据汇聚渠道，加强执法大数据智能应用服务，为下一步部平台数据反哺、数据应用提供有力数据支撑。调整完善执法办案业务流程，拓展执法监督业务，建设全省统一管理执法办案管理中心应用，助推我省法治公安建设质量变革、效率变革、动力变革。

二、建设内容

2.1 信息系统密码应用等级

本项目建设相关信息系统均应满足三级密评相关要求，需要与密码应用平台实现对接。

本项目不进行密码软、硬件基础设施建设，进行密码应用设计规划。密码软硬件基础设施建设相关预算在《陕西省公安厅网络安全体系升级项目（安全加固）》项目中统一规划。

本次建设系统需调用密码应用平台认证、签名验签、加解密、时间戳等安全服务能力，以期符合密码应用安全性评估要求，满足系统机密性、完整性和真实性和不可否认性要求，达到三级密评要求。

本项目不进行密码软、硬件基础设施建设，只进行密码应用设计规划。密码软硬件基础设施建设相关预算在《陕西省公安厅网络安全体系升级项目（安全加固）》项目中统一规划。

对密码应用平台的需求：

为给用户颁发具有高安全性的数字证书提供有效支撑

为在安全浏览器下实现应用程序无感知的数据加密传输提供有效支撑

为应用系统提供满足密评等级的各类算法的数据加密、数据解密等密码应用服务，为敏感数据的存储打下基础

为应用系统提供满足密评等级的各类算法的数据摘要、数据摘要验签等密码应用服务，为关键数据的防篡改打下基础

密码应用平台所提供的密码服务在网络通畅的情况下，密码应用服务单次调用的响应延迟应不超过1秒，在单个服务调用并发量上应大于应用系统的访问并发。

由于本次项目中将要对接的密码应用平台还处在建设阶段，因此在本项目的建设过程中将提前规划密码应用服务的应用，并把本项目中涉及到的密码应用需求提交到《陕西省公安厅网络安全体系升级项目（安全加固）》项目的承建部门以提前规划好相应的密码应用资源以便后续能满足本项目中涉及到的密码应用需求。

2.2 信息系统密码应用要求

本项目信息系统均应满足三级密评相关要求，需要与密码应用平台实现对接。

本项目不进行密码软、硬件基础设施建设，进行密码应用设计规划。密码软硬件基础设施建设相关预算在《陕西省公安厅网络安全体系升级项目（安全加固）》项目中统一规划。

密码应用平台功能需求为对云平台和云平台上承载的业务系统提供密码服务。密码服务具体包括身份鉴别服务、SSL VPN加密服务、签名验签服务、加解密服务、时间戳服务等。本次建设系统需调用密码应用平台认证、签名验签、加解密、时间戳等安全服务能力，以期符合密码应用安全性评估要求，满足系统机密性、完整性和真实性和不可否认性要求，达到三级密评要求。

根据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等层面，对云上业务系统进行风险分析，得出云上

业务系统密码应用需求。

1. 物理和环境安全

物理和环境安全主要实现三秦警务云云上业务系统所在物理机房环境安全。三秦警务云云上业务系统所在的物理和环境安全得不到保障,则设备、数据、应用等都将直接暴露在威胁之下,业务系统的安全就无从谈起。利用密码技术确保信息系统的物理和环境安全,可以有效阻断外界对信息系统各类重要场所、监控设备的直接入侵,并确保监控记录信息不被恶意篡改。对于物理和环境的密码应用需求主要有两方面:一是对于物理和环境的访问控制,即未授权人员无法访问重要场所、重要设备和监控设备;二是对各类物理和环境的监控信息的完整性保护,包括人员进入记录、监控记录等,实现事前威慑、事中监控、事后追责。具体来看,需要采用密码技术实现如下两个方面:

确保对进入三秦警务云云上业务系统所在人员进行基于密码技术的身份鉴别;确保电子门禁系统记录信息和机房视频数据的完整性。

2. 网络和通信安全

云上业务系统的网络和通信安全首先要确保用户和管理员对于云上系统的通信链路中的身份真实合法、数据机密性和完整性。同时应实现云上应用系统和其他业务系统的通信链路的安全,利用网络边界访问控制设备的自身安全机制保证访问控制信息的完整性,实现云上业务系统之间的通信链路的安全。

3. 设备和计算安全

云上业务系统的设备与计算安全首先要确保应用管理员登录云资源虚拟机身份的真实性,同时需要确保虚拟机内操作系统或数据库软件的访问控制信息、重要信息资源敏感标记、日志信息的机密性和完整性等。

4. 应用和数据安全

(1) 身份鉴别需求

云上业务应用系统用户登录时需使用密码技术对用户进行身份鉴别,保证登录人员身份的真实性,并确保身份鉴别信息的防截获、防假冒和防重用。

(2) 敏感数据传输安全

云上业务应用系统的身份鉴别信息、重要业务数据、密钥等敏感数据在传输过程中存在被非法窃取和非授权篡改的风险,需使用密码技术保证云上业务应用系统的敏感数据在传输过程中的保密性、完整性,实现各类重要数据的防窃取和防篡改保护。

(3) 敏感数据存储安全

云上业务应用系统的身份鉴别信息、重要业务数据、密钥等敏感数据在存储过程中存在被非法窃取和非授权篡改的风险,需使用密码技术保证云上业务应用系统的身份鉴别信息、重要业务数据、密钥等敏感信息在存储过程中的保密性、完整性。

同时,需保证云上业务应用系统资源访问控制信息、业务日志信息的完整性,重要应用程序的加载与卸载,实现各类重要数据的防窃取和防篡改保护以及重要应用程序的安全控制。

(4) 关键操作不可否认性

云上业务应用系统中在用户管理、权限划分、应用与数据库资源配置等涉及法律责任认定的数据或重要操作,需使用密码技术保证云上业务应用系统中涉及法律责任认定的数据或重要操作的不可否认性保护。

5. 安全管理

(1) 风险分析

由陕西省公安厅三秦警务云云平台协助云上业务系统制定管理制度、人员管理、建设运行、应急处置等与云上业务系统相适应的密码安全管理制度和操作规程。

(2) 密码应用需求

依据《基本要求》，制定陕西省公安厅三秦警务云云上系统密码应用方案，并委托密评机构对密码应用方案进行评估，评估通过后，建设密码保障系统，制定密码相关的管理制度，系统改造完成后，对相关系统进行密码应用安全性评估，落实密码相关国家政策，确保国产密码在业务系统中发挥支撑作用。

6. 密钥管理安全

(1) 风险分析

本项目中密钥管理存在以下安全风险：

- 1) 生成的密钥缺少随机性，未使用合规的硬件密码设备，容易被攻击者猜测。
- 2) 密钥未采用合规的保护措施，容易被非法获取篡改，或密钥与实体之间的关联关系被非法篡改。
- 3) 密钥备份和归档机制不健全，导致密钥泄露，或密钥被恢复到非法的设备中。
- 4) 密钥销毁不及时导致密钥泄露，或销毁的密钥被恶意恢复。

(2) 密码应用需求

- 1) 密钥需由安全合规的密钥管理系统产生，保证密钥高质量。
- 2) 密钥安全存储在安全合规的密钥管理系统或以密文的形式存储在安全合规的商用密码产品外部，分发过程采用非对称算法的形式进行加密，保证传输的安全性。
- 3) 建立完善的密钥备份和归档机制，确保密钥不会被泄露，不会被密钥被恢复到非法的设备中。
- 4) 制定合理的密钥销毁机制，及时销毁不适用的密钥，确保被销毁的密钥不会被恶意恢复。

三.采购清单

密码测评采购表

序号	产品名称	数量	单位	备注
一	密码应用安全性评估服务			
1	政法协同办案系统第三级密码应用安全性评估	1	套	
2	违法犯罪人员信息系统第三级密码应用安全性评估	1	套	

四、项目要求

1.商用密码安全性评估方案

1.1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。

1.2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。				
1.3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				
1.4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
密码技术应用	物理和环境安全	身份鉴别	1	应
		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		

1.5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。

1.6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性	宜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。	信息系统所在机房等重要区域及其电子门禁系统。	<p>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；</p> <p>核查电子门禁系统是否具有商用密码产品认证证书；</p> <p>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>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。	<p>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；</p> <p>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；</p> <p>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>

（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。	<p>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；</p> <p>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；</p> <p>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；</p> <p>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。</p>
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。	<p>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；</p> <p>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>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。</p>
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。	<p>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；</p> <p>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>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。</p>

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。	<p>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；</p> <p>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；</p> <p>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；</p> <p>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；</p> <p>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。</p>
---	------	-----------------------------------	---	--

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。	<p>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；</p> <p>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；</p> <p>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。</p>
3	系统资源访问控制信息完整性	宜采用密码技术保证系统资源访问控制信息的完整性。	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。	<p>查看相关技术文档，访谈系统管理员，了解系统资源访问控制信息完整性保护密码技术及实现机制；</p> <p>查看是否使用国家密码管理部门认可的密码算法；</p> <p>密码设备是否获得商用密码产品认证证书。</p>
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。	<p>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；</p> <p>查看是否使用国家密码管理部门认可的密码算法；</p> <p>密码设备是否获得商用密码产品认证证书。</p>

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
----	------	------	------	------

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。	<p>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；</p> <p>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；</p> <p>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。</p>
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。	<p>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；</p> <p>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；</p> <p>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；</p> <p>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。</p>
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。	<p>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；</p> <p>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。</p>

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。	<p>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；</p> <p>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；</p> <p>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。</p>
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。	<p>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、和重要用户信息等存储在存储过程中的机密性保护技术及实现机制；</p> <p>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；</p> <p>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>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。</p>
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。	<p>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；</p> <p>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>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。</p>

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。	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。

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	<p>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。</p> <p>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；</p> <p>2) 对关键岗位建立多人共管机制；</p> <p>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；</p> <p>4) 相关设备与系统的管理和使用账号不得多人共用。</p>	<p>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）。</p>	<p>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。</p>
3	建立上岗人员培训制度	<p>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。</p>	<p>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）。</p>	<p>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。</p>

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。

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。
---	---------------	--	-----------------------------	---

1.7商用密码安全性评估要求

1.7.1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。

1.7.2人员配置要求

密码测评项目组要求密码测评人员不少于5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”。

(二)硬件部分

一、服务内容要求：

按照国家密码安全评估工作要求，拟开展以下系统密码安全评估工作：针对陕西省公安机关执法办案综合管理平台部署环境需求项目第三级的系统进行测评、备案。根据国家密码安全评估要求(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》、《商用密码应用安全性评估量化评估规则》)，结合陕西省公安机关执法办案综合管理平台部署环境需求项目密码安全建设情况，开展密码测评及备案工作，出具相关报告，同时结合密码安全测评报告，出具整改加固建议。

二、服务流程要求

本次项目拟按照“密码安全测评-备案-整改建议-培训”的思路进行，具体要求如下：

第一阶段：密码安全测评过程及内容

- 1）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。
- 2）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。
- 3）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。
- 4）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《信息系统密码应用测评过程指南》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。

第二阶段：备案

对系统进行密评备案工作，取得商用密码应用安全性评估报告后，按照国家有关规定报送国家密码管理部门或者关键信息基础设施所在地省、自治区、直辖市密码管理部门备案，并获得相应密评备案证明。

第三阶段：整改建设建议

以商用密码应用安全性测评报告发现的密码安全问题为工作重点依据，结合公司实际情况开展公司机关密码加固及建设整改工作，编写《信息系统密码安全建设整改建议》。将信息系统的密码安全建设整改需求落实到可操作的密码安全技术和管理上，提出能够实现的技术参数或制度及其具体规范。之后在招标人依据相关《信息系统密码安全建设整改建议》开展建设整改工作时，投标人将提供建设整改过程中的与建设整改相关的咨询服务。对信息系统密码安全整改建议进行确认，并依照建议，协助我方进行漏洞修复，补丁升级等非硬件层面的密码安全加固，制定可执行的密码安全整改方案和计划，然后协助分步实施密码安全整改工作。

第四阶段：培训

按照甲方要求，提供密码安全相关知识培训。

第五阶段：售后服务

为期一年的售后服务工作中，投标人将向招标人提供包括安全培训、配合检查、安全咨询等相关服务。具体服务内容如下：

- 1）安全培训：在项目实施过程中或在项目实施结束后，通过安全培训使有关人员加深对密码安全工作的掌握程度，并对行业内的最佳实践案例进行分享，从而达到将密码安全工作与信息系统、安全设备的安全运维工作相结合的状态。
- 2）根据需要组织开展信息安全服务培训，通过大量的当前典型安全事件导入，从感性认知层面对目前的信息安全威胁给予直观、形象的描述，加深对当前信息安全威胁的认识。
- 3）配合检查服务：投标人免费协助招标人响应密码管理局、单位内部以及第三方机构针对商用密码应用安全性评估工作的检查工作。服务内容包括协助招标人进行系统资料准备、完善各类资料文档，配合检查过程中的答疑及技术支持及其他现场检查的响应。
- 4）安全咨询服务：投标人为招标人免费提供一年技术咨询服务，包括新建信息系统密码安全建设方案咨询服务以及其他相关安全咨询服务，技术服务工程师在接到招标人服务请求后应立即响应，帮助

	<p>客户解决信息安全相关技术问题，全面配合招标人做好业务系统安全保障工作。</p> <p>三、项目实施团队配置</p> <p>1）投标人针对本项目成立项目组，应配备项目负责人一名，项目组成员（不含项目负责人）不少于五人。</p> <p>2）项目负责人及项目组成员应具有国家密码管理局商用密码检测中心的商用密码应用安全性评估人员能力合格证书</p> <p>四、最终达到项目目标</p> <p>1）完成系统商用密码应用安全性评估，明确各被测系统达到该系统等级所需的密码安全要求，掌握系统商用密码应用和管理方面存在的安全风险，并形成《2025年度信息系统密码安全性评估项目报告》。</p> <p>2）针对测评报告中指出的系统密码安全防护措施方面存在的问题和安全建设整改需要解决的问题，编制密码安全加固及整体建设规划，形成《信息系统密码安全建设整改建议》，为完系统密码安全防护体系提供指导依据，协助运维部门进行安全整改，提供整改咨询服务。</p> <p>3）向属地密码管理部门提交全部备案资料，完成本年度合同约定范围内所有系统商用密码应用安全性评估备案手续，并取得有效备案证明。</p> <p>4）项目周期：合同签订之日起三个月内完成上述服务内容；项目验收合格之日起十二个月内提供密码安全咨询服务。</p> <p>5）项目交付成果（包括但不限于）：</p>
--	---

采购包5：《2025年度信息系统密码安全性评估项目方案》

供应商报价不允许超过标的金额《2025年度信息系统密码安全性评估项目报告》

（招单价的）供应商报价不允许超过标的单价《信息系统密码安全建设整改建议》

标的名称：服务

参数性质	序号	技术参数与性能指标
		<p>一、建设背景</p> <p>陕西省公安机关执法办案综合管理平台建设项目应按照《关于分批次组织开展全国执法办案数据治理和汇聚上报工作的通知》、《公安机关接报案与立案工作规定》、《公安机关执法细则》等相关工作规定，全面整合执法办案和监督管理数据资源，规范相关业务标准，联通部省数据汇聚渠道，加强执法大数据智能应用服务，为下一步部平台数据反哺、数据应用提供有力数据支撑。调整完善执法办案业务流程，拓展执法监督业务，建设全省统一管理执法办案管理中心应用，助推我省法治公安建设质量变革、效率变革、动力变革。</p> <p>二、测评目标</p> <p>陕西省公安机关执法办案综合管理平台建设项目主要是在现有医保信息平台的基础上，对公安部门数据协同标准和规范进行设计，并满足信创要求，构建具有陕西特色的政法一体化协同办案体系。需按要求完成对系统核心业务系统的软件测评服务，并出具经权威机构认可的《软件测评报告》，协助用户单位进行问题整改，整改后进行复测评工作。</p> <p>本次软件测评的目标是对项目应用系统的功能和性能进行全面、客观、准确的评估，确保系统的稳定性和可靠性，满足用户需求和业务发展要求。</p> <p>三、测评要求</p> <p>1. 测评单位开展软件测评，需确保测评结果的客观性和准确性。</p> <p>2. 测评单位应具备相关领域的丰富经验和专业团队，能够全面、深入地了解系统需求和业务场景。</p>

3. 测评单位应遵循相关标准和规范，采用科学、合理的测评方法和工具，确保测评结果的可信度和可重复性。
4. 测评单位应与委托方建立有效的沟通机制，及时反馈测评进展和结果，协助委托方完成相关的整改和优化工作。

四、项目具体要求

1.政法协同办案系统功能测试要求

模块	子模块	测试点要求
		<p>(1) 逮捕</p> <p>1.公安发起逮捕：刑事案件办理过程中，到一定环节时，可以向检察院发送《提请批准逮捕书》，公安机关可以收到检察院的审查决定；</p> <p>2.检察院逮捕决定：公安机关可以收到相关逮捕决定数据，如不需逮捕的可以向检察院发送不逮捕理由；</p> <p>3.公安机关可以对自己发出的提请逮捕进行撤回，检察院对撤回申请进行审查，公安机关可以收到相应的审查结果；</p> <p>4.公安机关可以收到法院或检察院对嫌疑人的逮捕通知，公安执行后可向法院或检察院反馈执行结果。</p>
		<p>(2)不捕异议</p> <p>1.公安机关提起复议/复核：公安局可向同级或上一级检察院提出复议/复核申请，含相应意见书。</p> <p>2.检察院复议/复核审查：公安机关可以收到检察院复议/复核结果。</p> <p>3.不捕复议/复核执行：公安机关可以开具相应的文书，如《逮捕证》或释放、变更强制措施的相关文书，并将相关数据发送至检察院。</p>
		<p>(3)变更强制措施</p> <p>1.检察院/法院决定变更强制措施：公安机关可以收到检察院或法院作出变更强制措施的决定。公安机关可以将执行结果反馈给检察院或法院。</p> <p>2.公安机关决定变更强制措施：公安机关可开具相关文书，并将相关数据一并发送给检察院。</p>
		<p>(4)延长侦查羁押期限</p> <p>公安机关可向检察院发送延长羁押申请，包括相关文书。</p> <p>公安机关可收到检察院作出的决定。</p>
		<p>(5)移送审查起诉</p> <p>公安机关可以将案件信息及《起诉意见书》等材料移送给检察院。</p> <p>若需补充侦查的，公安机关可以收到检察院发来的退回补充侦查决定，并支持补充材料后重新提交《补充侦查报告书》给检察院。</p> <p>公安机关可以收到检察院是否起诉决定。</p> <p>公安机关可对已移送的案件向检察院发起撤回申请。针对撤回申请，公安机关可以收到检察院作出的相应决定。</p>

政法协同	政法协同业务流程	(6)不诉异议 公安机关可向同级人民检察院提出复议申请开具《要求复议意见书》等文书，文书开具后自动触发相应的协同流程，接收到检察机关做出的审查决定后自动变更人员处理节点。
		(7)审理期间交互 公安机关可以接收法院通知侦查人员出庭材料。
		(8)交付监所执行 1.公安机关可接收法院推送的执行材料，可向法院反馈相应的执行结果。 2.公安机关可接收法院单处剥夺政治权利送达执行材料，可通知办案人员进行处理。 3.公安机关可接收监狱送刑满释放人员尚有附加剥夺政治权利法律文书材料，可通知办案人员处理。
		(9)暂予监外执行 1.公安机关可接收法院暂予监外执行决定。 2.公安机关可接受检察院提出的书面检查意见，及是否监外执行决定，同时公安机关可接收监狱管理局做出的是否暂予监外执行决定。
		(10)社区矫正调查评估 公安机关可向司法行政机关发起委托调查评估协同，协调中含委托调查函、评估意见。
		(11)交付社矫执行 公安机关可将罪犯监外执行的信息推送给社区矫正机构。 公安机关可接收、看守所、法院、监狱与社区矫正机构的执行材料，并向对方发送执行结果。 公安机关可接收社区矫正机构发送的补齐信息，补齐材料后可推送给社区矫正机构。 公安机关可接收社区矫正机构发送的送达回执，公安机关可推送《社区矫正对象基本信息表》给对方。 公安机关可接收社区矫正机构发送的漏管信息，并反馈社区矫正机构。
		(12)解除和终止——解除矫正 公安机关发可接收社区矫正机构发送的解除矫正通知和暂予监外执行刑期届满通知。
		（13）法律援助 公安机关可向司法行政机关发送法律援助或变更律师的申请，并推送相关材料。 公安机关可接收司法行政机关发送的指派法援律师或进行律师变更通知。 公安机关可向司法行政机关发起终止法律援助申请。

				<p>(14) 变更羁押期限</p> <p>公安机关可向看守所申请变更羁押期限，并推送相关文书材料。</p>
				<p>(15)补充材料</p> <p>公安机关可接收检察院、法院的补充材料通知，并可将相关材料补充完整并推送给检察院、法院。</p>
				<p>(16)网上电子换押</p> <p>移送、二审阶段，公安机关可通过开具一定文书的操作，手动/自动向检察院/法院发起换押流程。</p>
			一体化协同办案桌面	<p>协同工作台：可以通过工作台快速对协同业务的发起、接收操作，并支持查看协同节点。</p> <p>有办案提醒功能，展示检察院、法院、看守所推送的预警消息、待办消息，可以通过执法办案系统将消息推送给相应的处理人。</p> <p>系统有协同流程标准管理功能，可通过流程标准能配置XML文件，配置流程节点信息。</p> <p>系统提供协同数据统计功能，可查看各单位和各人员的业务协同交互次数，或者以协同角度统计各单位交互次数。</p> <p>系统有协同交互跟踪功能，通过协同交互跟踪能查看与检察院、法院的业务交互状态，如推送成功，接收失败、推送中。</p> <p>法制民警可接收检察院、法院回传的文书或材料或者发起相应的协同业务流程。</p>
			协同音视频	<p>系统可存储各地市音视频的结构化数据，协同推送时数据中包含下载地址。</p>
			协同对接	<p>(1) 机构用户同步接口</p> <p>业务系统调用。用户的机构有新增、更新、删除的，可以进行同步。</p> <p>(2) 单点认证接口</p> <p>业务系统调用。登录时认证授权。获取的apigwToken有效期默认30分钟，支持可配。</p> <p>第三方调用接口或页面跳转时，需要进行登录认证获得apigwToken。apigwToken的值会在接口返回的data参数中携带。</p> <p>(3) 流程发起处理、退回接口</p> <p>业务系统发起、处理或退回协同流程时，触发此接口，发送案件信息，嫌疑人以及文书数据，可返回协调成功或失败。</p> <p>(4) 流程数据同步接口</p> <p>业务系统调用协同平台数据，包括流程数据，基本案件信息和嫌疑人数据。</p> <p>(5) 消息通知接口</p> <p>业务系统发出的流程到达目标单位后，协同平台向发送方推送送达回执信息。业务系统可以根据消息通知接口变更当前协调所在节点。</p>

					<p>（6）消息接收接口</p> <p>业务系统在进行相关的签收或立案处理后通过该接口通知协同平台。</p>
					<p>（7）文件上传接口（可批量）</p> <p>由业务系统调用“跨部门大数据办案平台”，以文件的形式上传文件，返回文件地址。</p>
					支持110接警平台警情同步至执法系统，且数据准确；
					系统内支持本地接报警登记；
					系统内的警情支持多种字段的组合查询，且查询结果准确；
					警情支持删除操作，删除的警情在系统库中留痕
					警情列表页面支持导出操作，且导出数据准确；
					警情办理为案件后，案件信息与警情相关联，且关联关系显示正确；
					警情总台有人员管理、物品管理、文书管理、笔录管理和证据管理模块，支持人员、物品、文书、笔录的增/删/改/查操作；
					必要时民警可以通过流程，提交审批，审批通过后，对警情进行指派操作，如无必要，流程可省略；
					接收民警，可针对指派过来的警情继续办理；
					系统支持对个人或单位进行当场处罚
					警情处理为当场处罚类案件时，选择的案由均为当场处罚类案由；
					可开具《当场处罚决定书》，可正常展示填写页面、预览核对页面；
					文书内包含处罚时间、签名、意见签名、核对人签名等；
					文书可以正常保存、开具；
					开具后的文书支持线上查看。
					针对支持快办的案由案件，可以进行快速办理；
					需要快速办理的案件，由民警发起审批流程，领导审批通过后，案件转为快速办理案件，系统有相应标记；
					办案单位领导可直接标记案件为快速办理案件；
					针对快速办理的案件可以开具快速办理类文书，并支持查看。

			案件办理	行政案件	<p>1、民警将警情处理为行政案件，处理过程中需要领导审核审批，领导可对其进行同意或退回。</p> <p>2、已转换为行政案件的，系统支持查询功能</p> <p>3、对案件办理过程需要的业务，有审核审批流程，如：行政立案、移送、回避决定、办案人变更等</p> <p>2、针对行政案件，支持对人员的笔录制作功能，对案件材料电子化组卷功能</p> <p>4、民警在办案过程中可开具相关文书，开具过程中支持预览核对：核验内容以及功能。开具部分文书，案件的状态可以改变</p> <p>5、系统有预警功能，可通过预警模型的配置，实现相应的预警提醒功能。</p> <p>6、对行政案件办理过程中的信息及相关数据，支持查询操作。对应处以行政处罚的，可开具相关处罚决定，对无需处罚的可作出不予行政处罚决定。</p> <p>7、可对行政案件申请听证。</p> <p>8、可对发起的部分流程申请撤回操作</p>
				刑事案件	<p>1、民警将警情处理为刑事案件，处理过程中需要领导审核审批，领导可对其进行同意或退回。</p> <p>2、已转换为刑事案件的，系统支持查询功能</p> <p>3、系统针对经侦类案件可进行单独管理，支持相关信息查询</p> <p>4、对于受理为刑事案件的，可做出立案或不予立案决定，并支持在刑事案件台账页面的查询、查看</p> <p>5、案件办理过程，依照相关规定，记录相关日志信息，并支持查看</p> <p>6、在刑事案件总台，支持开具刑事案件相关文书，需要提交审批的文书，会对应有相关流程，对应的角色可对流程进行审核、审批，做出同意或退回处理。</p> <p>7、系统针对刑事案件，提供撤销案件、转行政类案件、侦查终结、移送起诉刑事和解等业务发起/功能操作</p> <p>8、对于刑事案件，支持司法监督业务流程，即立案监督协同；</p> <p>9、系统支持多种类型人员录入（涉案人员、证人、受害人），支持不同种类的物品录入</p> <p>10、针对刑事案件，支持对人员的笔录制作功能，对案件相关的文书开具功能，对案件材料电子化组卷功能</p> <p>11、可对发起的部分流程申请撤回操作</p>
				刑事复议复核	<p>1、法制民警可以在刑事复议复核模块查询需要复议的刑事案件；</p> <p>2、法制民警可以呈请复议相关文书，由上级公安机关进行审批</p> <p>3、向上级公安机关复核时，可以开具相关复核文书并自动加盖电子签章</p>

行政复议	1、民警可以登记提交至复议局的复议案件信息 2、登记复议案件信息后，可以跟踪复议情况 3、行政复议案件中可以制作《行政复议答复书》等文书材料
国家赔偿	1、民警可以登记国家赔偿案件、刑事国家赔偿案件 2、民警可以开具相应文书并自动加盖电子签章
知识详情服务对接	1.系统按公安部标准接入知识详情服务，功能展示合理
智能帮助服务对接	1.系统按公安部标准接入智能帮助服务，功能展示合理
智能搜索服务	1.系统按公安部标准接入智能搜索服务，功能展示合理
三个规定直报	1.刑事案件办理的特定环节正常调用三个规定页面服务 2.可以集成公安部提供的三个规定页面 3.办案民警、审核民警、审批领导等角色可以在办案环节触发三个规定直报 4.可以正常填写直报内容，三个规定可以会自动将数据上报至公安部
送押送拘	1：系统可对嫌疑人发起送押送拘； 2：选择对应拘留所、看守所、戒毒所，进入对应的填写页面，关联文书时能关联对应的已开具文书。针对填报信息支持查看； 4：在送押送拘列表，点击上传体检信息能上传体检信息，点击同步人员照片能上传人员照片，点击流程轨迹能查看流程轨迹； 5：公安机关可接收监管综合管理信息平台的相关信息，并对相关信息作出反馈。
远程提讯	1、公安能够针对某案件中嫌疑人发起远程提讯，系统会自动记录发起时间、发起人信息。 2、在远程办案列表管理页面展示发起的远程提讯预约记录，可以查询和数据导出 3、远程提讯发起预约成功后，可以调用笔录客户端对嫌疑人制作远程提讯笔录 4、笔录制作并签名完成后，信息可回传至执法系统，并与案件绑定。 。
印章管理	电子签章系统，覆盖印章申请、印章制作、印章注册、印章管理、授权管理、验证管理、查询统计、日志管理、系统管理等功能
	系统支持文档印章、密钥盘信息、印章信息查看、印章管理配置等功能

法综数据上报	<p>1.可以依照法综数据上报要求将法综专题库数据通过法综数据上报通道</p> <p>2.可以完成人员、组织、物品、文书、笔录、卷宗、案件业务以及中心业务等多个方面数据的上报工作</p> <p>3.相关人员、单位、物品、法律文书、笔录记录、卷宗信息、案件详情及中心业务等详尽内容正常涵盖</p> <p>4.上报数据正确并且准确</p>
移动执法	<p>1：能对人员进行笔录的制作，可以选择不同的类型和模版，制作完成后能在我的笔录中查看到笔录信息；</p> <p>2：可开具治安调解类文书，并支持查看；</p> <p>3.可在待审批中查看所有待审批数据，可对警情、案件、人员等相关审核流程进行审核审批，并支持记录的查看；</p> <p>4.APP有消息提醒功能，可通过消息提醒直接进入业务办理页面</p>
案卷管理	<p>系统对实体案卷进行台账管理，记录存放位置、存（取）时间、流转记录、卷宗所属单位、主办民警等信息；</p> <p>系统支持扫描存取功能、打印二维码功能；</p> <p>流转记录中包含上交实体案卷、签入实体案卷、签出实体案卷的时间、操作人等信息</p>

		执法办案管理中心	涉案财物管理	<p>1.支持对物品进行入库操作，入库时需要填写部分相关信息，如：存放位置、物品来源等。</p> <p>2.支持款项入账，并支持银行存单的拍照上传；</p> <p>3.支持物品需要移交到其他办案单位时可对物品进行拆分，然后再移交出库；</p> <p>4.支持物品远程示证，打开智能示证-视频示证-视频示证申请，选择需要视频示证的物品，输入示证时间、说明，提交之后，单位物品管理员收到视频示证审批任务，物品保管单位的物证管理员打开视频示证审批页面，进行审批，审批通过之后，办案民警收到待视频示证清单页面生成示证清单，物证管理员在示证时间内进行示证；</p> <p>5.支持对物品进行盘库操作，核对物品信息匹配情况进行核对；</p> <p>6.针对未及时入库的、案结物品仍在库、取保候审金1年以上未退还等异常场景的，系统有预警功能，且可通过预警信息进行快捷处理。</p> <p>7.保证金管理：开具行政或刑事收取保证金通知后系统自动生成保证金数据，也可以选择文书后手动添加；收取保证金时，需要台账信息录入，包含选择账户、填写票据号、选择缴纳时间、填写确认人（默认当前登录人）、上传票据照片。保证金处理需要台账管理，包含处理方式（退还、没收）、填写金额（必须为数字），选择处理时间。收取保证金账号和银行支持配置。</p> <p>8.系统支持罚没款的管理，开具处罚决定书、没收保证金执行通知书后系统自动生成罚没款数据；选择相关的文书手动添加。缴款信息提供台账管理，包含账户、填写票据号、选择缴纳时间、填写确认人（默认当前登录人）、上传票据照片等信息。系统提供银行账号和银行配置管理功能。</p> <p>9.支持对物品出入库查询操作；民警在物品出入库页面，对物品出入库信息进行查询；民警在在库管理页面对物品进行出库，调用出库后，在待入库涉案财物页面中显示本次调用出库的物品，筛选调用出库物品查看，待调用物品送回后，可以再次进行入库；民警在物品出入库页面，对需要移交的物品进行出库，填写出库原因移交，选择接收单位，填写出库详细原因，点击出库即可；</p> <p>10.支持物证室管理：登记管理中心后，录入物证室，填写物证室编号、物证室名称、物证室位置、具体地址、备注信息。</p> <p>11.共管：民警可通过执法系统对物品移送共管中心对物品进行统一管理。公安机关可以在系统内看到物品的签收、入库状态。可以看到物品的存放位置等信息，并支持修改。支持民警发起出库和调用申请。对已出库、临时出库的物品可查看其流程轨迹信息。</p>

办案区管理	<p>1.系统支持办案中心的管理，包括新增、删除、修改、关联登操作。</p> <p>2.针对违法犯罪嫌疑人，可以实现信息登记、人身健康检查、一体化采集、吸毒检测信息管理、吸毒样品登记、嫌疑人酒精检测信息管、随身物品管理、活动轨迹管理、嫌疑人饮食休息管理、嫌疑人候问信息管理、嫌疑人讯询问信息管理、嫌疑人辨认信息管理、嫌疑人会见信息管理、远程办案信息管理等业务功能。</p>
办案区场所数据汇聚	人员在办案区内活动信息符合公安部提供的法综数据要求，涉及环节包含人员入区、安全检查登记、随身物品登记、信息采集、临时人员登记、人员出区、临时出区审批、人员出区等
音视频数据汇聚	针对办案区内的音视频资料，执法平台可存储相关非结构化数据，包含文件名称、文件类型、文件播放、下载地址、文件拍摄时间、上传单位等
音视频管理	执法平台可对音视频管理平台的集中管理，管理平台分为平台节点管理、接口服务管理、采集站管理、执法记录仪管理、摄像头管理、存储管理、视音频文件管理、文件关联、统计分析等模块。
笔录服务器管理	<p>1、笔录客户端可以配系统名称、服务器地址、服务器端口</p> <p>2、配置正确后输入正确的账号密码可以实现系统登录</p>
笔录客户端管理	<p>1、在笔录系统-配置管理-版本管理中可以新增、修改、删除客户端版本</p> <p>2、设置最新版本后，双击打开笔录客户端图标时会自动检测版本并自动进行升级</p> <p>3、在笔录客户端“设置”界面，支持配置更新模式：自动、提醒、手动</p> <p>4、在笔录客户端“关于”界面，支持检测更新</p>
笔录方案模版管理	<p>1、在笔录系统-方案管理中可以对笔录方案进行新增、修改、删除、查询操作</p> <p>2、笔录方案模板中设置笔录类型、适用案件类型、适用案由、适用人员后，在客户端制作笔录时会根据设置的范围出现对应的笔录方案模板</p>
权利义务告知书	<p>1、在笔录系统-配置管理中可以对权利义务告知书进行新增、修改、删除、查看操作</p> <p>2、权利义务告知书中设置使用人员类型、适用案件类型、是否通用后，在客户端制作笔录时会根据设置的范围出现对应的权利义务告知书</p>
法律法规	<p>1、在笔录系统-配置管理中对法律法规进行新增、修改、删除、查看操作</p> <p>2、在客户端制作笔录时可供民警查阅并使用法律法规</p>

智能笔录

笔录组件配置	<ol style="list-style-type: none"> 1.用户在系统配置中配置组件，笔录客户端可同步笔录系统配置的内容。 2.配置不同办案区的组件配置，笔录客户端会根据登陆用户的单位，正确同步到对应办案区的配置项。
笔录资源配置	<ol style="list-style-type: none"> 1.在资源配置界面中进行新增、编辑、检索、删除操作 2.用户可以选择对应的资源类型进行上传资源包，填写资源描述。
笔录照片库	<ol style="list-style-type: none"> 1.笔录照片库支持同步到本地； 2.已同步照片库内的照片，支持调用及查看功能； 3.照片有对应的人物描述，年龄、性别、长相特征等；
远程提审	<ol style="list-style-type: none"> 1.新增、编辑、检索、删除功能可以正常使用。 2.可以正常配置远程提审终端、远程提审客户端、远程提审摄像头、远程审讯室。 3.配置完成后可以使用远程提审功能。 4.远程提审完成后，有提审记录。
笔录管理	<ol style="list-style-type: none"> 1、在笔录管理界面支持对笔录进行新增操作 2、在笔录管理界面支持对笔录进行查询操作 3、系统支持查看笔录对应的操作日志；
笔录人员管理	<ol style="list-style-type: none"> 1.在系统中可以对警情、案件中的人员制作笔录 2.制作的笔录支持查看
笔录制作	<ol style="list-style-type: none"> 1、笔录客户端笔录制作可选择不同类型的笔录模板，例如：询问笔录、讯问笔录、盘问笔录、辨认笔录、通用笔录、听证笔录 2、笔录制作时，可对笔录进行：保存、上传、预览、法律法规、权利义务告知书、备份还原、投屏、语音朗读、加载笔录方案、导入方案模板操作 3、笔录制作时，可修改笔录文本大小、是否有下划线、分色显示 4、笔录保存后，点击上传，可以进行笔录的推送以及签字捺印 5、制作时保存和上传的笔录可在“我的笔录”界面进行“编辑”、“删除”、“预览”、“绑定案件”、“设置密码”等操作 6、支持查看当前用户制作的所有笔录 7、支持离线制作笔录
材料导入	<p>系统支持纸质材料拍照、扫描后上传到执法系统；</p> <p>在系统内开具的文书、制作的笔录等数据，可上传至材料内</p>
卷宗配置	<ol style="list-style-type: none"> 1.材料配置：用户可以把执法办案相关的文书配置到电子卷宗中，案件总台-材料管理中的材料就会与执法办案的文书进行同步，民警也可以进行本地上传与扫描仪上传配置好的材料。 2.材料显示配置：用户在对材料进行上传时，材料的显示项进行配置。 3.卷宗配置：系统支持对分卷进行增、删、改、查操作，可以配置推送的组卷目录。可以针对协同的文书，单独配置展示顺序。

智能电子卷宗		<p>4.卷宗绑定材料配置：用户可以对分卷进行绑定材料。</p> <p>5.材料页码配置：用户可以在这里对文书进行拆分，可以从多联的文书中拆分需要组卷的部分命名为拆分后的材料名称。材料管理与执法办案文书进行同步时，就会仅仅同步多联的文书中拆分出来的部分到材料管理界面中来参与组卷。</p>
	自动组卷	用户可以选择在卷宗配置中配置好的分卷，对选中分卷下的所有的材料进行自动组卷，自动组卷时先进行卷宗封面编辑，再显示案件下的所有人员可以勾选人员。音视频材料可以参与组卷，卷宗中可以查看音视频材料
	人工组卷	用户可以选择在卷宗配置中配置好的分卷，然后在编辑封面，进入人员选择界面。最后进入分卷编辑界面，民警可以编辑选中分卷下的材料，选择分卷下的部分材料参与组卷，音视频材料可以参与组卷，卷宗中可以查看音视频材料。
	卷宗封面	<p>1.用户可以编辑卷宗名称、立卷时间、立卷单位、立卷人。</p> <p>2.可以编辑案件相关的嫌疑人</p> <p>3.选中分卷，可以对分卷下的材料进行添加与移除</p>
	电子书签	在卷宗预览时，用户可以对卷宗内的某一页进行收藏。在书签列表，可以查看所有的书签，可以跳转、删除。
	电子标记	在卷宗预览时，用户可以对卷宗内的某一段进行添加手记。在手记列表，可以查看所有的手记，可以跳转、删除。
	电子批注	在卷宗预览时，用户可以对卷宗内的某一段进行添加批注。在批注列表，可以查看所有的批注，可以跳转、删除。
	阅卷日志	民警可以查看卷宗的操作日志
	智能阅卷	<p>系统提供智能阅卷功能，此功能包含：</p> <p>1、阅卷工作台：消息提醒、急办任务、统计分析</p> <p>2、分级审阅：发起阅卷、待审列表、卷宗审查、犯罪事实登记、审查结论、审查报告、阅卷记录</p> <p>3、全卷检索</p> <p>4、人证关系图谱</p> <p>5、案件办理流程管控</p> <p>6、卷宗分析：缺失证据分析、瑕疵证据分析、犯罪事实分析、人证关系分析</p> <p>7、超级检索：多维度检索、高级检索条件、检索结果展示、检索历史和保存、搜索建议和纠错</p>
	预警生成	<p>系统支持预警模型配置；</p> <p>根据已配置的预警模型，达到预警条件的，则触发预警机制，系统自动生成预警；</p> <p>生成的预警有单独的管理页面，支持查看、处理操作；</p> <p>针对不同的预警，在系统中做对应的业务操作，方可解除预警；</p> <p>预警未及时处理触发问题生成条件，问题生成。</p>

执法监督	预警闭环管理	<p>1.预警管理：查看预警的基本信息；对重点预警进行签收，一般预警无需签收；对预警操作提醒/不提醒；预警信息查询、导出、流程轨迹查看；</p> <p>2.问题管理：分为模型问题、巡查问题；不同角色对单位级，区县级，市级，省级流程有不同的操作权限；</p> <p>3.预警配置：对预警模型的基本信息进行增删改查。</p>
	执法考评管理	<p>法制可以针对所管辖的单位统一配置考评标准；</p> <p>考评标准配置包含个案考评、抽案考评；</p> <p>已配置考评标准后，法制可对个人、案件进行考评，考评结果支持查询；</p>
	执法考评情况统计分析	<p>系统可以对民警个人以及对单位的考评情况，进行排名。</p> <p>民警排名支持用户根据部门、民警、时间范围来查询民警排名情况。</p> <p>单位排名支持用户根据部门、时间范围来查询单位排名情况。</p>
	综合查询	系统可以针对警情、事件、案件、人员、物品、笔录等不同类别进行多维度查询，根据查询内容的不同，支持相应的报表展示方式。
	执法档案	对办案单位，办案民警，执法办案管理中心等对象的档案进行查询；档案包括工作情况，问题情况，执法培训三个主要内容
	执法白皮书	系统内展示执法状况白皮书，样式展示美观，展示内容清晰准确。

2.政法协同办案系统性能测试要求

1) 用户并发数要求

1.政法协同办案系统

系统支持平均登录并发要求：不小于800。

系统支持峰值登录并发要求：不小于1200。

2) 响应性能要求

1.交互类业务平均响应时间 ≤ 2 秒，峰值平均响应时间 ≤ 4 秒。

2.查询业务简单查询平均响应时间 ≤ 2 秒，峰值平均响应时间 ≤ 4 秒；复杂查询平均响应时间 ≤ 3 秒，峰值平均响应时间 ≤ 5 秒。

3) 网络带宽要求

本项目考虑到突发的峰值流量情况，实际所需开设带宽不小于1000Mbps。

4) 可用性指标要求

(1) 稳定性要求

对于本项目中的各个业务系统，要求采用高可靠的硬件配置确保平台的长期稳定运行，提供7×24小时不间断服务，系统可用性>99%，数据库需做好相应的备份和恢复策略。

(2) 可扩展性要求

本项目是全省公安行业基础性、综合性业务应用平台，对系统内部和外部的可扩展性要求非常高，除需要满足与现有业务系统的集成整合外，还要满足后续规划建设信息系统的数据交换和功能接入需要。并且，不仅要满足全省公安系统内各部门、各业务系统间的数据交换需求，还要满足公安与政法部门的数据交换需求。

(3) 可操作性要求

为使平台满足各类用户的应用需求，所有功能模块的操作终端应具有较强的可操作性。要求界面设计友好，简单易用，同时符合用户的业务操作习惯，最大限度的降低系统使用的复杂程度。

（4）安全性要求

本项目所涵盖的数据，包括公安部门的重要业务数据等，对数据的安全性要求较高，投标人需要对数据的安全和开放设计良好的安全机制。

投标人提供的方案必须在设计上保护用户身份的安全、实现功能和数据权限、身份信息的安全传递、数据的加密；对关键业务操作必须提供安全审计功能，所有子系统必须实现统一和一致的日志功能。

3.违法犯罪系统功能测试要求

模块名称	子功能	测试点
政法协同	一审公诉	用户可通过一审公诉模块接收查看一审公诉信息、反馈裁判文书回执、更新在押人员当前办案人信息、关押期限信息、当前办案单位信息
	二审上诉	用户可通过二审上诉模块接收查看二审上诉信息、反馈裁判文书回执、更新在押人员当前办案人信息、关押期限信息、当前办案单位信息
	二审抗诉	用户可通过二审抗诉模块接收查看二审抗诉信息、反馈裁判文书回执、更新在押人员当前办案人信息、关押期限信息、当前办案单位信息
	审理期间交互	用户可通过审理期间交互模块接收查看审理期间交互信息、反馈签收回执、更新在押人员当前办案人信息、关押期限信息、当前办案单位信息
	交付监所执行	1、用户可通过交付监所执行模块接收查看执行材料信息 2、用户可通过交付监所执行模块推送交付执行材料、接收监狱情况反馈
	暂予监外执行	1、用户可通过暂予监外执行模块提请暂予监外执行 2、用户可通过暂予监外执行模块结合、查看检察院反馈意见、通报情况、暂予监外执行决定、不予监外执行决定
	刑满释放	用户可通过刑满释放模块推送刑满释放信息至办案单位
	社区矫正解除矫正	用户可通过社区矫正解除矫正模块接收、查看解除矫正信息
	社区矫正提请减刑	用户可通过社区矫正提请减刑模块接收、查看提请减刑信息
	社区矫正提请撤销假释	用户可通过社区矫正提请撤销假释模块接收、查看提请撤销假释信息

纠违及检察建议	<p>1、用户可通过纠违及检察建议模块接收、查看纠违及检察建议信息；</p> <p>2、用户可通过纠违及检察建议模块推送纠违及检察建议反馈信息；</p>
变更羁押期限	<p>1、用户可通过变更羁押期限模块接收、查看变更羁押期限信息；</p> <p>2、用户可通过变更羁押期限模块推送变更羁押期限信息反馈信息；</p>
超期羁押通知	<p>1、可通过超期羁押通知模块推送超期羁押信息、即将届满信息至办案单位；</p>
监狱提审/庭审	<p>1、用户可通过监狱提审/庭审模块接收、查看监狱提审/庭审申请信息；</p> <p>2、用户可通过监狱提审/庭审模块审核监狱提审/庭审信息，并推送审核结果至办案单位；</p>
刑事申诉	<p>用户可通过刑事申诉模块推送刑事申诉信息至办案单位</p>
看守所检察监督	<p>1、可通过看守所检察监督模块推送看守所执法活动信息、看守所管理活动信息至检察院</p> <p>2、可通过看守所检察监督模块查看已推送至检察院的看守所执法活动信息、看守所管理活动信息</p>
提讯	<p>1、用户可通过提讯模块接收、查看办案单位的提讯预约信息；</p> <p>2、用户可通过提讯模块推送提讯预约审批信息至办案单位；</p>
网上电子换押	<p>1、用户可通过网上电子换押模块接收、查看办案单位的网上电子换押移送、退回信息；</p> <p>2、用户可通过网上电子换押模块推送电子换押移送、退回审核信息至办案单位；</p>
入所	<p>1、用户可通过入所流程对需收押人员信息进行录入，内容包括：人员姓名、案件类别、监室号、入所原因、入所日期等；</p> <p>2、用户可通过入所流程输入人员姓名、入所日期、入所原因对入所信息进行筛选查询，查询结果符合查询条件要求。</p>
出所	<p>1、用户可通过出所流程对需出所人员的出所信息进行录入，内容包括：人员姓名、出所原因、出所日期、出所去向等；</p> <p>2、用户可通过出所流程输入人员姓名、出所日期、出所原因对出所信息进行筛选查询，查询结果符合查询条件要求。</p>

				提押	<p>1、用户可通过提押模块对提押记录进行录入，内容包括：人员姓名、提押时间、提押原由、办案民警、办案单位等；</p> <p>2、用户可通过提押模块通过输入人员姓名、提押时间对提押记录进行筛选查询，查询结果符合查询条件要求。</p>
			收押接待	提讯	<p>1、用户可通过提讯模块对提讯记录进行录入，内容包括：人员姓名、提讯时间、提讯地点、办案民警、办案单位等；</p> <p>2、用户可通过提讯模块通过输入人员姓名、提讯时间对提讯记录进行筛选查询，查询结果符合查询条件要求。</p>
				律师会见	<p>1、用户可通过律师会见模块对律师会见记录进行录入，内容包括：人员姓名、律师会见时间、律师会见地点、会见律师、律师单位等；</p> <p>2、用户可通过律师会见模块通过输入人员姓名、律师会见时间对律师会见记录进行筛选查询，查询结果符合查询条件要求。</p>
				变更强制措施	用户可通过变更强制措施模块对需变更强制措施人员的变更强制措施信息进行录入，内容包括：人员姓名、出所原因、出所日期、出所去向等；
				异地羁押	<p>1、用户可通过异地羁押模块对异地羁押信息进行录入，内容包括：人员姓名、证件号码、原羁押监所、拟羁押监所、登记日期等；</p> <p>2、用户可通过异地羁押模块通过输入人员姓名、登记日期对异地羁押记录进行筛选查询，查询结果符合查询条件要求。</p>
				解回再审	用户可通过解回再审模块对需解回再审人员信息进行录入，内容包括：人员姓名、案件类别、监室号、入所原因、入所日期等；
				取保候审	用户可通过取保候审模块对需取保候审出所人员的取保候审信息进行录入，内容包括：人员姓名、出所原因、出所日期、出所去向等；
				谈话教育	<p>1、用户可通过谈话教育模块对谈话教育记录进行录入，内容包括：人员姓名、谈话地点、谈话时间、谈话内容、谈话民警等；</p> <p>2、用户可通过谈话教育模块通过输入人员姓名、谈话时间对谈话内容进行筛选查询，查询结果符合查询条件要求。</p>

					每日进监	<p>1、用户可通过每日进监模块对每日进监记录进行录入，内容包括：进监民警、进监时间、出监时间、进监监室等；</p> <p>2、用户可通过每日进监模块通过输入进监监室、进监时间对每日进监信息进行筛选查询，查询结果符合查询条件要求。</p>
					械具使用	<p>1、用户可通过械具使用流程对械具使用记录进行录入，内容包括：人员姓名、械具使用开始时间、械具使用结束时间、械具使用类型、械具使用原因等；</p> <p>2、用户可通过械具使用模块通过输入人员姓名、械具使用时间对械具使用信息进行筛选查询，查询结果符合查询条件要求。</p>
					禁闭管理	<p>1、用户可通过禁闭管理流程对禁闭管理记录进行录入，内容包括：人员姓名、禁闭管理开始时间、禁闭管理结束时间、禁闭管理原因等；</p> <p>2、用户可通过禁闭管理模块通过输入人员姓名、禁闭管理时间对禁闭管理信息进行筛选查询，查询结果符合查询条件要求。</p>
					单独关押	<p>1、用户可通过单独关押流程对单独关押记录进行录入，内容包括：人员姓名、单独关押开始时间、单独关押结束时间、单独关押原因等；</p> <p>2、用户可通过单独关押模块通过输入人员姓名、单独关押时间对单独关押信息进行筛选查询，查询结果符合查询条件要求。</p>
				管理教育	三固定	<p>1、用户可通过三固定模块对三固定记录进行录入，内容包括：每周三固定安排、值班安排、值日安排等；</p> <p>2、用户可通过三固定模块通过输入查询周期对三固定信息进行筛选查询，查询结果符合查询条件要求。</p>
					奖惩登记	<p>1、用户可通过奖惩登记模块对奖惩记录进行录入，内容包括：人员姓名、时间、奖惩形式、奖惩原因等；</p> <p>2、用户可通过奖惩登记模块通过输入人员姓名、时间对奖惩信息进行筛选查询，查询结果符合查询条件要求。</p>

		通讯登记	<p>1、用户可通过通讯登记模块对通讯记录进行录入，内容包括：人员姓名、通讯时间、通讯人、通讯方式等；</p> <p>2、用户可通过通讯登记模块通过输入人员姓名、时间对通讯信息进行筛选查询，查询结果符合查询条件要求。</p>
		信件收发	<p>1、用户可通过信件收发模块对信件收发进行录入，内容包括：人员姓名、信件收发时间、信件收发类型、信件收发人等；</p> <p>2、用户可通过信件收发模块通过输入人员姓名、时间对信件收发信息进行筛选查询，查询结果符合查询条件要求。</p>
		风险评估	<p>1、用户可通过风险评估模块对风险评估进行录入，内容包括：人员姓名、风险评估时间、风险评估等级、风险评估类型等；</p> <p>2、用户可通过风险评估模块通过输入人员姓名、时间对风险评估信息进行筛选查询，查询结果符合查询条件要求。</p>
		七日跟踪	<p>1、用户可通过七日跟踪模块对七日跟踪信息进行录入，内容包括：人员姓名、考核日期、考核民警、考核内容等；</p> <p>2、用户可通过七日跟踪模块通过输入人员姓名、入所日期对七日跟踪信息进行筛选查询，查询结果符合查询条件要求。</p>
		行为规范	<p>1、用户可通过行为规范模块对行为规范进行录入，内容包括：人员姓名、发现时间、考核目标、行为类别等；</p> <p>2、用户可通过行为规范模块通过输入人员姓名、时间对行为规范信息进行筛选查询，查询结果符合查询条件要求。</p>
		巡视记录	<p>1、用户可通过巡视记录模块对巡视记录进行录入，内容包括：登记日期、起始时间、截止时间、巡视民警等；</p> <p>2、用户可通过巡视记录模块通过输入巡视民警、时间对巡视记录信息进行筛选查询，查询结果符合查询条件要求。</p>

			监控巡视	监控记录	<p>1、用户可通过监控记录模块对监控记录进行录入，内容包括：值机开始时间、值机结束时间、值班人员、设备运行情况等；</p> <p>2、用户可通过监控记录模块通过输入值班民警、时间对监控记录信息进行筛选查询，查询结果符合查询条件要求。</p>
				重点人员评判	<p>1、用户可通过重点人员评判模块对重点人员评判进行录入，内容包括：人员姓名、评判时间、评判内容、评判结果等；</p> <p>2、用户可通过重点人员评判模块通过输入人员姓名、时间对重点人员评判信息进行筛选查询，查询结果符合查询条件要求。</p>
				监视对讲	<p>1、用户可通过监视对讲模块对监视对讲信息进行录入，内容包括：对讲时间、监室号、对讲民警、对讲内容等；</p> <p>2、用户可通过监视对讲模块通过输入监室号、时间对监视对讲信息进行筛选查询，查询结果符合查询条件要求。</p>
				每日点名	<p>1、用户可通过每日点名模块对每日点名信息进行录入，内容包括：点名时间、监室号、点名情况等；</p> <p>2、用户可通过每日点名模块通过输入监室号、时间对每日点名信息进行筛选查询，查询结果符合查询条件要求。</p>
				健康检查	<p>1、用户可通过健康检查模块对健康检查进行录入，内容包括：人员姓名、检查日期、健康状况、身高、体重等；</p> <p>2、用户可通过健康检查模块通过输入人员姓名、监室号对健康检查信息进行筛选查询，查询结果符合查询条件要求。</p>
				伤情登记	<p>1、用户可通过伤情登记模块对伤情登记进行录入，内容包括：人员姓名、检查人、送押民警、受伤部位、受伤情况等；</p> <p>2、用户可通过伤情登记模块通过输入人员姓名、入所日期对伤情信息进行筛选查询，查询结果符合查询条件要求。</p>

医疗卫生	危重疾病	<p>1、用户可通过危重疾病模块对危重疾病进行录入，内容包括：人员姓名、疾病类别、疾病名称、登记日期、登记人员等；</p> <p>2、用户可通过危重疾病模块通过输入人员姓名、登记日期对危重疾病信息进行筛选查询，查询结果符合查询条件要求。</p>
	传染病情况	<p>1、用户可通过传染病情况模块对传染病情况进行录入，内容包括：人员姓名、疾病类别、疾病名称、登记日期、登记人员等；</p> <p>2、用户可通过传染病情况模块通过输入人员姓名、登记日期对传染病情况信息进行筛选查询，查询结果符合查询条件要求。</p>
	孕检管理	<p>1、用户可通过孕检管理模块对孕检信息进行录入，内容包括：人员姓名、检查日期、健康状况、妊娠检测情况等；</p> <p>2、用户可通过孕检管理模块通过输入人员姓名、监室号对孕检管理信息进行筛选查询，查询结果符合查询条件要求。</p>
	所内就医	<p>1、用户可通过所内就医模块对所内就医进行录入，内容包括：人员姓名、治疗日期、治疗医生、诊疗类别、治疗措施等；</p> <p>2、用户可通过所内就医模块通过选择监室号、人员姓名对所内就医信息进行筛选查询，查询结果符合查询条件要求。</p>
	所外就医	<p>1、用户可通过所外就医模块对所外就医进行录入，内容包括：人员姓名、申请日期、申请医生、就医种类、申请就医时间等；</p> <p>2、用户可通过所外就医模块通过输入人员姓名、申请日期对所外就医信息进行筛选查询，查询结果符合查询条件要求。</p>
	跟踪观察	<p>1、用户可通过跟踪观察模块对跟踪观察情况进行录入，内容包括：人员姓名、监室号、医生、护士、特殊情况记录及处理情况等；</p> <p>2、用户可通过跟踪观察模块通过输入检查日期对跟踪观察信息进行筛选查询，查询结果符合查询条件要求。</p>
	提讯预约审批	用户可通过提讯预约审批模块对提讯预约信息进行审批，内容包括：审批人、审批意见、审批时间。
	提押预约审批	用户可通过提押预约审批模块对提押预约信息进行审批，内容包括：审批人、审批意见、审批时间。

		所领导	械具审批	用户可通过械具审批模块对械具使用信息进行审批，内容包括：审批人、审批意见、审批时间。
			禁闭审批	用户可通过禁闭审批模块对禁闭信息进行审批，内容包括：审批人、审批意见、审批时间。
			单独关押审批	用户可通过单独关押审批模块对单独关押信息进行审批，内容包括：审批人、审批意见、审批时间。
			重点人员审批	用户可通过重点人员审批模块对重点人员信息进行审批，内容包括：审批人、审批意见、审批时间。
			入所审批	用户可通过入所审批模块对需入所人员进行审批，内容包括：审批人、审批意见、审批时间。
			出所审批	用户可通过出所审批模块对需出所人员进行审批，内容包括：审批人、审批意见、审批时间。
			变更强制措施审批	用户可通过变更强制措施审批模块对变更强制措施信息进行审批，内容包括：审批人、审批意见、审批时间。
		分析研判	综合查询	用户可通过综合查询模块，通过输入人员姓名、证件号码、监室号等条件对人员信息进行筛选查询，查询结果符合查询条件要求。
			月报表	用户可通过月报表模块，通过输入统计日期条件对月报表信息进行筛选查询，查询结果符合查询条件要求。
			预警信息	用户可通过预警信息模块，通过输入日期条件对预警信息进行筛选查询，查询结果符合查询条件要求。
			风险预警评估模型	用户可通过风险预警评估模型查看风险预警信息，内容包括：风险人员分析、风险监室分析、风险监所分析。
			法治规范监督	用户可通过法治规范监督查看各监督信息，内容包括：收押入所流程闭环监督、羁押期限预警监督、提讯流程规范监督、提解流程规范监督、出所流程规范监督、械具使用流程规范监督、管教谈话监督、医疗卫生工作监督
4.违法犯罪系统性能测试要求 对系统的性能进行测试和评估，包括但不限于以下方面： 系统响应时间：测试系统在不同负载下的响应时间，包括空闲状态和高峰期的响应时。 1.交互类业务 是指日常工作中在系统进行的业务处理，如录入，修改或删除一条记录、发布一条信息等操作。平均响应时间≤2秒，峰值平均响应时间≤4秒。				

采购包6：2.查询业务简单查询平均响应时间 ≤ 2 秒，峰值平均响应时间 ≤ 4 秒；复杂查询平均响应时间 ≤ 3 秒，峰值响应时间 ≤ 5 秒。

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

3.系统支持峰值登录并发要求：不小于200。

参数性质	序号	技术参数与性能指标
		<p style="text-align: center;">(一)软件平台部分</p> <p>一、建设背景</p> <p>本次项目建设应按照《关于分批次组织开展全国执法办案数据治理和汇聚上报工作的通知》、《公安机关接报案与立案工作规定》、《公安机关执法细则》等相关工作规定，全面整合执法办案和监督管理数据资源，规范相关业务标准，联通部省数据汇聚渠道，加强执法大数据智能应用服务，为下一步部平台数据反哺、数据应用提供有力数据支撑。调整完善执法办案业务流程，拓展执法监督业务，建设全省统一管理执法办案管理中心应用，助推我省法治公安建设质量变革、效率变革、动力变革。</p> <p>二、建设内容</p> <p>本项目需第三方监理机构进行监管，负责对项目的实施进行监督和检查，确保项目按照合同要求进行。</p> <p>三、服务内容</p> <p>新建政法协同办案系统和升级改造违法犯罪人员信息系统，国产操作系统、国产数据库和中间件，数据治理与数据共享。</p> <p>针对以上内容提供监理服务。</p> <p>四、服务要求</p> <p>1.监理服务范围</p> <p>依据《信息技术服务监理》规范，对项目提供全过程周期监理服务，包括质量控制、进度控制、投资控制、变更控制、风险控制、合同管理、信息管理、数据保密管理、安全管理、知识产权管理和组织协调。</p> <p>为项目建设提供项目技术方案的咨询；协助审核有关合同、协议；进行有关技术文档等文件的管理；对项目建设内容进行全过程周期咨询监理；定期向建设单位汇报项目进展情况，提交项目监理服务报告；代表建设单位协调与承建单位的工作关系和协调解决项目建设过程中的各类纠纷，确保本项目按期、保质、顺利地完成。</p> <p>2.监理服务目标</p> <p>监理服务工程的整体目标是：对本项目建设进行全过程的监督和管理，依照有关标准规范和法律法规以及建设单位的需求，本着科学、公正、严格、守信、守纪、守法的原则，以高度的责任心、丰富的项目管理和专业技术经验，对该项目实施全面的、有重点的、精线条的监督管理，包括受建设单位委托负责审核项目建设合同条款、控制项目进度和成本核算，按期分段参与项目验收，以确保该项目顺利进行，保证项目按期、保质地完成并交付，最终提交建设单位满意的效果。</p> <p>依据国家相关的法律法规、标准规范、项目磋商文件和项目合同书，保证项目建设符合国内国际相关的行业技术规范标准，满足项目建设磋商文件的要求，防止项目建设工作的随意性和盲目性，保证工程的总体进度和质量要求，保证工程规范化、科学化和经济性；促进建设单位、各承建单位的有效沟通，使各承建单位全面准确了解项目建设的实际需求，并使建设单位及时了解项目的进展情况；保证项目运行的全过程有一套明确、合理、可行的计划或规程，以及与之相应的审核、监理机制和手段；保证工程的关键技术指标在项目实施过程中处于受控状态，预测和发现可能影响施工计划的各种因素，及时纠正影响工程质量的缺陷，实时控制工程计量与付款。</p> <p>2.1质量控制目标</p> <p>2.1.1符合国家相关技术标准和规范要求。</p>

2.1.2符合本项目监理委托合同书要求。

2.1.3符合项目建设内容要求的建设原则和建设要求。

2.1.4项目建设质量满足建设单位、使用单位对项目建设内容、系统功能、系统性能及系统安全的要求。

2.1.5符合国家、省有关信息系统系统建设的相关文件要求。

2.1.6符合项目合同书、设计文件、建设单位案、质量标准的质量要求。

2.1.7工程质量符合磋商文件的要求及成交单位响应文件的承诺。

2.2进度控制目标

保证项目在合同书约定的工期内完成，使系统按照本项目建设的总体规划按期投入运行和使用，并顺利通过最终验收。

2.3投资控制目标

以本项目建设合同文件为依据，以合同总金额为投资控制目标，保证项目投资金额在相关法律、政策规范要求的范围内，保证项目投资的有效性。

2.4信息安全控制目标

信息安全符合GB 17859-1999《计算机信息系统安全保护等级划分准则》、《信息安全技术网络安全等级保护基本要求》GBT 22239-2019等与信息安全有关标准的要求，及国家的相关标准和要求。项目建设符合密码应用安全性评估要求；满足平台的安全要求，满足合同要求和用户使用需求。

检查、督促承建单位建立健全项目建设安全管理体系，经常检查现场安全技术措施的实施情况和安全设施的配备情况，及时发现施工中不安全因素，把安全隐患消灭在萌芽状态，促进安全目标的实现，杜绝安全生产事故的发生。

2.5知识产权保护控制目标

符合国家相关知识产权保护规定和法律。同时保证建设单位、承建单位、监理方和设备/软件原厂商各方资料和产品的知识产权不受侵害。

2.6信息文档管理目标

保证本项目建设过程中的所有文档，包括施工方案文档、建设单位方案文档、软件开发文档、系统安装部署文档、调试文档、配置文档、运行维护文档、竣工文档、会议纪要、变更文件和其他往来文件，分门别类，妥善保管，科学调用，并具有完整性和可读性。

2.7合同管理目标

以合同规定的工期和费用为依据，监督建设单位和承建单位的履约情况，确保合同的顺利执行。通过监理工作，有力地协调保障建设单位与承建单位进行良好的合作，加强对本项目工程质量、进度和成本的控制和管理，更有效地进行合同管理和项目文档管理，同时弥补建设单位在技术、工程管理经验及掌握市场信息等方面的不足，使本项目建设达到国家相关行业规范和标准要求，以及项目合同规定的质量目标、进度目标和投资目标。

2.8组织协调目标

认真履行建设单位、承建单位、使用单位等各方关系，通过例会、报告等制度，通过各种监理方法使本项目顺利、高效进行，保证各相关方的良好沟通和无缝衔接，保证项目相关信息传递的及时性和有效性。

2.9变更控制目标

审核项目各相关方提出的项目变更申请和建议，组织项目变更委员会讨论项目变更方案，确保项目变更的必要性、可行性、合理性、科学性，确定最优化的变更方案，并跟踪、监督变更的执行效果。

3.监理服务内容

监理服务工作内容主要包括质量控制、进度控制、投资控制、变更控制、风险控制、合同管理、信息管理、数据保密管理、安全管理、知识产权管理和组织协调。按照《陕西省省级政务信息化项目管理办法》（暂行）对项目的相关要求，配合采购人完成到货验收和档案专项验收、项目验收，并根据要求组织提供项目第三方审计报告等相关必要材料，直至项目竣工。

4. 监理服务要求

4.1 项目服务范围：本项目全过程监理服务

4.2 工作质量要求

投标人应该在投资控制、进度控制、质量控制、合同管理、文件管理、组织协调和其他工作等方面对监理工程采取必要和完善的监督、控制和管理措施，保证监理工程能够按时、按质、按量竣工。

投标人必须定时向建设单位通报工程进展情况及工程实施过程中所遇到的问题。投标人在发现工程存在问题后应于3日内向采购方提交书面情况反映文件并提出切实可行的改进意见，逾期未反映情况，导致工期延误或其他问题，投标人应承担违约责任并赔偿采购人因此产生的损失。未经采购人同意投标人不得以此为拖延工程施工进度及工程验收。

4.3 能力要求

在本项目建设过程中，投标人必须通过发挥监督、控制、协调等几方面的作用，通过信息工程监理专业化知识和技能，确保全部建设项目实现质量、进度和成本三个方面的控制目标。投标人应该具有发现问题和预警问题的能力；解决处理工程建设中的各种问题；应该是咨询建议的提供者、是项目建设过程中的推动者、是各项目承建单位的粘和剂。对能力要求概括为：

协调能力：在信息化建设项目中，建设单位和承建单位在项目实施过程中难免存在争议和冲突。要求投标人必须以公正、公平和第三方的立场，通过充分地发挥协调作用，来积极解决这些争议和冲突，促进建设单位和承建单位的良好合作，努力把全部建设项目顺利完成。

控制能力：承建单位在信息化建设项目中，对工程质量、进度、投资的控制是最重要和最关心的内容。投标人应该发挥对承建单位管理职能的再控制，通过规范和约束承建单位的项目管理机制，确保对项目工程质量、进度和成本的有效控制。

专业能力：投标人应该具有 IT 专业化能力，具备有甄别承建单位提供的整体解决方案是否满足建设要求的能力，并能提出评估报告和改进建议，提供技术层面上支持。能依靠雄厚的信息化建设经验，为建设单位提供整体方案是否满足先进性、经济性、实用性、成熟性、可靠性、安全性、可管理性和可扩展性等多方面的技术需求。

管理能力：投标人应根据合同明确建设单位和承建单位各自的责任、权利和利益，保证合同执行的公正性；工程实施过程中应该及时向建设单位通报合同变更的情况，协助保持合同、协议及其附件内容的有效性、一致性；监督合同执行情况，定期向建设单位、承建单位通报合同执行情况。投标人必须妥善管理整个项目过程中所产生的监理文档资料，要求承建单位按照规范编制相应的技术文档。

4.4 责任要求

投标人有责任为建设单位提供项目顾问咨询意见，有义务帮助承建单位实现合同所规定的目标，公正维护各方的合法权益。在本合同期内及合同终止后，未征得建设单位同意，不得泄露与本工程项目有关的资料。由于承建单位在工程实施中不符合工程规范和质量要求，投标人要监督承建单位停工整改或返工。如承建单位人员工作不力，可提出调换有关人员。如果承建单位违反合同规定的质量要求和完工时限，投标人应协助建设单位追究有关承建单位的责任。如果因投标人监督不力，造成建设单位经济损失的，投标人要向建设单位赔偿承建单位造成的损失。

投标人使用建设单位提供的设备和物品属建设单位所有，在监理工作完成或终止时，应将设备和剩余

物品在合同规定的时间和方式移交给建设单位。

4.5项目验收

投标人应对所有正式交付件的综合质量审查负责，制定各交付件的相关责任人，明确相关职责。

投标人应提交验收方案，供采购人和最终用户参考。

5.项目承诺

本项目监理工作，必须在采购人和最终用户的指定地点进行。对于在工作中获取的重要资料和结果，投标人不得带离该地点。

投标人对本磋商文件中的内容及在应标过程中接触的项目信息、数据资料等负有保密责任，不得泄露给任何第三方。无论投标人中标与否，其对上述内容的保密责任将长期存在。

(二)硬件部分

一、监理技术规格要求

1.监理基本原则

1.1监理服务应遵守的基本准则

1.1.1遵照国家《信息技术服务监理》（GB/T 19668.1）参照监理服务各阶段内的具体监理工作，以“守法、诚信、公正、科学”的准则执业，维护建设单位与承建单位的合法权益。

1.1.2执行有关项目建设的国家法律、法规、规范、标准和制度，履行监理合同规定的义务和职责；

1.1.3不得泄漏所监理项目各方认为需要保密的事项；

1.1.4遵守国家的法律和政府的有关条例、规定和办法等；

1.1.5坚持公正、公平、公开、独立地处理有关项目各方的争议；

1.1.6坚持科学的态度和实事求是的原则；

1.1.7在坚持按监理合同的规定向建设单位提供技术服务的同时，帮助承建单位完成所担负的建设任务。

1.2服务依据

设计方案

监理合同

《信息技术服务监理第1部分：总则》 GB/T19668.1- 2014

《信息技术服务监理第2部分：基础设施工程监理规范》 GB/T19668.2- 2017

《信息技术服务监理第3部分：运行维护监理规范》 GB/T19668.3- 2017

《信息技术服务监理第4部分：信息安全监理规范》 GB/T19668.4- 2017

《信息技术服务监理第5部分：软件工程监理规范》 GB/T19668.5- 2018

《信息技术服务监理第6部分：应用系统数据中心工程监理规范》 GB/T 19668.6-2019

2.监理范围

2.1监理范围

监理范围主要为陕西省公安机关执法办案综合管理平台部署环境需求项目方案的规划设计、招投标文件、建设合同及施工方案中的建设内容。

2.2监理基本内容：

A. 准备阶段

(1) 严格按照设备招标文件、承建单位的投标文件及施工合同对承建单位提供的所有设备进行验收，确认设备品目、型号、配置、数量、性能。

(2) 审核系统承建单位的集成方案，确保系统承建单位按照其投标文件所做的承诺执行集成工作。

B. 施工阶段

- (1) 审批施工方案，确认开工报告，签发开工指令。
- (2) 每天检查施工现场和施工的安全防护设施及工作情况。
- (3) 检查承建单位的施工组织、施工技术方案和进度计划，检查计划执行情况实际进度与计划进度对比分析，纠正进度计划偏离，审查有关技术合同附件，确保工程在合同规定期限内完成。
- (4) 检查承建单位的管理规范与质量控制体系是否符合要求。严格监督与管理督促承建单位按规范、设计方案及工艺标准施工，确保工程按质按量完成。
- (5) 对项目的各个分项分部及单位工程质量控制及检查验收把关，各分项、隐蔽工程自检，签发子系统检验认可书，进行质量事故分析，监督事故处理方案执行。
- (6) 当质量有问题时，分析查明原因并及时提出要求，若工程需变更，提出变更的参考意见，并督促承建单位返修返工。
- (7) 督促履行工程合同，协助调解合同有关问题，检查工程质量，督促工程进度。

C. 试运行阶段

- (1) 检查系统调试和试运行情况，做出试运行检测报告。
- (2) 对于运行系统中出现的质量问题，写出质量分析报告，督促承建单位负责解决。
- (3) 按合同要求督促完成培训工作，建立运行规章制度。

D. 验收阶段

- (1) 按项目招标文件、承建单位投标文件和合同中的技术指标做出详细的检测报告，配合对各系统进行验收测试。
- (2) 监督督促承建单位整理并提交工程相关的技术资料和提交验收的材料。
- (3) 完成工程竣工验收的准备工作，并参与工程验收，编写竣工验收评估报告。

项目建设运维期间，监理单位需要随时关注相关安全及运维管理工作进展，配合建设单位方完成对承建单位管理工作。

3. 监理工作责任

3.1 本项目的监理应该严格按照有关规定开展工作，对项目的进度、质量进行有效的控制和管理，督促、检查承建单位落实安全及质量保证措施，做好组织协调工作，为建设单位提供技术、经济和法律等方面的咨询服务，协助建设单位实现预定的合理建设目标，帮助承建单位实现合同所规定的目标、公正维护各方的合法权益。

3.2 未经建设单位同意，不得泄露任何与本工程项目有关的资料。

3.3 若承建单位在工程施工中不符合工程规范和质量要求，监理单位要监督承建单位停工整改或返工。若遇到确实需要变更设备或施工方案的情况时，在确保工程建设质量的前提下，监理单位须提出合理建议并报建设单位批准后方可执行。

3.4 承建单位违反合同规定的完工时限，监理单位需协助建设单位追究有关承建单位的责任。

3.5 由于监理单位监督不力，造成建设单位经济损失的，需扣除相应监理费（该费用协商解决）；如由于承建单位的责任造成建设单位的经济损失，监理单位必须负责配合追究承建单位，赔偿给建设单位造成的全部经济损失。

3.6 监理单位使用建设单位提供的设备和物品属建设单位所有，在监理工作完成或终止时，应将设备和剩余物品在合同规定的时间和方式移交给建设单位。

3.7 监理单位不得对监理工程进行分包或转包，否则建设单位有权终止合同，监理单位要承担由此造成的一切经济损失。

3.8 监理单位不得在工程监理期间对投标文件中已经明确的监理人员进行更换，如遇特殊情况须经建设单位同意；如现场监理人员工作不力时，建设单位有权提出更换监理人员，更换后的监理人员必须

及时到达监理现场。

4.监理工作质量要求

监理单位应该在质量控制、投资控制、进度控制、信息管理、合同管理/组织协调等几个方面对监理工程采取必要和完善的监督、控制和管理措施，保证所监理的工程能够按时、按质、按量竣工。

监理单位必须每周定期向建设单位通报工程进展情况及工程实施过程中所遇到的问题。

监理工作的质量控制目标：达到国家规定的质量评定标准。

监理工作的计划控制目标：工程工期必须在合同工期内完成。

监理工作的投资控制目标：工程总投资必须严格控制在批复概算范围以内。

5.监理人员要求

针对本项目技术含量高，施工涉及面多，实施工期长、建设内容多等特点，监理单位应成立专门项目监理工作组，该项目组由具有类似监理业绩、丰富监理经验和过硬的专业理论与实践知识的人员组成。监理组成员将严格遵循“守法、公平、公正、独立”的监理原则，对建设项目的全过程进行科学、公正、公平的质量跟踪监控、协调与处理，并以良好的职业道德，遵纪守法，以丰富的实践经验来作好本项目的监理工作。总监理工程师对本项目的实施全面负责，管理项目部的日常工作，对本项目的监理工作提供参考意见和技术咨询指导；总监代表组织信息系统监理工程师负责现场的“四控三管一协调”工作，实施现场监理。

监理人员必须全程到位，监理单位必须保证按照建设单位通知要求，能及时委派负责本项目的总监及专职监理工程师及时到位参与各项工作。同时保证，在项目承建单位进场日期开始至项目竣工验收完毕之日，有不少于*名的项目监理人员常驻施工现场，对整个项目建设全程作现场监理。

监理人员的人身安全及劳务关系等由监理单位负责。本监理项目的费用包括监理人员在采购人驻地外开展工作时的全部费用，包括因为本项目产生的差旅费用；监理人员由于项目工作需要产生的加班，值班等工作不另外计费。监理单位应充分考虑响应报价，所有监理人员一切费用均包含在项目报价中。

三、监理的工作内容及要求

本次项目监理工作需按照国家信息化工程监理的国标（GB/T 196681 《信息技术服务监理》）针对各项目分别开展信息系统工程监理，工作应按照“四控、三管、一协调”的监理基本原则进行，即对项目进度、质量、投资、变更进行控制，对项目对合同执行情况、资料编制及整理情况、施工安全进行管理，并协调建设方、供应商、业务部门等干系人，对参与的各方进行沟通协调。同时，监理单位为采购人提供项目建设全过程的技术咨询服务，对项目建设中的技术难点、问题及风险为建设单位提供全方位的解答和咨询服务

监理工作内容包括项目施工阶段、验收阶段、运维阶段和工程缺陷期的全过程监理。按照相关国家标准，监理工作包括至少以下内容及要求：

1.质量控制

1.1质量控制目标

监理单位应正确处理项目进度、费用、质量三大控制目标之间的关系，对项目实施全过程中所有影响质量的活动进行恰当有效连续监控，使影响工程质量的技术、管理和人的因素处于受控状态，预防和减少质量问题的发生，以及质量事故纠正，保证项目各个阶段、各个过程的每一项活动都符合质量要求

1.2质量控制的方法

1.2.1质量的事前控制

1）在设计方案会审前总监理工程师组织专业监理工程师熟悉设计文件，并对设计方案中存在的问题

提出书面意见，总监理工程师负责组织设计方案会审汇总或指定人员汇总。

2) 总监理工程师组织专业监理工程师审查承建单位报送的施工组织设计方案及专项方案，签认后交建设单位。

3) 监理工程师审查承建单位现场项目质量管理、技术管理和质量保证的组织机构；质量管理、技术管理制度；专职管理人员和特种作业人员的资格证、上岗证。

4) 监理工程师对工程所需原材料、半成品及设备的质量控制，对工程所用材料、半成品严格审核其出厂证明、技术合格证或质保证书。对试验材料，必须按规定进行抽检或试验，送样实行监理现场见证。所有设备在安装前必须按其技术说明书进行质量验收。

5) 监理工程师及时审查承建单位报送的工程开工报审资料并签署意见。

6) 参加由建设单位主持召开的第一次工地会议，介绍项目监理机构、人员分工；建设单位宣布对监理授权，建设单位、承建单位介绍开工前的准备情况，总监对施工准备情况的意见与要求，介绍监理规划的内容、监理程序，制定工地共同遵守的会议制度及其监理过程中各方配合协调事宜。

1.2.2 质量的事中控制

1) 施工工艺过程质量控制

按照国家规范及实际设计方案的要求，采用巡视、旁站、检测、试验等手段检查施工过程，确保施工质量。严格施工工艺的质量控制。监理工程师对施工工艺过程的各个质量控制点，施工各工序进行跟班巡视和检查，对施工重点部位、关键部位进行旁站监督施工，现场发现质量问题及时要求施工人员整改。

监理工程师将编写《监理细则》时应明确旁站监理范围。

2) 工序交接检查

坚持上道工序不经检查验收不准进行下道工序的原则，上道工序完成后，先由承建单位进行自检、专职检，认为合格后再通知现场监理工程师到现场会同检验，检验合格后签署认可方能进行下道工序。

3) 隐蔽工程检查验收

隐蔽工程完成后，先由承建单位自检、专职检，初验合格后填报隐蔽工程报验单。监理、建设单位、承建单位现场联合检验，确认合格后隐蔽。

4) 工程质量事故处理

包括质量事故原因、责任分析；质量事故处理措施的商定；批准处理工程质量事故的技术措施或方案；处理措施效果的检查。

5) 行使监理质量监督权，出现问题时下达停工指令。

6) 建立质量监理日记，现场质量监理工程师及质量检验人员应逐日记录有关工程质量动态及影响因素的情况。

7) 组织现场工程例会及专题会议

现场工程例会由总监理工程师或总监代表主持。会议将讨论质量及工程的其他事宜，解决施工遇到的各种问题。会后形成会议纪要。

8) 定期向建设单位报告有关工程质量动态情况

现场监理组每月在《监理月报》中向建设单位报告有关工程质量方面的情况。重大质量事故及其它质量方面的重大事宜则及时提出报告。

1.2.3 质量的事后控制

1) 每一检验批、分项、分部工程完成后，必须先经承建单位自行检查并进行验收，再经监理工程师复验达标并签认后，方可进行后续工程的施工。

- 2) 审核竣工资料,对工程质量进行竣工预验收。工程完工后,由承建单位提出工程验收申请,并提交全部工程技术资料,质量自评报告及与质量有关的技术文件,经监理工程师(总监)审核后,组织有关各方进行初验,对初验提出的问题,要求承建单位限期内进行整改。
- 3) 单位、单项工程竣工验收
- 初验合格后,建设单位主持竣工验收,监理协助建设单位作好竣工验收、备案工作。
- 4) 承担保修期的监理工作时,监理单位应安排监理人员对建设单位提出的工程质量缺陷进行检查和记录,对承建单位进行修复的工程质量进行验收,合格后予以签认。
- 1.3质量控制措施**
- 1.3.1质量控制的组织措施**
- 1) 明确职责分工。监理及施工均制定质量管理体系和质量保证体系并接受监督管理。
- 2) 监理单位领导定点联系制度,监理单位领导对各项目监理部定期巡视检查,解决项目部内部及施工中遇到的各项问题以提高监理能力及水平
- 3) 监理单位实行定期到监理工地进行质量检查制度,及时发现和解决存在问题,提高监理水平,加大对质量监理力度。
- 4) 督促和审查承建单位建立健全质量管理体系和质量保证体系,落实人员,完善措施和制度。
- 1.3.2质量控制的技术措施**
- 1) 材料设备供应阶段,通过实地考察、现场抽样,审查供应厂家的资质证、准销证、产品合格证等各种手段,确保材料达到设计和规范要求。
- 2) 施工阶段严格事前、事中和事后的质量控制
- (1) 事前控制:监理工程师应熟悉质量控制的技术依据,并对施工现场、施工机械、施工队伍资质、进场材料进行检查验收,审查施工组织设计和施工方案的技术可靠性和质量保证措施。
- (2) 事中控制:监理工程师在质量检查中,用观察、量测、测量、试验等手段按规范要求完成施工工艺过程的质量控制,做好工序交接和隐蔽工程检查验收,做好工程变更、质量事故的监理工作方法
- 及措施
- (3) 事后控制:检验批验收或分项验收时严格设计文件及相关标准验收,发现问题及时纠正整改,保证在上道工序合格的基础上进行下道工序施工。监理工程师要做好单位、单项及项目竣工验收,审核竣工图及其它技术文件资料,整理工程技术文件资料并编目建档。
- 1.3.3质量控制的经济措施及合同措施**
- 1) 监理工程师在质量检查和验收中,严格按合同规定的质量要求,对承建单位不符合要求的拒付工程款。
- 2) 根据施工合同,对可能的违约行为提出警告。
- 3) 按合同条款,对造成损失一方进行经济处罚。
- 2.进度控制**
- 2.1进度控制目标**
- 运用先进的项目进度控制与管理技术,对项目的设计、采购、施工、安装、调试直至投产等工作中所有影响项目建设进度的因素进行连续的、全过程的监控、测量、分析和预测,在确保项目质量及费用在受控的状态下,快速推进项目建设,保证项目优质、高效、快速建成。
- 2.2进度控制方法**
- 2.2.1进度的事前控制**
- 进度的事前控制,即为工期预控,主要工作内容有:
- 1) 审批项目实施总进度计划

监理工程师审批承建单位编制的总进度计划；

2) 审核承建单位提交的施工进度计划

审核是否符合总工期控制目标的要求；审核施工进度计划与施工方案的协调性和合理性等。

3) 审核承建单位提交的施工方案

审核保证工期，充分利用时间的技术组织措施的可行性、合理性。

4) 制定由建设单位供应材料、设备的需用量及供应时间参数，编制有关材料、设备部分的采供计划。

2.2.2进度的事中控制

1) 建立反映工程进度的监理日志

逐日如实记载每日形象部位及完成的实物工程量。同时，如实记载影响工程进度的内、外、人为和自然的各种因素。

2) 工程进度的检查

审核承建单位每月、周提交的工程进度报告，审核的要点：

- (1) 计划进度与实际进度的差异。
- (2) 形象进度、实物工程量与工作量指标完成情况的一致性。
- (3) 按合同要求，及时进行工程计量验收。
- (4) 有关进度、计量方面的签证。

进度、计量方面的签证是支付工程进度款、计算索赔、延长工期的重要依据。

(5) 工程进度的动态管理

实际进度与计划进度发生差异时，分析产生的原因，并提出进度调整的措施和方案，并相应调整施工进度计划及设计、材料设备、资金等进度计划；必要时调整工时目标。

3) 需要时组织现场协调会

4) 在监理月报中向建设单位报告有关工程进度和所采取进度控制措施的执行情况，并提出合理预防由建设单位原因导致的工期及其相关费用索赔的建议。

2.2.3进度的事后控制

当实际进度与滞后于计划进度时，专业监理工程师书面通知承建单位，在分析原因的基础上采取纠偏措施，并监督实施：

1) 制定保证总工期不突破的对策措施。

——技术上：如缩短工艺时间、减少技术间歇期、实行平行流水立体交叉作业等；

——组织上：如增加作业队数、增加工作人数、工作班次等；

——经济上：如实行包干资金、提高计件单价、资金水平等；

——其它配套措施：如改善外部配合条件、改善劳动条件、实施强有力调度等。

2) 制定总工期突破后的补救措施。

3) 调整相应的施工计划、材料设备、资金供应计划等，在新的条件下组织新的协调和平衡。

2.3进度控制措施

2.3.1进度控制的组织措施

1) 落实进度控制的责任，由总监理工程师（或总监代表）负责工程进度的整体控制，解决进度控制的重大问题，并指定一个监理工程师做进度控制的具体工作。

2) 进度监理工程师根据建设工期总目标要求，编制监理项目的控制进度和各阶段的控制工期，实行项目分解。并审查施工承建单位的单项工程施工进度计划与年、季、月的施工计划，并将结果报总监

理工程师和建设单位。

3) 建立进度监理协调制度, 建立反映工程进度状况的监理日志, 每周工程例会均进行工程进度目标实现分析, 承建单位、监理单位、建设单位负责进度人员均应到会, 每月按时将工程进度情况和进度分析意见报建设单位和采购人。

4) 总监理工程师(或总监代表)负责为工程进度款签署进度和计量方面的认证意见。

2.3.2进度控制的技术措施

1) 在施工进行阶段监理工程师应认真审核施工进度计划与施工方案的协调性和合理性, 审核施工方案能否保证工期, 保证“全天候”施工的技术组织措施的可行性、合理性, 审核施工总平面图与施工进度计划的协调性, 审核材料、设备的采、供计划的用量和时间参数。

2) 审核承建单位每月提交的工程进度报告, 检查计划进度与实际进度的差异, 当实际进度与计划进度发生差异时, 应提出调整措施和方案, 技术上采取缩短工艺时间, 减少技术间歇, 实行平行立体交叉作业, 配合相应的组织经济措施补救。

2.3.3进度控制的经济措施和合同措施

按合同要求及时协调有关各承建单位的进度, 以确保项目的形象进度要求, 确保合同工期的实现, 执行对工期提前或拖后者的奖罚制度。

2.4进度变更控制

审查进度计划

监理工程师要实际检查、审查进度计划草案, 了解项目最初的进度期望值, 把握可能出现的变更, 并分析、记录。

进度计划的实际检查

通过现场旁站、项目干系人会议、审查项目文档等获取有关项目进展方面的信息。了解项目中各项活动为什么遵守或没有遵守进度计划, 并采取预防性措施。当出现进度的严重冲突时, 监理工程师首先会同承建单位提出更改计划和措施, 报请总监理工程师审核、签字, 然后报客户单位批准。若总监理工程师或客户单位未批准, 则由监理人员协助承建单位根据返回的意见对变更计划和措施进行修改或重新制定。

2.5进度计划调整

项目进度计划调整过程是进度监测过程的后续工作过程。当工程进度出现偏差并且客户单位审核批准《信息工程建设延期审批表》后, 监理工程师启动该过程对进度计划实施调整。

3.投资控制

3.1投资控制的目标

投资控制的主要目标是在保证实现项目质量、进度的前提下, 以降低工程投资为出发点, 按照批准的投资计划, 建立有效的费用控制、跟踪、分析系统, 使项目全体工作人员提高费用控制的意识, 在项目实施的全过程中对所有影响工程费用的活动进行恰当而连续的有效控制, 将工程项目投资控制在批准的项目初步设计概算内, 为项目建成投产后能够取得良好的经济效益奠定基础。

3.2投资控制的方法

3.2.1投资事前控制

投资事前控制, 监理单位依据施工合同有关条款、施工图, 对工程项目造价对策, 目标进行工程风险预测, 并采取相应的防范性对微量, 尽量减少承建单位提出索赔的可能。

3.2.2投资事中控制

1) 按合同规定, 及时答复承建单位提出的问题及配合要求, 避免造成违约和对方索赔的条件。

2) 监理工程师应从造价、功能要求、质量、工期等方面审查工程变更方案, 并宣布工程变更实施前

与建设单位、承建单位协商确定工程变更的价款。

3) 按合同规定, 及时对已完工程量进行计量。

4) 监督承建单位按合同规定, 及时申报工程量, 监理工程师及时审批进度款, 避免延误工期违约造成索赔。

5) 定期、不定期地进行工程费用超支分析, 并提出控制工程费用突破的方案和措施。

3.2.3 投资事后控制

1) 审核承建单位提交的工程结算书。

2) 公正处理双方单位提出的索赔申请。

3.3 投资控制措施

3.3.1 投资控制的组织措施

建立健全监理组织, 完善职责分工及有关制度, 落实投资控制的责任。

1) 由驻现场监理工程师通过工程量支付来控制合同价款, 工程承建单位按约定的时间向监理工程师提交已完工工程报告, 监理工程师核实已完工程数量, 并由承建单位、监理工程师共同参与计量, 承建单位无正当理由不参与计量, 由监理工程师自行进行, 计量仍然有效, 作为工程价款支付依据。

2) 由驻现场监理工程师核实签字后, 须经总监理工程师 (或总监代表) 审核签字, 才作为有效的凭证。

3) 项目监理部每月应以规范的格式向监理单位报告工程投资情况。

3.3.2 投资控制的技术措施

1) 材料设备供应阶段, 监理工程师根据建设单位的要求, 对材料提出自己的建议。

2) 施工阶段, 监理工程师督促承建单位采用先进合理的施工组织设计和施工方案, 合理编排工期, 避免不必要的赶工费用。

3.3.3 投资控制的经济措施

1) 驻现场监理工程师每月定期进行计划费用与实际费用的比较分析, 并提出控制工程费用突破的方案和措施。经总监理工程师 (或总监代表) 审查签字后, 报监理单位。经主管领导审批后报建设单位。

2) 驻现场监理工程师应预测和防范可能发生的索赔, 及时向建设单位和上级报告可能发生的索赔, 并制定对策, 减少向建设单位索赔的发生。

3) 鼓励监理工程师对原设计或施工方案提出合理化建议, 如合理化建议被采用并对工程产生的投资节约, 应按合同予以一定的奖励。

3.3.4 投资控制的合同措施

1) 监理单位应协助建设单位如期向承建单位提供施工现场, 如期、保质、保量供应由建设单位负责的材料、设备, 及时提供设计方案等技术资料, 不违约, 不造成索赔条件。

2) 监理单位应按合同条款经审核支付工程款, 但防止过早、过量的现金支付。

4. 变更控制

4.1 变更控制的原则

(1) 对变更申请快速响应

(2) 任何变更都要得到三方确认

(3) 明确界定项目变更的目标

(4) 防止变更范围的扩大化

(5) 三方都有权提出变更

(6) 加强变更风险以及变更效果的评估

(7) 及时公布变更信息

(8) 选择冲击最小的方案

4.2 变更控制的流程

4.2.1 了解变化

在项目实施过程中，监理工程师与项目组织者要发现和把握变化，认真分析变化的性质，确定变化的影响，适时地进行变化一的描述，监理工程是要对整个项目的执行情况做到心中有数。

4.2.2 接受变更申请

变更申请单位向监理工程师提出变更要求或建议，提交书面工程变更建议书。工程变更建议书主要包括以下内容：变更的原因及依据；变更的内容及范围；变更引起的合同总价增加或减少；变更引起的合同工期提前或缩短；为审查所提交的附件及计算资料等。工程变更建议书应在预计可能变更的时间之前14天提出。在特殊情况下，工程变更可不受时间的限制。

4.2.3 变更的初审

项目监理机构应了解实际情况和收集与项目变更有关的资料，首先明确界定项目变更的目标，再根据收集的变更信息判断变更的合理性和必要性。对于完全无必要的变更，可以驳回此申请，并给出监理意见；对于有必要的变更，可以进一步进行变更分析。

4.2.4 变更分析

把项目变化融入项目计划中是一个新的项目规划过程，只不过这规划过程是以原来的项目计划为框架，在考察项目变化的基础上完成的。通过与新项目计划的对比，监理工程师可以清楚地看到项目变化对项目预算、进度、资源配置的影响与冲击。把握项目变化的影响和冲击是相当重要的，否则就难以做出正确的决策，做出合理的项目变更。

4.2.5 确定变更方法

三方进行协商和讨论，根据变更分析的结果，确定最优变更方案。做出项目变更时，力求在尽可能小的变动幅度内对主要因素进行微调。根据变更方案下达变更通知书并进行变更公布，并把变更实施方案告知有关实施部门和实施人员，为变更实施做好准备。

4.2.6 监控变更的实施

变更后的内容作为新的计划和方案，可以纳入正常的监理工作范围，监理工程师对变更部分的内容要密切注意，项目变更控制是一个动态的过程，在这一过程中，要记录这一变化过程，充分掌握信息，及时发现变更引起的超过估计的后果，以便及时控制和处理。

4.2.7 变更效果评估

在变更实施结束后，要对变更效果进行分析和评估。整个变更控制流程如图所示。

5. 合同管理

5.1 合同管理的原则

合同管理的原则是指监理单位在信息系统工程监理过程中针对各类合同的管理须遵循的宗旨，贯穿合同管理的全过程，包括：事前预控原则、实时纠偏原则、充分协商原则和公正处理原则。

5.2 合同管理的主要内容

本项目合同管理的工作内容包括：

拟定信息工程的管理制度，其中应包括合同草案的拟定、会签、协商、修改、审批、签署、保管等工作制度及流程；

协助建设单位拟定信息工程合同的各类条款，参与建设单位和承建单位的谈判活动；

及时分析合同的执行情况，并进行跟踪管理；

协调建设单位与承建单位的有关索赔及合同纠纷事宜。

归纳起来，监理单位在合同管理中的主要内容应由三部分组成，即合同的签订管理、合同的档案管理和

合同的履行管理。

5.3 合同的签订管理

合同的签订管理是指监理协助建设单位与承建单位、设备材料供应单位等各方之间的各种合同进行分析、谈判、协商、拟定、签署等。

合同分析是合同签订中最重要的内容和环节，是合同签订的前提。监理工程师应对工程承建、共同承担风险的合同条款、法律条款分别进行仔细的分析解释。同时也要对合同条款的更换、延期说明、投资变化等事件进行仔细分析。合同分析和项目检查等工作要与其联系起来。

监理工程师在订立合同的过程中要按条款逐条分析，如果发现对建设单位产生风险较大的条款，要增加相应的抵御条款。要详细分析哪些条款与建设单位有关、与承建单位有关、与项目检查有关、与工期有关等，分门别类地分析各自责任和相互联系的关联要素，做到一清二楚，心中有数。

5.4 合同的履行管理

合同的履行管理是指监理工程师对合同各方关于合同约定的工期、质量和费用、争议解决及索赔处理等工作的管理。

1) 履约管理的方式—合同控制

合同控制指为保证合同所约定的各项义务的全面完成及各项权利的实现，以合同分析的成果为基准，监理对整个合同实施过程的全面监督、检查、对比、引导及纠正的管理活动。

合同控制的首要内容是对合同实施情况进行追踪，追踪的对象包括：

具体的合同事件。包括项目的质量、工期、成本。

承建单位的工作。对承建单位的项目缺陷提出意见，提出警告，责成他们改进。

建设单位是否及时下达命令，做出答复，及时支付项目款项。

总体情况，如整体项目的秩序如何，已完项目是否通过验收，有无大的项目事故，进度是否出现拖期，计划和实际成本有无大的偏差等。

2) 履约管理的保证—合同监督

合同监督就是要对合同条款经常与实际实施情况进行比对，以便根据合同来掌握项目的进展。保证设计、开发、实施的精确性，并符合合同要求。合同监督的另一个重要的内容是检查解释双方来往的信函和文件，以及会议记录、建设单位指示等，因为这些内容对合同管理是非常重要的

5.5 合同档案的管理

合同档案的管理，也即合同文件管理，是整个合同管理的基础。所有与合同有关的文件都是重要的文字依据，合同管理人员必须及时填写并妥善保存经有关方面签证的文件和单据，并建立合同档案数据库，以免在合同履行中发生纠纷时缺少有关的文字根据。

6. 安全管理内容

审核工程信息安全方案，监督信息安全策略的实施；审核施工组织安全管理措施，监督安全制度的落实，确保施工安全。

7. 信息管理

7.1 项目信息的划分

项目信息应划分为：

1) 投资控制信息

投资控制信息包括：费用规划信息，如投资计划、投资估算、工程预算等；实际费用信息，如各类费用支出凭证、工程变更情况、工程结算签证，以及物价指数、人工、软件环境、硬件设备等市场价格等；投资控制的分析比较信息，如费用的历史经验数据、现行数据、预测数据及经济与财务分析的评

价数据等。

2) 进度控制信息

进度控制信息包括：信息工程项目进度规划，如总进度计划、分目标进度计划、各实施阶段的进度计划、单项工程及单位工程实施进度计划、资金及物资供应计划、劳动力及设备的配置计划等；工程实际进度的统计信息，如项目日志、实际完成工程量、实际完成工作量等；进度控制比较信息，如工期定额、实现指标等。

3) 质量控制信息

质量控制信息包括：信息工程项目实体质量信息，如质量检查、测试数据、隐蔽验收记录、质量事故处理报告，以及材料、设备质量证明及技术验证单等；信息工程项目的功能及使用价值信息，如有关标准和规范，质量目标指标，设计文件、资料、说明等；信息工程项目的工作质量信息，如质量体系文件，质量管理工作制度，质量管理的考核制度，质量管理工作的组织制度等。

4) 合同管理信息

合同管理信息包括：合同管理法规，如招标投标法、经济合同法等；信息系统工程合同文本，如设计合同、实施合同、采购合同等；合同实施信息，如合同执行情况、合同变更、签证记录、工程索赔等。

5) 组织协调信息

组织协调信息包括：工程质量调整及信息工程项目调整的指令；工程建设合同变更及其协议书；政府及主管部门对工程项目建设过程中的指令、审批文件；有关信息系统工程有关的法规及技术标准。

6) 其他用途的信息

其他用途的信息是除上述五类用途的信息外，对信息系统工程项目建设决策提供辅助支持的某些其他信息，如工程中往来函件等。

7.2 目信息管理的方法

7.2.1 文档管理过程应该注意事项

文档的格式应该统一。

文档版本的管理。新的版本出来后，旧的版本应该进行相应的改变，同时彻底从管理库中清除，以保持文档版本的统一。

关于文档的存档标准。文档的存档标准是指某一类型的文档究竟应该保存多长时间，这个问题应该由监理单位根据国家档案管理相关的要求，统一进行规定。

7.2.2 监理工程师在归集监理资料时注意事项

监理资料应及时整理、真实完整、分类有序；

监理资料的管理应由总监理工程师负责，并指定专人具体实施；

监理资料应在各阶段监理工作结束后及时整理归档；

监理档案的编制及保存应按有关规定执行。

7.3 监理机构文档管理的职责

监理单位对文档工作的支持。监理单位应为编写文档的人员提供指导和实际鼓励，并使各种资源有效地用于文档开发。

监理单位的主要职责：

建立编制、登记、出版、分发系统文档和软件文档的各种策略；

把文档计划作为整个开发工作的一个组成部分；

建立确定文档质量、测试质量和评审质量的各种方法的规程；

为文档的各个方面确定和准备各种标准和指南；

	<p>积极支持文档工作以形成在开发工作中自觉编制文档的团队风气；</p> <p>不断检查已建立起来的过程，以保证符合策略和各种规程并遵守有关标准和指南。</p> <p>8.项目协调</p> <p>8.1协调的原则</p> <p>在协调项目实施过程中项目进度、工程质量与合同支付等合同目标之间的矛盾时，遵循以下原则：</p> <p>8.1.1在确保项目质量的条件下，促进项目实施进展；</p> <p>8.1.2在寻求建设单位更大投资效益的基础上，正确处理合同目标之间的矛盾；</p> <p>8.1.3在维护建设单位合同权益的同时，实事求是的维护承建单位地合法权益。</p> <p>8.2监理协调内容</p> <p>8.2.1工程项目内部需求关系协调</p> <p>1）监理过程中抓计划环节，平衡人员、材料、设备、能源动力的需求，要注意抓住期限的及时性，规格上的明确性，数量上的准确性，质量上的规定性，体现计划的严肃性，发挥指导作用。</p> <p>2）指导承建单位对施工力量的平衡，要抓住瓶颈环节，发现瓶颈环节，要通过资源力量的调整，集中力量打攻坚战。抓关键、抓主要矛盾、运用网络计划技术的关键线路法是有效的工具。</p> <p>3）对专业工种配合，要抓住调度环节，项目施工中需要机械化施工、土建、机电安装等专业工种交替配合进行，交替进行抓好衔接问题，配合进行抓好步调问题，就是抓好调度协调工作。</p> <p>4）施工准备阶段的协调：</p> <p>作好施工准备是顺利组织施工的先决条件。满足开工的条件是：有完善有效的施工设计方案；有政府管理部门签发的施工许可证；财务和材料渠道已落实，能按工程进度需要拨款、供料；施工组织设计已经批准；加工订货和设备已基本落实；施工准备工作已基本完成，现场已“五通一平”。监理工程师应协助落实上述开工条件，保持建设单位与承建单位的信息沟通，协商办事，督促双方严格按合同执行。建设单位和承建双方对施工准备工作应有明确的约定和分工，以便协调。</p> <p>5）施工阶段的协调：</p> <p>包括解决进度、质量、中间计量与支付、合同纠纷等一系列问题。</p> <p>进度问题有两项有效协调工作应作好，一是建设单位和承建单位双方商定工程计划方案，并双方负责人在上面签字，作为工程承包合同附件；二是设立进度考核规范，按工程计划节点考核，分期预付。</p> <p>质量问题的协调：实行监理工程师质量签字认可，对没有出厂证明，不符合使用要求的原材料、设备和构件，不准使用，对不合格的工程部位不予验收签证，也不予计算工程量，不予支付进度款。</p> <p>合同争议的协调：合同纠纷，应协商解决，不能协调解决时再向合同管理机关申请调解或仲裁。</p> <p>6）交工验收阶段的协调：</p> <p>对交工验收中建设单位提出的问题，承建单位应根据技术文件、合同、中间验收签证及验收规范作出解释，对不符合要求应督促其采取补救措施，使其达到设计、合同、规范要求，而后办理竣工结算。</p>
--	--

3.2.3人员配置要求

- 采购包1：
- 投标供应商须提供针对本项目的详细人员配备情况。要求拟派项目成员相关专业人员搭配合理、职能健全，岗位分工明确、职责清晰，包括人员配备情况及水平、人员安排、专业配置、从业经历、参与工作经验等方面，均应满足本项目采购需求，具体以3.2.2服务要求为准。
- 采购包2：
- 投标供应商须提供针对本项目的详细人员配备情况。要求拟派项目成员相关专业人员搭配合理、职能健全，岗位分工明确、职责清晰，包括人员配备情况及水平、人员安排、专业配置、从业经历、参与工作经验等方面，均应满足本项目采购需求。

求，具体以3.2.2服务要求为准。

采购包3:

投标供应商须提供针对本项目的详细人员配备情况。要求拟派项目成员相关专业人员搭配合理、职能健全，岗位分工明确、职责清晰，包括人员配备情况及水平、人员安排、专业配置、从业经历、参与工作经验等方面，均应满足本项目采购需求，具体以3.2.2服务要求为准。

采购包4:

投标供应商须提供针对本项目的详细人员配备情况。要求拟派项目成员相关专业人员搭配合理、职能健全，岗位分工明确、职责清晰，包括人员配备情况及水平、人员安排、专业配置、从业经历、参与工作经验等方面，均应满足本项目采购需求，具体以3.2.2服务要求为准。

采购包5:

投标供应商须提供针对本项目的详细人员配备情况。要求拟派项目成员相关专业人员搭配合理、职能健全，岗位分工明确、职责清晰，包括人员配备情况及水平、人员安排、专业配置、从业经历、参与工作经验等方面，均应满足本项目采购需求，具体以3.2.2服务要求为准。

采购包6:

投标供应商须提供针对本项目的详细人员配备情况。要求拟派项目成员相关专业人员搭配合理、职能健全，岗位分工明确、职责清晰，包括人员配备情况及水平、人员安排、专业配置、从业经历、参与工作经验等方面，均应满足本项目采购需求，具体以3.2.2服务要求为准。

3.2.4设施设备配置要求

采购包1:

投标供应商须提供履行本项目所必需的设备，具体以3.2.2服务要求为准。

采购包2:

投标供应商须提供履行本项目所必需的设备，具体以3.2.2服务要求为准。

采购包3:

投标供应商须提供履行本项目所必需的设备，具体以3.2.2服务要求为准。

采购包4:

投标供应商须提供履行本项目所必需的设备，具体以3.2.2服务要求为准。

采购包5:

投标供应商须提供履行本项目所必需的设备，具体以3.2.2服务要求为准。

采购包6:

投标供应商须提供履行本项目所必需的设备，具体以3.2.2服务要求为准。

3.2.5其他要求

采购包1:

1.项目质保 整体质保三年。 2.质量标准 满足国家及行业现行技术标准、规范要求。 3.售后服务要求 （1）中标供应商必须拥有一套切实可行的质保保证体系，确保项目的实施及服务质量。（2）为保证系统的正常运行，中标供应商必须承诺保障本项目的本地化服务能力，中标后于项目所在地设立常驻服务和技术支持机构，并配备较强的专业技术队伍，能提供快捷的售后服务响应。（3）服务内容包括现场服务、定期巡检、故障服务。（4）中标供应商应建立运行维护团队，故障响应要求：（5）提供7×24小时响应。（6）故障在1小时内响应，如电话、网络等不能解决问题，2小时到现场，24小时解决问题，紧急状况1小时到现场，4小时解决问题。（7）如遇紧急、重大服务事项，需在保证提供多人、快速服务响应的情况下配合管理方协调产品的研发单位进行现场应急事件处理。（8）中标供应商应有完善的文档管理制度，保证运行维护过程中产生的文档。（9）在提供服务的过程中，获悉的一切资讯需严格遵守保密协议，严禁自行使用或向他人传播，泄漏或擅自使用或允许他人使用上述信息，由此造成的损失应承担相应的法律责任。 4.培训要求 （1）项目实施方需提供详细的培训计划。（2）

培训授课人必须是承担本项目实施服务工作的工程师、技术人员等。（3）培训时间不少于两天，地点为采购方选定，培训方式为一人一机集中培训。（4）培训内容与课程要求：培训内容为系统操作以及常见问题处理，确保工作人员具备独立工作的能力。

采购包2:

1.项目质保 整体质保五年。2.质量标准 满足国家及行业现行技术标准、规范要求。3.售后服务要求（1）中标供应商必须拥有一套切实可行的质保保证体系，确保项目的实施及服务质量。（2）为保证系统的正常运行，中标供应商必须承诺保障本项目的本地化服务能力，中标后于项目所在地设立常驻服务和专业技术支持机构，并配备较强的专业技术队伍，能提供快捷的售后服务响应。（3）服务内容包括现场服务、定期巡检、故障服务。（4）中标供应商应建立运行维护团队，故障响应要求：（5）提供7×24小时响应。（6）故障在1小时内响应，如电话、网络等不能解决问题，2小时到现场，24小时解决问题，紧急状况1小时到现场，4小时解决问题。（7）如遇紧急、重大服务事项，需在保证提供多人、快速服务响应的情况下配合管理方协调产品的研发单位进行现场应急事件处理。（8）中标供应商应有完善的文档管理制度，保证运行维护过程中产生的文档。（9）在提供服务的过程中，获悉的一切资讯需严格遵守保密协议，严禁自行使用或向他人传播，泄漏或擅自使用或允许他人使用上述信息，由此造成的损失应承担相应的法律责任。4.人员培训方案（1）在设备安装调测时，必须对现场（至少2名）采购方人员进行培训，培训内容必须能够满足系统维护人员能够顺利完成日常的维护工作并由中标人在项目实施前书面提供并经采购方确认，培训后必须有现场（至少2名）采购方人员书面确认，否则对该现场的项目实施不予确认，因此而造成的项目延误由中标人负全部责任。（2）中标人应负责项目实施后的买方技术人员和管理专家的技术培训，培训内容包括初级培训和高级培训。（3）初级培训应使得系统维护人员能够顺利地完的维护工作，保证系统的正常运行；高级培训应使得高级维护人员对建成后的系统的运行机制有着清晰明确的认识并能够高效及时地解决系统突发运行故障；系统开发人员应能够独立地开发新业务的管理模块，并提供全套培训教材(中文)和培训课程计划表。4.中标人应详细开列所能提供的各种培训的具体情况，包括培训时间、培训地点、培训内容、培训进度、培训人员数量等及相应的各种培训费用。

采购包3:

1.售后服务要求 售后服务期从项目验收合格之日起，具体要求如下：（1）配合检查服务 投标人需协助采购人响应第三方机构针对信息系统安全的检查工作。服务内容包括协助客户准备、完善各类资料文档，配合检查过程中的答疑及技术支持及其他现场检查的响应。（2）电话支持服务 投标人需提供7*24不间断的电话支持服务，解答采购人在使用过程中遇到的问题，及时提出解决问题的建议 and 操作方法。电话响应时间不超过10分钟，到达现场时间不超过2小时，解决问题不超过24小时。（3）技术咨询服务 投标人需为采购人提供技术咨询服务，包括信息系统整改建设咨询服务以及其他相关安全咨询服务，一旦接到采购人的服务请求，技术服务工程师将立即开始提供服务，帮助客户解决信息安全相关技术问题，全面配合比选人做好业务系统全保障工作。

采购包4:

1.质保期要求 项目验收合格之日起十二个月内提供密码安全咨询服务。2.售后服务要求 售后服务期从项目验收合格之日起，具体要求如下： 投标人自项目终验之日起1年内，7*24不间断的电话支持服务，解答采购人在使用过程中遇到的问题，及时提出解决问题的建议 and 操作方法。电话响应时间不超过10分钟，解决问题不超过24小时。

采购包5:

1.售后服务要求 售后服务期从项目验收合格之日起，具体要求如下：（1）技术支持：投标方应保证在售后服务期内提供7×24小时技术支持服务，应提供本单位的热线电话、E-mail、传真、网站等途径，随时接受系统使用人员提出的各种技术问题，并在24小时内提供解决方案。（2）故障响应：投标方应保证在售后服务期内，各类故障应在1小时内响应，2小时内提供应急解决方案。影响系统正常使用的bug在使用方提出后8小时内修正；系统安全漏洞的修复，要在使用方提出后24小时内解决。（3）本地服务：投标人能够在中标后提供及时迅速的本地售后运维服务。

采购包6:

1.售后服务要求 售后服务期从项目验收合格之日起，具体要求如下： 投标人需提供7*24不间断的电话支持服务，解答采购人在使用过程中遇到的问题，及时提出解决问题的建议 and 操作方法。电话响应时间不超过10分钟，解决问题不超过24小

时。

3.3商务要求

3.3.1服务期限

- 采购包1：
合同签订后90个日历日内
- 采购包2：
合同签订后90个日历日内
- 采购包3：
合同签订后90个日历日内
- 采购包4：
合同签订后90个日历日内
- 采购包5：
合同签订后90个日历日内
- 采购包6：
自合同签订之日起，到项目整体验收通过之日止。

3.3.2服务地点

- 采购包1：
采购人指定地点
- 采购包2：
采购人指定地点
- 采购包3：
采购人指定地点
- 采购包4：
采购人指定地点
- 采购包5：
采购人指定地点
- 采购包6：
采购人指定地点

3.3.3考核（验收）标准和方法

采购包1：

1.本项目由政法系统各单位联合验收。 2.初验:系统上线前，应对系统的各项功能进行详细验证，确保系统功能符合要求，并完成系统压力测试，采购人及中标人对系统功能、业务流程确认无误，中标人向采购人交付需求确认书、系统设计方案、系统作手册、使用说明等相关资料。各方共同签署系统检验确认书，但有关功能、业务、流程、性能等的检验不应视为最终检验。 3.终验: (1)通过初验后，系统上线试运行，试运行结束后，能够实现技术要求中标人准备验收文件并书面通知采购人。(2)采购人确认中标人的自检初验合格后，组织中标人(必要时请有关专家)进行系统验收，验收合格后，填写政府采购项目验收单(一式伍份)作为对项目的最终认可。 4.验收依据 (1)招标文件、投标文件、澄清表(如有); (2)本项目采购合同及附件文本; (3)合同签订时国家及行业现行的标准和技术规范。 4.中标人向采购人提交项目实施过程中的所有资料，以便采购人日后管理和维护。

采购包2：

此次项目主要涉及设备验收、系统集成的验收。项目申请验收时，由项目单位组织参与方包括项目单位、政法系统各单

位、监理单位、信息化相关专家共同联合验收。1.到货设备验收 设备验收分设备的到货验收和设备的最终验收，具体的验收步骤包括：设备到货验收，货物经检验合格并运抵指定地点后，由采购人对货物的种类、规格、型号、数量、外观、包装设备及有关文件资料（如产品检验合格证书、商检证书、装箱单、保修单等）进行初步验收，查看是否符合合同的规定，并出具设备到货验收证书。此验收为“非加电”验收，只是设备的到货验收，并不是设备的最终验收。货物最终验收，货物的质量、性能等，待安装调试、局部配套设备联结，构成相应的硬件平台、软件平台和网络平台后，再进行测试验收，此测试验收和系统集成验收一同进行，硬件设备及软件产品必须在标书规定的地点和环境下实现正常运行，并达到标书要求的性能和产品技术规格中的性能。采购人委将依据签署的合同，并参照产品生产厂商提供的应标书对其提供的全部设备进行到货验收。对产品的验收包括检查产品的型号、规格、数量、外型、外观、包装、资料及文件（如装箱单、保修单、随箱介质等）是否与合同完全一致。2.系统集成验收 2.1初验:系统上线前，应对系统的各项功能进行详细验证，确保系统功能符合需求，并完成系统压力测试，采购人及中标人双方对系统功能、业务流程确认无误，中标人向采购人交付需求确认书、系统设计方案、系统作手册、使用说明等相关资料。双方共同签署系统检验确认书，但有关功能、业务、流程、性能等的检验不应视为最终检验。2.2终验:(1)通过初验后，系统上线试运行，试运行结束后，能够实现技术要求中标人准备验收文件并书面通知采购人。(2)采购人确认中标人的自检初验合格后，组织中标人(必要时请有关专家)进行系统验收，验收合格后，填写政府采购项目验收单(一式伍份)作为对项目的最终认可。2.3验收依据 (1)招标文件、投标文件、澄清表(如有):(2)本项目采购合同及附件文本;(3)合同签订时国家及行业现行的标准和技术规范。3.中标人向采购人提交项目实施过程中的所有资料，以便采购人日后管理和维护。

采购包3:

采购人及相关人员组成验收小组完成验收。双方根据最终验收情况，编写验收报告。中标人应完成项目验收资料的准备。本项目的实施过程中将产生大量的技术及管理文档，中标人应协助采购人，负责建立、维护、交接项目实施过程中产生的各类文档，确保项目文档的内容体现本项目的实施过程，并确保项目文档的完整性和准确性。投标人按照要求提交全部项目文档。

采购包4:

采购人及相关人员组成验收小组完成验收。双方根据最终验收情况，编写验收报告。中标人应完成项目验收资料的准备。本项目的实施过程中将产生大量的技术及管理文档，中标人应协助采购人，负责建立、维护、交接项目实施过程中产生的各类文档，确保项目文档的内容体现本项目的实施过程，并确保项目文档的完整性和准确性。投标人按照要求提交全部项目文档。

采购包5:

采购人及相关人员组成验收小组完成验收。双方根据最终验收情况，编写验收报告。中标人应完成项目验收资料的准备。本项目的实施过程中将产生大量的技术及管理文档，中标人应协助采购人，负责建立、维护、交接项目实施过程中产生的各类文档，确保项目文档的内容体现本项目的实施过程，并确保项目文档的完整性和准确性。投标人按照要求提交全部项目文档。

采购包6:

采购人及相关人员组成验收小组完成验收。双方根据最终验收情况，编写验收报告。中标人应完成项目验收资料的准备。本项目的实施过程中将产生大量的技术及管理文档，中标人应协助采购人，负责建立、维护、交接项目实施过程中产生的各类文档，确保项目文档的内容体现本项目的实施过程，并确保项目文档的完整性和准确性。投标人按照要求提交全部项目文档。

3.3.4支付方式

采购包1:

分期付款

采购包2:

分期付款

采购包3:

分期付款

采购包4:

分期付款

采购包5:

分期付款

采购包6:

分期付款

3.3.5.支付约定

采购包1: 付款条件说明: 签订合同后, 达到付款条件起 30 日内, 支付合同总金额的 40.00%。

采购包1: 付款条件说明: 通过项目初验后, 达到付款条件起 30 日内, 支付合同总金额的 20.00%。

采购包1: 付款条件说明: 通过项目终验后, 达到付款条件起 30 日内, 支付合同总金额的 40.00%。

采购包2: 付款条件说明: 签订合同后, 达到付款条件起 30 日内, 支付合同总金额的 40.00%。

采购包2: 付款条件说明: 通过项目初验后, 达到付款条件起 30 日内, 支付合同总金额的 20.00%。

采购包2: 付款条件说明: 通过项目终验后, 达到付款条件起 30 日内, 支付合同总金额的 40.00%。

采购包3: 付款条件说明: 签订合同后, 达到付款条件起 20 日内, 支付合同总金额的 40.00%。

采购包3: 付款条件说明: 验收合格后, 达到付款条件起 20 日内, 支付合同总金额的 60.00%。

采购包4: 付款条件说明: 签订合同后, 达到付款条件起 20 日内, 支付合同总金额的 40.00%。

采购包4: 付款条件说明: 验收合格后, 达到付款条件起 20 日内, 支付合同总金额的 60.00%。

采购包5: 付款条件说明: 签订合同后, 达到付款条件起 20 日内, 支付合同总金额的 40.00%。

采购包5: 付款条件说明: 验收合格后, 达到付款条件起 20 日内, 支付合同总金额的 60.00%。

采购包6: 付款条件说明: 签订合同后, 达到付款条件起 20 日内, 支付合同总金额的 40.00%。

采购包6: 付款条件说明: 验收合格后, 达到付款条件起 20 日内, 支付合同总金额的 60.00%。

3.3.6违约责任与争议解决的方法

采购包1:

以采购合同相关条款要求为准。

采购包2:

以采购合同相关条款要求为准。

采购包3:

以采购合同相关条款要求为准。

采购包4:

以采购合同相关条款要求为准。

采购包5:

以采购合同相关条款要求为准。

采购包6:

以采购合同相关条款要求为准。

3.5其他要求

3.5.1项目技术移交 (1) 中标供应商在项目终验后, 应将本项目所有相关的技术文件、资料档案, 包括技术文档、需求分析文档、验收报告等整个服务期间所需要制订的文档汇集成册交付采购人。(2) 未经采购人认可的情况下, 所有的文件用中文书写或有完整的中文注释。(3) 本项目要求所有文档向采购人提供纸质文档至少4套, 电子文档1套。中标供应商应设

置专人在项目建设期间对文档进行检查和管理，项目最终验收后全部移交给采购人。（4）中标供应商应在中标后签订保密协议，承诺不将任何涉及本项目的信息向外界泄露。

3.5.2知识产权要求（1）中标供应商应保证本项目所采用的技术、产品、服务或其任何一部分不会产生因第三方提出侵犯其专利权、商标权或其他知识产权而引起的法律和经济纠纷；如因第三方提出其专利权、商标权或其他知识产权的侵权之诉，则一切法律责任及采购人的损失（包括但不限于重新招投标费用、律师费、诉讼费等）由中标供应商承担。（2）中标供应商所提供采购人的项目成果或其它技术文档等项目成果（包括草案和正式稿）所有权、使用权及知识产权等权利均由采购人享有；同时，未经采购人书面许可，中标供应商不得使用本项目的项目成果，不得自行使用或者将本项目的项目成果提供给第三方，否则全部收益归采购人所有，中标供应商另向采购人承担全部责任。

（3）本项目运行在云平台上的任何形式的数据、文件的所有权均属于采购人和用户单位，中标供应商无权处置。

3.5.3纸质文件要求（1）供应商需要在线提交所有通过电子化交易平台实施的政府采购项目的投标文件，同时，线下提交纸质投标文件正本壹份、副本贰份。若电子投标文件与纸质投标文件不一致的，以电子投标文件为准。（2）投标文件，正、副本分别各自装订成册密封。在封口处加盖供应商公章。（3）线下投标文件递交截止时间与线上开评标时间一致。（4）纸质投标文件可邮寄递交，应于递交投标文件截止时间前邮寄到西安市高新区丈八一路1号汇鑫中心D座2206室（陕西德勤招标有限公司）。

3.5.4投标保证金注意事项（1）投标保证金须从投标人户名支付，如从个人户名或非投标人户名支付，将被拒绝，视为自动放弃投标权利（该个人是投标人的情形除外）；以保函形式交纳投标保证金的，投标人应在投标截止时间前将保函扫描成清晰的PDF文件，发送至邮箱deqinjxm@126.com（邮件命名：项目编号）；投标人应在投标文件中附保函扫描件。保函必须由具有开具投标保函资格的单位开具；若中标人违约，开具保函单位承担连带责任；（2）投标保证金的提交金额、时间不满足招标文件要求的，投标无效；（3）未按指定账户提交的，我公司将退回，投标人须在文件递交截止时间前按照指定账户再次提交。

3.5.5合同签订注意事项 中标人应当在中标通知书发出之日起25日内与采购人签订政府采购合同。

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招标文件的规定，对投标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。	投标函 投标人应提交的相关资格证明材料
2	供应商应提供健全的财务会计制度的证明材料；	提供2023年度经审计的财务报告（成立时间至提交投标文件截止时间不足一年的可提供成立后任意时段的资产负债表），或其开标前三个月内基本开户银行出具的资信证明，或信用担保机构出具的投标担保函（以上三种形式的资料提供任何一种即可）。	投标人应提交的相关资格证明材料
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。	投标函

采购包2：

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。	投标函 投标人应提交的相关资格证明材料
2	供应商应提供健全的财务会计制度的证明材料；	提供2023年度经审计的财务报告（成立时间至提交投标文件截止时间不足一年的可提供成立后任意时段的资产负债表），或其开标前三个月内基本开户银行出具的资信证明，或信用担保机构出具的投标担保函（以上三种形式的资料提供任何一种即可）。	投标人应提交的相关资格证明材料

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。	投标函
---	--	---------------------------------------	-----

采购包3:

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。	投标函 投标人应提交的相关资格证明材料
2	供应商应提供健全的财务会计制度的证明材料；	提供2023年度经审计的财务报告（成立时间至提交投标文件截止时间不足一年的可提供成立后任意时段的资产负债表），或其开标前三个月内基本开户银行出具的资信证明，或信用担保机构出具的投标担保函（以上三种形式的资料提供任何一种即可）。	投标人应提交的相关资格证明材料
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。	投标函

采购包4:

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。	投标函 投标人应提交的相关资格证明材料
2	供应商应提供健全的财务会计制度的证明材料；	提供2023年度经审计的财务报告（成立时间至提交投标文件截止时间不足一年的可提供成立后任意时段的资产负债表），或其开标前三个月内基本开户银行出具的资信证明，或信用担保机构出具的投标担保函（以上三种形式的资料提供任何一种即可）。	投标人应提交的相关资格证明材料

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。	投标函
---	--	---------------------------------------	-----

采购包5:

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。	投标函 投标人应提交的相关资格证明材料
2	供应商应提供健全的财务会计制度的证明材料；	提供2023年度经审计的财务报告（成立时间至提交投标文件截止时间不足一年的可提供成立后任意时段的资产负债表），或其开标前三个月内基本开户银行出具的资信证明，或信用担保机构出具的投标担保函（以上三种形式的资料提供任何一种即可）。	投标人应提交的相关资格证明材料
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。	投标函

采购包6:

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。	投标函 投标人应提交的相关资格证明材料
2	供应商应提供健全的财务会计制度的证明材料；	提供2023年度经审计的财务报告（成立时间至提交投标文件截止时间不足一年的可提供成立后任意时段的资产负债表），或其开标前三个月内基本开户银行出具的资信证明，或信用担保机构出具的投标担保函（以上三种形式的资料提供任何一种即可）。	投标人应提交的相关资格证明材料

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。	投标函
---	--	---------------------------------------	-----

4.2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	营业执照等主体资格证明文件	提供有效存续的企业营业执照（副本）/事业单位法人证书/专业服务机构执业许可证/民办非企业单位登记证书。	投标人应提交的相关资格证明材料
2	财务状况报告	提供 2023 年度经审计的财务报告（成立时间至提交投标文件截止时间不足一年的可提供成立后任意时段的资产负债表），或其递交投标文件截止之日前三个月内基本开户银行出具的资信证明，或信用担保机构出具的投标担保函(以上三种形式的资料提供任何一种即可）。	投标人应提交的相关资格证明材料
3	书面声明	提供书面声明，包括声明具有履行合同所必需的设备和专业技术能力；未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。	书面声明
4	社保缴纳证明	提供递交投标文件截止之日前一年内任意一个月的社会保障资金缴存单据或社保机构开具的社会保险参保缴费情况证明。依法不需要缴纳社会保障资金的投标供应商应提供相关证明文件。	投标人应提交的相关资格证明材料
5	税收缴纳证明	提供递交投标文件截止之日前一年内任意一个月的依法缴纳税收的相关凭据（时间以税款所属日期为准、税种至少包含增值税或企业所得税），凭据应有税务机关或代收机关的公章或业务专用章。依法免税或无须缴纳税收的投标供应商，应提供相应证明文件。	投标人应提交的相关资格证明材料
6	近三年无重大违法、违纪书面声明	提供《近三年无重大违法、违纪书面声明》。	近三年无重大违法、违纪书面声明

7	信用记录	投标供应商未被列入“信用中国”网站记录的“失信被执行人”或“重大税收违法案件当事人”名单；不处于“中国政府采购网”记录的“政府采购严重违法失信行为记录名单”中的禁止参加政府采购活动期间。（以采购人或采购代理机构开标当天查询结果为准）；	投标人应提交的相关资格证明材料
8	控股管理关系	提供直接控股和管理关系清单。若与其他投标人存在单位负责人为同一人或者存在直接控股、管理关系的，则投标无效。	控股管理关系
9	法定代表人授权委托书	法定代表人参加投标的，须提供本人身份证复印件；法定代表人授权他人参加投标的，须提供法定代表人授权委托书。招标文件中凡是需要法定代表人盖章之处，非法人单位的负责人均参照执行。法人的分支机构参与投标时，除提供《法定代表人授权委托书》外，还须同时提供总公司给分支机构出具的授权书。	法定代表人授权书
10	本项目不接受联合体投标，不允许分包	投标供应商应提供《非联合体不分包投标声明》，视为独立投标，不分包。	非联合体不分包投标声明

采购包2:

序号	资格审查要求概况	评审点具体描述	关联格式
1	营业执照等主体资格证明文件	提供有效存续的企业营业执照（副本）/事业单位法人证书/专业服务机构执业许可证/民办非企业单位登记证书。	投标人应提交的相关资格证明材料
2	财务状况报告	提供2023年度经审计的财务报告（成立时间至提交投标文件截止时间不足一年的可提供成立后任意时段的资产负债表），或其递交投标文件截止之日前三个月内基本开户银行出具的资信证明，或信用担保机构出具的投标担保函(以上三种形式的资料提供任何一种即可）。	投标人应提交的相关资格证明材料
3	书面声明	提供书面声明，包括声明具有履行合同所必需的设备和专业技术能力；未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。	书面声明
4	社保缴纳证明	提供递交投标文件截止之日前一年内任意一个月的社会保障资金缴存单据或社保机构开具的社会保险参保缴费情况证明。依法不需要缴纳社会保障资金的投标供应商应提供相关证明文件。	投标人应提交的相关资格证明材料

5	税收缴纳证明	提供递交投标文件截止之日前一年内任意一个月的依法缴纳税收的相关凭据（时间以税款所属日期为准、税种至少包含增值税或企业所得税），凭据应有税务机关或代收机关的公章或业务专用章。依法免税或无须缴纳税收的投标供应商，应提供相应证明文件。	投标人应提交的相关资格证明材料
6	近三年无重大违法、违纪书面声明	提供《近三年无重大违法、违纪书面声明》。	近三年无重大违法、违纪书面声明
7	信用记录	投标供应商未被列入“信用中国”网站记录的“失信被执行人”或“重大税收违法案件当事人”名单；不处于“中国政府采购网”记录的“政府采购严重违法失信行为记录名单”中的禁止参加政府采购活动期间。（以采购人或采购代理机构开标当天查询结果为准）；	投标人应提交的相关资格证明材料
8	控股管理关系	提供直接控股和管理关系清单。若与其他投标人存在单位负责人为同一人或者存在直接控股、管理关系的，则投标无效。	控股管理关系
9	法定代表人授权委托书	法定代表人参加投标的，须提供本人身份证复印件；法定代表人授权他人参加投标的，须提供法定代表人授权委托书。招标文件中凡是需要法定代表人盖章之处，非法人单位的负责人均参照执行。法人的分支机构参与投标时，除提供《法定代表人授权委托书》外，还须同时提供总公司给分支机构出具的授权书。	法定代表人授权书
10	本项目不接受联合体投标，不允许分包	投标供应商应提供《非联合体不分包投标声明》，视为独立投标，不分包。	非联合体不分包投标声明

采购包3:

序号	资格审查要求概况	评审点具体描述	关联格式
1	营业执照等主体资格证明文件	提供有效存续的企业营业执照（副本）/事业单位法人证书/专业服务机构执业许可证/民办非企业单位登记证书。	投标人应提交的相关资格证明材料
2	财务状况报告	提供2023年度经审计的财务报告（成立时间至提交投标文件截止时间不足一年的可提供成立后任意时段的资产负债表），或其递交投标文件截止之日前三个月内基本开户银行出具的资信证明，或信用担保机构出具的投标担保函(以上三种形式的资料提供任何一种即可)。	投标人应提交的相关资格证明材料
3	书面声明	提供书面声明，包括声明具有履行合同所必需的设备和专业技术能力；未为本项目提供整体设计、规范编制或者项目管理、监理等服务。	书面声明

4	社保缴纳证明	提供递交投标文件截止之日前一年内任意一个月的社会保障资金缴存单据或社保机构开具的社会保险参保缴费情况证明。依法不需要缴纳社会保障资金的投标供应商应提供相关证明文件。	投标人应提交的相关资格证明材料
5	税收缴纳证明	提供递交投标文件截止之日前一年内任意一个月的依法缴纳税收的相关凭据（时间以税款所属日期为准、税种至少包含增值税或企业所得税），凭据应有税务机关或代收机关的公章或业务专用章。依法免税或无须缴纳税收的投标供应商，应提供相应证明文件。	投标人应提交的相关资格证明材料
6	近三年无重大违法、违纪书面声明	提供《近三年无重大违法、违纪书面声明》。	近三年无重大违法、违纪书面声明
7	信用记录	投标供应商未被列入“信用中国”网站记录的“失信被执行人”或“重大税收违法案件当事人”名单；不处于“中国政府采购网”记录的“政府采购严重违法失信行为记录名单”中的禁止参加政府采购活动期间。（以采购人或采购代理机构开标当天查询结果为准）；	投标人应提交的相关资格证明材料
8	控股管理关系	提供直接控股和管理关系清单。若与其他投标人存在单位负责人为同一人或者存在直接控股、管理关系的，则投标无效。	控股管理关系
9	法定代表人授权委托书	法定代表人参加投标的，须提供本人身份证复印件；法定代表人授权他人参加投标的，须提供法定代表人授权委托书。招标文件中凡是需要法定代表人盖章之处，非法人单位的负责人均参照执行。法人的分支机构参与投标时，除提供《法定代表人授权委托书》外，还须同时提供总公司给分支机构出具的授权书。	法定代表人授权书
10	本项目不接受联合体投标，不允许分包	投标供应商应提供《非联合体不分包投标声明》，视为独立投标，不分包。	非联合体不分包投标声明
11	特殊资格要求	具备《网络安全等级测评与检测评估机构服务认证证书》。	投标人应提交的相关资格证明材料

采购包4:

序号	资格审查要求概况	评审点具体描述	关联格式
1	营业执照等主体资格证明文件	提供有效存续的企业营业执照（副本）/事业单位法人证书/专业服务机构执业许可证/民办非企业单位登记证书。	投标人应提交的相关资格证明材料

2	财务状况报告	提供 2023 年度经审计的财务报告（成立时间至提交投标文件截止时间不足一年的可提供成立后任意时段的资产负债表），或其递交投标文件截止之日前三个月内基本开户银行出具的资信证明，或信用担保机构出具的投标担保函(以上三种形式的资料提供任何一种即可）。	投标人应提交的相关资格证明材料
3	书面声明	提供书面声明，包括声明具有履行合同所必需的设备和专业技术能力；未为本项目提供整体设计、规范编制或者项目管理、监理等服务。	书面声明
4	社保缴纳证明	提供递交投标文件截止之日前一年内任意一个月的社会保障资金缴存单据或社保机构开具的社会保险参保缴费情况证明。依法不需要缴纳社会保障资金的投标供应商应提供相关证明文件。	投标人应提交的相关资格证明材料
5	税收缴纳证明	提供递交投标文件截止之日前一年内任意一个月的依法缴纳税收的相关凭据（时间以税款所属日期为准、税种至少包含增值税或企业所得税），凭据应有税务机关或代收机关的公章或业务专用章。依法免税或无须缴纳税收的投标供应商，应提供相应证明文件。	投标人应提交的相关资格证明材料
6	近三年无重大违法、违纪书面声明	提供《近三年无重大违法、违纪书面声明》。	近三年无重大违法、违纪书面声明
7	信用记录	投标供应商未被列入“信用中国”网站记录的“失信被执行人”或“重大税收违法案件当事人”名单；不处于“中国政府采购网”记录的“政府采购严重违法失信行为记录名单”中的禁止参加政府采购活动期间。（以采购人或采购代理机构开标当天查询结果为准）；	投标人应提交的相关资格证明材料
8	控股管理关系	提供直接控股和管理关系清单。若与其他投标人存在单位负责人为同一人或者存在直接控股、管理关系的，则投标无效。	控股管理关系
9	法定代表人授权委托书	法定代表人参加投标的，须提供本人身份证复印件；法定代表人授权他人参加投标的，须提供法定代表人授权委托书。招标文件中凡是需要法定代表人盖章之处，非法人单位的负责人均参照执行。法人的分支机构参与投标时，除提供《法定代表人授权委托书》外，还须同时提供总公司给分支机构出具的授权书。	法定代表人授权书
10	本项目不接受联合体投标，不允许分包	投标供应商应提供《非联合体不分包投标声明》，视为独立投标，不分包。	非联合体不分包投标声明

11	特殊资格要求	具备国家密码管理部门同意其开展商用密码应用安全性评估的证明资料。	投标人应提交的相关资格证明材料
----	--------	----------------------------------	-----------------

采购包5:

序号	资格审查要求概况	评审点具体描述	关联格式
1	营业执照等主体资格证明文件	提供有效存续的企业营业执照（副本）/事业单位法人证书/专业服务机构执业许可证/民办非企业单位登记证书。	投标人应提交的相关资格证明材料
2	财务状况报告	提供2023年度经审计的财务报告（成立时间至提交投标文件截止时间不足一年的可提供成立后任意时段的资产负债表），或其递交投标文件截止之日前三个月内基本开户银行出具的资信证明，或信用担保机构出具的投标担保函(以上三种形式的资料提供任何一种即可)。	投标人应提交的相关资格证明材料
3	书面声明	提供书面声明，包括声明具有履行合同所必需的设备和专业技术能力；未为本项目提供整体设计、规范编制或者项目管理、监理等服务。	书面声明
4	社保缴纳证明	提供递交投标文件截止之日前一年内任意一个月的社会保障资金缴存单据或社保机构开具的社会保险参保缴费情况证明。依法不需要缴纳社会保障资金的投标供应商应提供相关证明文件。	投标人应提交的相关资格证明材料
5	税收缴纳证明	提供递交投标文件截止之日前一年内任意一个月的依法缴纳税收的相关凭据（时间以税款所属日期为准、税种至少包含增值税或企业所得税），凭据应有税务机关或代收机关的公章或业务专用章。依法免税或无须缴纳税收的投标供应商，应提供相应证明文件。	投标人应提交的相关资格证明材料
6	近三年无重大违法、违纪书面声明	提供《近三年无重大违法、违纪书面声明》。	近三年无重大违法、违纪书面声明
7	信用记录	投标供应商未被列入“信用中国”网站记录的“失信被执行人”或“重大税收违法案件当事人”名单；不处于“中国政府采购网”记录的“政府采购严重违法失信行为记录名单”中的禁止参加政府采购活动期间。（以采购人或采购代理机构开标当天查询结果为准）；	投标人应提交的相关资格证明材料
8	控股管理关系	提供直接控股和管理关系清单。若与其他投标人存在单位负责人为同一人或者存在直接控股、管理关系的，则投标无效。	控股管理关系

9	法定代表人授权委托书	法定代表人参加投标的，须提供本人身份证复印件；法定代表人授权他人参加投标的，须提供法定代表人授权委托书。招标文件中凡是需要法定代表人盖章之处，非法人单位的负责人均参照执行。法人的分支机构参与投标时，除提供《法定代表人授权委托书》外，还须同时提供总公司给分支机构出具的授权书。	法定代表人授权书
10	本项目不接受联合体投标，不允许分包	投标供应商应提供《非联合体不分包投标声明》，视为独立投标，不分包。	非联合体不分包投标声明
11	特殊资格要求	投标供应商须具备检验检测机构资质认定(CMA)证书或CNAS实验室认可证书。	投标人应提交的相关资格证明材料

采购包6:

序号	资格审查要求概况	评审点具体描述	关联格式
1	营业执照等主体资格证明文件	提供有效存续的企业营业执照（副本）/事业单位法人证书/专业服务机构执业许可证/民办非企业单位登记证书。	投标人应提交的相关资格证明材料
2	财务状况报告	提供2023年度经审计的财务报告（成立时间至提交投标文件截止时间不足一年的可提供成立后任意时段的资产负债表），或其递交投标文件截止之日前三个月内基本开户银行出具的资信证明，或信用担保机构出具的投标担保函(以上三种形式的资料提供任何一种即可)。	投标人应提交的相关资格证明材料
3	书面声明	提供书面声明，包括声明具有履行合同所必需的设备和专业技术能力；未为本项目提供整体设计、规范编制或者项目管理、检测等服务。	书面声明
4	社保缴纳证明	提供递交投标文件截止之日前一年内任意一个月的社会保障资金缴存单据或社保机构开具的社会保险参保缴费情况证明。依法不需要缴纳社会保障资金的投标供应商应提供相关证明文件。	投标人应提交的相关资格证明材料
5	税收缴纳证明	提供递交投标文件截止之日前一年内任意一个月的依法缴纳税收的相关凭据（时间以税款所属日期为准、税种至少包含增值税或企业所得税），凭据应有税务机关或代收机关的公章或业务专用章。依法免税或无须缴纳税收的投标供应商，应提供相应证明文件。	投标人应提交的相关资格证明材料
6	近三年无重大违法、违纪书面声明	提供《近三年无重大违法、违纪书面声明》。	近三年无重大违法、违纪书面声明

7	信用记录	投标供应商未被列入“信用中国”网站记录的“失信被执行人”或“重大税收违法案件当事人”名单；不处于“中国政府采购网”记录的“政府采购严重违法失信行为记录名单”中的禁止参加政府采购活动期间。（以采购人或采购代理机构开标当天查询结果为准）；	投标人应提交的相关资格证明材料
8	控股管理关系	提供直接控股和管理关系清单。若与其他投标人存在单位负责人为同一人或者存在直接控股、管理关系的，则投标无效。	控股管理关系
9	法定代表人授权委托书	法定代表人参加投标的，须提供本人身份证复印件；法定代表人授权他人参加投标的，须提供法定代表人授权委托书。招标文件中凡是需要法定代表人盖章之处，非法人单位的负责人均参照执行。法人的分支机构参与投标时，除提供《法定代表人授权委托书》外，还须同时提供总公司给分支机构出具的授权书。	法定代表人授权书
10	本项目不接受联合体投标，不允许分包	投标供应商应提供《非联合体不分包投标声明》，视为独立投标，不分包。	非联合体不分包投标声明

4.3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
无			

采购包2:

序号	资格审查要求概况	评审点具体描述	关联格式
无			

采购包3:

序号	资格审查要求概况	评审点具体描述	关联格式
无			

采购包4:

序号	资格审查要求概况	评审点具体描述	关联格式
无			

采购包5:

序号	资格审查要求概况	评审点具体描述	关联格式
无			

采购包6:

序号	资格审查要求概况	评审点具体描述	关联格式
----	----------	---------	------

无

第五章 评标办法

5.1 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》《政府采购货物和服务招标投标管理办法》等法律法规，结合采购项目特点制定本评标办法。

二、评标工作由代理机构负责组织，具体评标事务由采购人或代理机构依法组建的评标委员会负责。评标委员会由采购人代表和评审专家组成。

三、评标工作应遵循公平、公正、科学及择优的原则，并以相同的评标程序 and 标准对待所有的投标人。

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。评标委员会成员、采购人、代理机构和投标人应当按照本招标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标活动。

五、评标过程中的书面材料往来均通过项目电子化交易系统传递，投标人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，评标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、评标过程应当独立、保密，任何单位和个人不得非法干预评标活动。投标人非法干预评标活动的，其投标文件将作无效处理；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标活动的，将依法追究其责任。

5.2 评标委员会

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。

二、评标委员会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、推荐评标委员会组长。采购人代表可以使用采购人代表专用签章确认评审意见。

三、评标委员会成员获取解密后的投标文件，开展评标活动。出现应当回避的情形时，评标委员会成员应当主动回避；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投标文件，按规定重新组建评标委员会，解封投标文件后，开展评标活动。

四、评标委员会按照招标文件规定的评标程序、评标方法和标准进行评标，并独立履行下列职责：

- （一）熟悉和理解招标文件；
- （二）审查供应商投标文件等是否满足招标文件要求，并作出评价；
- （三）根据需要要求采购组织单位对招标文件作出解释；根据需要要求供应商对投标文件有关事项作出澄清、说明或者更正；
- （四）推荐中标候选供应商，或者受采购人委托确定中标供应商；
- （五）起草评标报告并进行签署；
- （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。

5.3 评标方法

采购包1：综合评分法

采购包2：综合评分法

采购包3：综合评分法

采购包4：综合评分法

采购包5：综合评分法

5.4 评标程序

5.4.1 熟悉和理解招标文件和停止评标

一、评标委员会正式评审前，应当对招标文件进行熟悉和理解，内容主要包括招标文件中供应商资格资质性要求、采购项目技术、服务和商务要求、评审方法和标准以及可能涉及签订政府采购合同的内容等。

二、本招标文件有下列情形之一的，评标委员会应当停止评标：

- （一）招标文件的规定存在歧义、重大缺陷的；
- （二）招标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，但是招标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，但是招标文件未依法体现促进中小企业发展相关规定的；
- （五）招标文件规定的评标方法是综合评分法、最低评标价法之外的评标方法，或者虽然名称为综合评分法、最低评标价法，但实际上不符合国家规定；
- （六）招标文件将投标人的资格条件列为评分因素的；
- （七）招标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标情形的，评标委员会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，评标委员会不得以任何方式和理由停止评标。

出现上述应当停止评标情形的，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。采购组织单位认为评标委员会不应当停止评标的，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。

5.4.2 符合性审查

评标委员会依据本招标文件的实质性要求，对符合资格的投标文件进行审查，以确定其是否满足本招标文件的实质性要求。本项目符合性审查事项，必须以本招标文件的明确规定的实质性要求作为依据。

在符合性审查过程中，如果出现评标委员会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招标文件规定。

符合性审查标准见下表（按以下顺序审查）：

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.在评标过程中，评标委员会认为投标人报价明显低于其他实质性响应的投标人报价，有可能影响产品质量或者不能诚信履约的，评标委员会应当要求其在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，逐项就投标人提供的货物、工程和服务的主营业务成本（应根据投标人企业类型予以区别）、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.投标人提交的相关说明和证明材料，应当加盖投标人（法定名称）电子印章，在评标委员会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。投标人不能证明其投标报价合理性的，评标委员会应当将其投标文件作为无效处理。</p>	开标一览表 标的清单
2	投标文件签署、盖章	均按招标文件要求签字、盖章（评分标准中要求提供的证明材料除外）。	开标一览表 技术偏离表 分项报价表 中小企业声明函 商务应答表 保证金汇款声明函、保函 控股管理关系 法定代表人授权书 投标人应提交的相关资格证明材料 近三年无重大违法、违纪书面声明 投标函 残疾人福利性单位声明函 服务方案 标的清单 非联合体不分包投标声明 投标文件封面 书面声明 监狱企业的证明文件
3	开标一览表	（1）投标报价符合唯一性要求；（2）开标一览表填写符合要求；（3）计量单位、报价货币均符合招标文件要求；（4）未超出采购预算或招标文件规定的最高限价。	开标一览表 标的清单
4	商务条款响应	完全理解接受招标文件商务条款。	商务应答表
5	投标保证金	保证金交纳符合招标文件要求。	保证金汇款声明函、保函

6	无其他招标文件或法规明确规定响应无效的事项	没有不符合招标文件规定的被视为无效响应的其他条款。	开标一览表 技术偏离表 分项报价表 中小企业声明函 商务应答表 保证金汇款声明函、保函 控股管理关系 法定代表人授权书 投标人应提交的相关资格证明材料 近三年无重大违法、违纪书面声明 投标函 残疾人福利性单位声明函 服务方案 标的清单 非联合体不分包投标声明 投标文件封面 书面声明 监狱企业的证明文件
---	-----------------------	---------------------------	---

采购包2:

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.在评标过程中，评标委员会认为投标人报价明显低于其他实质性响应的投标人报价，有可能影响产品质量或者不能诚信履约的，评标委员会应当要求其在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，逐项就投标人提供的货物、工程和服务的主营业务成本（应根据投标人企业类型予以区别）、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.投标人提交的相关说明和证明材料，应当加盖投标人（法定名称）电子印章，在评标委员会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。投标人不能证明其投标报价合理性的，评标委员会应当将其投标文件作为无效处理。</p>	开标一览表 标的清单

2	投标文件签署、盖章	均按招标文件要求签字、盖章（评分标准中要求提供的证明材料除外）。	开标一览表 技术偏离表 分项报价表 中小企业声明函 商务应答表 技术方案 保证金汇款声明函、保函 控股管理关系 法定代表人授权书 投标人应提交的相关资格证明材料 近三年无重大违法、违纪书面声明 投标函 残疾人福利性单位声明函 非联合体不分包投标声明 标的清单 投标文件封面 书面声明 监狱企业的证明文件
3	开标一览表	（1）投标报价符合唯一性要求；（2）开标一览表填写符合要求；（3）计量单位、报价货币均符合招标文件要求；（4）未超出采购预算或招标文件规定的最高限价。	开标一览表 标的清单
4	商务条款响应	完全理解接受招标文件商务条款。	商务应答表
5	投标保证金	保证金交纳符合招标文件要求。	保证金汇款声明函、保函
6	无其他招标文件或法规明确规定响应无效的事项	没有不符合招标文件规定的被视为无效响应的其他条款。	开标一览表 技术偏离表 分项报价表 中小企业声明函 商务应答表 技术方案 保证金汇款声明函、保函 控股管理关系 法定代表人授权书 投标人应提交的相关资格证明材料 近三年无重大违法、违纪书面声明 投标函 残疾人福利性单位声明函 标的清单 非联合体不分包投标声明 投标文件封面 书面声明 监狱企业的证明文件

采购包3:

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.在评标过程中，评标委员会认为投标人报价明显低于其他实质性响应的投标人报价，有可能影响产品质量或者不能诚信履约的，评标委员会应当要求其在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，逐项就投标人提供的货物、工程和服务的主营业务成本（应根据投标人企业类型予以区别）、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.投标人提交的相关说明和证明材料，应当加盖投标人（法定名称）电子印章，在评标委员会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。投标人不能证明其投标报价合理性的，评标委员会应当将其投标文件作为无效处理。</p>	开标一览表 标的清单
2	投标文件签署、盖章	均按招标文件要求签字、盖章（评分标准中要求提供的证明材料除外）。	开标一览表 分项报价表 中小企业声明函 商务应答表 保证金汇款声明函、保函 控股管理关系 法定代表人授权书 投标人应提交的相关资格证明材料 近三年无重大违法、违纪书面声明 投标函 残疾人福利性单位声明函 服务方案 标的清单 非联合体不分包投标声明 投标文件封面 书面声明 监狱企业的证明文件
3	开标一览表	（1）投标报价符合唯一性要求；（2）开标一览表填写符合要求；（3）计量单位、报价货币均符合招标文件要求；（4）未超出采购预算或招标文件规定的最高限价。	开标一览表 标的清单
4	商务条款响应	完全理解接受招标文件商务条款。	商务应答表
5	投标保证金	保证金交纳符合招标文件要求。	保证金汇款声明函、保函

6	无其他招标文件或法规明确规定响应无效的事项	没有不符合招标文件规定的被视为无效响应的其他条款。	开标一览表 分项报价表 中小企业声明函 商务应答表 保证金汇款声明函、保函 控股管理关系 法定代表人授权书 投标人应提交的相关资格证明材料 近三年无重大违法、违纪书面声明 投标函 残疾人福利性单位声明函 服务方案 非联合体不分包投标声明 标的清单 投标文件封面 书面声明 监狱企业的证明文件
---	-----------------------	---------------------------	---

采购包4:

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.在评标过程中，评标委员会认为投标人报价明显低于其他实质性响应的投标人报价，有可能影响产品质量或者不能诚信履约的，评标委员会应当要求其在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，逐项就投标人提供的货物、工程和服务的主营业务成本（应根据投标人企业类型予以区别）、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.投标人提交的相关说明和证明材料，应当加盖投标人（法定名称）电子印章，在评标委员会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。投标人不能证明其投标报价合理性的，评标委员会应当将其投标文件作为无效处理。</p>	开标一览表 标的清单

2	投标文件签署、盖章	均按招标文件要求签字、盖章（评分标准中要求提供的证明材料除外）。	开标一览表 分项报价表 中小企业声明函 商务应答表 保证金汇款声明函、保函 控股管理关系 法定代表人授权书 投标人应提交的相关资格证明材料 近三年无重大违法、违纪书面声明 投标函 残疾人福利性单位声明函 服务方案 标的清单 非联合体不分包投标声明 投标文件封面 书面声明 监狱企业的证明文件
3	开标一览表	（1）投标报价符合唯一性要求；（2）开标一览表填写符合要求；（3）计量单位、报价货币均符合招标文件要求；（4）未超出采购预算或招标文件规定的最高限价。	开标一览表 标的清单
4	商务条款响应	完全理解接受招标文件商务条款。	商务应答表
5	投标保证金	保证金交纳符合招标文件要求。	保证金汇款声明函、保函
6	无其他招标文件或法规明确规定响应无效的事项	没有不符合招标文件规定的被视为无效响应的其他条款。	开标一览表 分项报价表 中小企业声明函 商务应答表 保证金汇款声明函、保函 控股管理关系 法定代表人授权书 投标人应提交的相关资格证明材料 近三年无重大违法、违纪书面声明 投标函 残疾人福利性单位声明函 服务方案 标的清单 非联合体不分包投标声明 投标文件封面 书面声明 监狱企业的证明文件

采购包5:

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.在评标过程中，评标委员会认为投标人报价明显低于其他实质性响应的投标人报价，有可能影响产品质量或者不能诚信履约的，评标委员会应当要求其在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，逐项就投标人提供的货物、工程和服务的主营业务成本（应根据投标人企业类型予以区别）、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.投标人提交的相关说明和证明材料，应当加盖投标人（法定名称）电子印章，在评标委员会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。投标人不能证明其投标报价合理性的，评标委员会应当将其投标文件作为无效处理。</p>	开标一览表 标的清单
2	投标文件签署、盖章	均按招标文件要求签字、盖章（评分标准中要求提供的证明材料除外）。	开标一览表 分项报价表 中小企业声明函 商务应答表 保证金汇款声明函、保函 控股管理关系 法定代表人授权书 投标人应提交的相关资格证明材料 近三年无重大违法、违纪书面声明 投标函 残疾人福利性单位声明函 服务方案 标的清单 非联合体不分包投标声明 投标文件封面 书面声明 监狱企业的证明文件
3	开标一览表	（1）投标报价符合唯一性要求；（2）开标一览表填写符合要求；（3）计量单位、报价货币均符合招标文件要求；（4）未超出采购预算或招标文件规定的最高限价。	开标一览表 标的清单
4	商务条款响应	完全理解接受招标文件商务条款。	商务应答表
5	投标保证金	保证金交纳符合招标文件要求。	保证金汇款声明函、保函

6	无其他招标文件或法规明确规定响应无效的事项	没有不符合招标文件规定的被视为无效响应的其他条款。	开标一览表 分项报价表 中小企业声明函 商务应答表 保证金汇款声明函、保函 控股管理关系 法定代表人授权书 投标人应提交的相关资格证明材料 近三年无重大违法、违纪书面声明 投标函 残疾人福利性单位声明函 服务方案 标的清单 非联合体不分包投标声明 投标文件封面 书面声明 监狱企业的证明文件
---	-----------------------	---------------------------	---

采购包6:

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.在评标过程中，评标委员会认为投标人报价明显低于其他实质性响应的投标人报价，有可能影响产品质量或者不能诚信履约的，评标委员会应当要求其在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，逐项就投标人提供的货物、工程和服务的主营业务成本（应根据投标人企业类型予以区别）、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.投标人提交的相关说明和证明材料，应当加盖投标人（法定名称）电子印章，在评标委员会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。投标人不能证明其投标报价合理性的，评标委员会应当将其投标文件作为无效处理。</p>	开标一览表 标的清单

2	投标文件签署、盖章	均按招标文件要求签字、盖章（评分标准中要求提供的证明材料除外）。	开标一览表 分项报价表 中小企业声明函 商务应答表 保证金汇款声明函、保函 控股管理关系 法定代表人授权书 投标人应提交的相关资格证明材料 近三年无重大违法、违纪书面声明 投标函 残疾人福利性单位声明函 服务方案 非联合体不分包投标声明 标的清单 投标文件封面 书面声明 监狱企业的证明文件
3	开标一览表	（1）投标报价符合唯一性要求；（2）开标一览表填写符合要求；（3）计量单位、报价货币均符合招标文件要求；（4）未超出采购预算或招标文件规定的最高限价。	开标一览表 标的清单
4	商务条款响应	完全理解接受招标文件商务条款。	商务应答表
5	投标保证金	保证金交纳符合招标文件要求。	保证金汇款声明函、保函
6	无其他招标文件或法规明确规定响应无效的事项	没有不符合招标文件规定的被视为无效响应的其他条款。	开标一览表 分项报价表 中小企业声明函 商务应答表 保证金汇款声明函、保函 控股管理关系 法定代表人授权书 投标人应提交的相关资格证明材料 近三年无重大违法、违纪书面声明 投标函 残疾人福利性单位声明函 服务方案 标的清单 非联合体不分包投标声明 投标文件封面 书面声明 监狱企业的证明文件

以上实质性要求全部响应并满足采购需求的，则通过符合性审查；如有任意一项未响应或不满足采购需求的，则按无效投标文件处理。如果评标委员会认为投标人有任意一项不通过的，应在符合性审查表中载明不通过的具体原因。

5.4.3解释、澄清有关问题

一、评标过程中，评标委员会认为招标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招标文件的原义或者影响公平、公正，解释事项如果涉及投标人权益的以有利于投标人的原则进行解释。

二、对投标文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，评标委员会应当要求投标人作出必要的澄清、说明或更正，并给予投标人必要的反馈时间。投标人应当按评标委员会的要求进行澄清、说明或者更正。投标人的澄清、说明或者更正不得超出投标文件的范围或者改变投标文件的实质性内容。澄清、说明或者更正不影响投标文件的效力，有效的澄清、说明或者更正材料是投标文件的组成部分。

三、投标人的澄清、说明或者更正需进行电子签章，应当不超出投标文件的范围、不实质性改变投标文件的内容、不影响投标人的公平竞争、不导致投标文件从不应响应招标文件变为响应招标文件的条件。下列内容不得澄清：

- （一）投标人投标文件中不应响应招标文件规定的技术参数指标和商务应答；
- （二）投标人投标文件中未提供的证明其是否符合招标文件资格、符合性规定要求的相关材料。
- （三）投标人投标文件中的材料因印刷、影印等不清晰而难以辨认的。

四、投标文件报价出现下列情况的，按以下原则处理：

- （一）投标文件中开标一览表（报价表）内容与投标文件中相应内容不一致的，以开标一览表（报价表）为准；
- （二）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；
- （三）单价金额小数点或者百分比有明显错位的，以开标一览表总价为准，并修改单价；
- （四）总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。

同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的报价经投标人确认后产生约束力，投标人不确认的，其投标无效。

五、对不同语言文本投标文件的解释发生异议的，以中文文本为准。

六、代理机构宣布评标结束前，投标人应通过项目电子化交易系统随时关注评标消息提示，及时响应评标委员会发出的澄清、说明或更正要求。投标人未能及时响应的，自行承担不利后果。

评标委员会应当积极履行澄清、说明或者更正的职责，不得滥用权力。

5.4.4比较与评价

评标委员会应当按照招标文件规定的评标细则及标准，对符合性检查合格的投标文件进行商务和技术评估，综合比较和评价。

5.4.5复核

评分汇总结束后，评标委员会应当进行复核，对拟推荐为中标候选人、报价最低、投标文件被认定为无效等进行重点复核。

评标结果汇总完成后，评标委员会拟出具评标报告前，代理机构应当组织不少于2名工作人员，在采购监督人员的监督之下，依据有关的法律制度和招标文件对评标结果进行复核，出具复核报告。

评标结果汇总完成后，除下列情形外，任何人不得修改评标结果：

- （一）分值汇总计算错误的；
- （二）分项评分超出评分标准范围的；
- （三）评标委员会成员对客观评审因素评分不一致的；
- （四）经评标委员会认定评分畸高、畸低的。

评标报告签署前，经复核发现存在以上情形之一的，评标委员会应当当场修改评标结果，并在评标报告中记载；评标报告签署后，采购人或者代理机构发现存在以上情形之一的，应当组织原评标委员会进行重新评审，重新评审改变评标结果的，书面报告本级财政部门。

5.4.6确定中标候选人名单

采购包1：按投标人综合得分从高到低进行排序，确定3名中标候选人。综合得分相同的，按投标报价由低到高顺序排列；得分且投标报价相同的，按投标人提供的优先采购产品认证证书数量由多到少顺序排列；得分且投标报价且提供的优先采

购产品认证证书数量相同的并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。

采购包2：按投标人综合得分从高到低进行排序，确定3名中标候选人。综合得分相同的，按投标报价由低到高顺序排列；得分且投标报价相同的，按投标人提供的优先采购产品认证证书数量由多到少顺序排列；得分且投标报价且提供的优先采购产品认证证书数量相同的并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。

采购包3：按投标人综合得分从高到低进行排序，确定3名中标候选人。综合得分相同的，按投标报价由低到高顺序排列；得分且投标报价相同的，按投标人提供的优先采购产品认证证书数量由多到少顺序排列；得分且投标报价且提供的优先采购产品认证证书数量相同的并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。

采购包4：按投标人综合得分从高到低进行排序，确定3名中标候选人。综合得分相同的，按投标报价由低到高顺序排列；得分且投标报价相同的，按投标人提供的优先采购产品认证证书数量由多到少顺序排列；得分且投标报价且提供的优先采购产品认证证书数量相同的并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。

采购包5：按投标人综合得分从高到低进行排序，确定3名中标候选人。综合得分相同的，按投标报价由低到高顺序排列；得分且投标报价相同的，按投标人提供的优先采购产品认证证书数量由多到少顺序排列；得分且投标报价且提供的优先采购产品认证证书数量相同的并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。

采购包6：按投标人综合得分从高到低进行排序，确定3名中标候选人。综合得分相同的，按投标报价由低到高顺序排列；得分且投标报价相同的，按投标人提供的优先采购产品认证证书数量由多到少顺序排列；得分且投标报价且提供的优先采购产品认证证书数量相同的并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。

5.4.7编写评标报告

评标报告是评标委员会根据全体评标成员签字的评标记录和评标结果编写的报告，其主要内容包括：

- 一、招标公告刊登的媒体名称、开标日期和地点；
- 二、投标人名单和评标委员会成员名单；
- 三、评标方法和标准；
- 四、开标记录和评标情况及说明，包括投标无效投标人名单及原因；
- 五、评标结果，确定的中标候选人名单或者经采购人委托直接确定的中标人；
- 六、其他需要说明的情况，包括评标过程中投标人根据评标委员会要求进行的澄清、说明或者更正，评标委员会成员的更换等；
- 七、报价最高的投标人为中标候选人的，评标委员会应当对其报价的合理性予以特别说明。

评标委员会成员应当在评标报告中签字或加盖电子签章确认，对评标过程和结果有不同意见的，应当在评标报告中写明并说明理由。签字但未写明不同意见或者未说明理由的，视同无意见。拒不签字或加盖电子签章又未另行说明其不同意见和理由的，视同同意评标结果。

5.5评标争议处理规则

评标委员会在评标过程中，对于符合性审查、对投标人文件作无效投标处理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，但不得违背法律法规和招标文件规定。持不同意见的评标委员会成员应当在评标报告上签署不同意见及理由，否则视为同意评标报告。持不同意见的评标委员会成员认为认定过程和结果不符合法律法规或者招标文件规定的，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。

5.6评标细则及标准

一、评标委员会只对通过资格审查的投标文件，根据招标文件的要求采用相同的评标程序、评分办法及标准进行评价和比较。

二、评标委员会成员应依据招标文件规定的评分标准和方法独立评审。

5.6.1评分办法

（综合评分法适用）采用综合评分法的，由评标委员会各成员对通过资格检查和符合性审查的投标人的投标文件进行独立评审。

投标报价得分=（评标基准价 / 投标报价）×100

评标总得分=F1×A1+F2×A2+.....+Fn×An

F1、F2.....Fn分别为各项评审因素的得分；

A1、A2、.....An 分别为各项评审因素所占的权重（A1+A2+.....+An=1）。

评标过程中，不得去掉报价中的最高报价和最低报价。

因落实政府采购政策进行价格调整的，以调整后的价格计算评标基准价和投标报价。

5.6.2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
	需求理解	投标人提供的项目技术方案对现状及需求分析准确充分、系统建设重点了解透彻、系统功能模块描述准确，满足陕西省公安机关执法办案综合管理平台建设项目建设需要。对本项目需求进行分析，分析全面详细、科学合理、重难点清晰准确、针对性强的得3分； 分析较全面、基本合理、重难点分析较准确、有一定针对性的得2分； 分析缺漏、不合理、重难点分析不够准确、无针对性的得1分； 不提供需求分析不得分。	3.0000	主观	商务应答表 服务方案
	技术指标	服务内容 & 标准要求需提供技术偏离表，并对技术指标逐条响应。全部满足得10分，每一项带▲项指标不满足或不能提供足够证明材料的扣1分，扣完为止。	10.0000	客观	技术偏离表 商务应答表 服务方案

项目整体方案	<p>投标人根据系统建设需求理解，从平台架构、系统集成等方面，对整个项目进行整体方案设计，包括应用软件开发、能力集成等设计方案，并提供系统架构图，满足业务需求；制定的项目整体设计方案需符合公安部相关规范性技术文件要求，并按照实际实施需求，进行重组整合、深化设计。整体方案好，完全满足本项目建设要求，且系统各功能设计和系统性能优于招标需求，得3分；整体方案一般，基本满足本项目建设要求，且系统各功能设计和系统性能与招标需求基本相当，得2分；整体方案差，部分满足本项目建设要求，且系统各功能设计和系统性能与招标需求部分相当，得1分；整体方案极差，无法满足本项目建设要求，或未提供设计方案的不得分。</p>	3.0000	主观	商务应答表 服务方案
数据标准化和迁移方案	<p>根据陕西省公安厅信息化需求，提供采购人本次系统建设相关历史数据标准化和迁移方案，方案合理，并能结合业务系统提供充分说明的得3分；数据标准化和迁移方案一般，并能结合业务系统提供较充分说明的得2分；数据标准化和迁移方案不够合理或未能结合业务提供说明的得1分；不提供不得分。</p>	3.0000	主观	商务应答表 服务方案 技术偏离表
数据共享交换	<p>根据陕西省公安厅信息化需求，提供采购人本次系统建设数据交换共享方案，包含：交换软件设计、内外部数据资源共享内容及方式，整体方案合理，并能结合业务系统提供充分说明的得3分；数据共享交换方案一般，并能结合业务系统提供较充分说明的得2分；数据共享交换方案不够合理或未能结合业务提供说明的得1分；不提供不得分。</p>	3.0000	主观	商务应答表 服务方案 技术偏离表

政法协同	根据陕西省公安厅信息化需求，结合执法办案综合管理平台项目业务目标：实现政法跨部门协同办案，提供公安侧涵盖政法协同新建流程及流程节点设计方案；方案合理，方案中应提供业务流程图、流程节点明细表，并能结合业务系统提供充分说明的得 3 分；方案一般，并能结合业务系统提供较充分说明的得 2 分；方案不够合理或未能结合业务提供说明的得 1 分；不提供不得分。	3.0000	主观	商务应答表 服务方案 技术偏离表
案件办理	投标人对案件办理模块进行详细的功能；提供详细设计方案，方案功能设计能够深入理解系统的功能要求，完全满足业务需求，得 3 分；方案一般，功能设计描述基本清晰基本完备的得 2 分；方案不够合理不够详细的得 1 分；不提供不得分。	3.0000	主观	商务应答表 服务方案 技术偏离表
智能电子卷宗	投标人对智能电子卷宗模块进行详细的功能；提供详细设计方案，方案功能设计能够深入理解系统的功能要求，完全满足业务需求，得 3 分；方案一般，功能设计描述基本清晰基本完备的得 2 分；方案不够合理不够详细的得 1 分；不提供不得分。	3.0000	主观	技术偏离表 商务应答表 服务方案
执法办案管理中心	投标人对执法办案管理中心模块进行详细的功能；提供详细设计方案，方案功能设计能够深入理解系统的功能要求，完全满足业务需求，得 3 分；方案一般，功能设计描述基本清晰基本完备的得 2 分；方案不够合理不够详细的得 1 分；不提供不得分。	3.0000	主观	技术偏离表 商务应答表 服务方案

智能笔录	<p>投标人对智能笔录模块进行详细的功能；提供详细设计方案，方案功能设计能够深入理解系统的功能要求，完全满足业务需求，得3分；</p> <p>方案一般，功能设计描述基本清晰基本完备的得2分； 方案不够合理不够详细的得1分； 不提供不得分。</p>	3.0000	主观	技术偏离表 商务应答表 服务方案
执法监督	<p>投标人对执法监督模块进行详细的功能；提供详细设计方案，方案需包含预警管理、执法考评管理及统计，功能设计能够深入理解系统的功能要求，完全满足业务需求，得3分； 方案一般，功能设计描述基本清晰基本完备的得3分； 方案不够合理不够详细的得1分； 不提供不得分。</p>	3.0000	主观	技术偏离表 商务应答表 服务方案
违法犯罪人员信息系统建设方案	<p>根据陕西省公安厅信息化需求，结合违法犯罪人员信息系统业务目标：实现政法跨部门协同办案，提供监管侧政法协同新建及升级改造流程和流程节点设计方案。方案合理，方案中应提供业务流程图、流程节点明细表，并能结合业务系统提供充分说明的得3分； 方案一般，并能结合业务系统提供较充分说明的得2分； 方案不够合理或未能结合业务提供说明的得1分； 不提供不得分。</p>	3.0000	主观	商务应答表 服务方案 技术偏离表
	<p>投标人需根据演示要求进行系统功能演示，全部满足演示要求的得16分，某项演示功能不全或演示内容不符合业务需求的扣分，扣完为止。</p> <p>演示要求如下： 1、行政处罚决定书开具：系统支持通过选择处罚裁量情形等处罚依据、条件自动生成处罚意见（包含单处、并处、可以并处等多种类型）及处罚结果。</p> <p>（1）演示通过行政处罚选择器选择处罚裁量情形等处罚依据得1</p>			

详细评审	系统功能演示	<p>分；（2）演示根据处罚依据、条件自动生成处罚意见（包含单处、并处、可以并处等多种类型）得2分；（3）演示根据处罚依据、处罚意见自动生成处罚结果得1分。</p> <p>2、预警闭环：实现预警问题签收、反馈、确认反馈、提级核销、问题重启、责任追究等业务功能。（1）演示预警问题签收、反馈、确认反馈功能得1分；（2）演示预警闭环的提级核销功能得1分；（3）演示预警闭环的问题重启功能得1分；（4）演示预警闭环责任追究功能得1分；</p> <p>3、执法办案管理中心：基于办案区相关业务数据实现执法办案系统与监管系统送拘送押业务协同办理。（1）演示在政法协同办案系统案件中同步办案区人员至案件嫌疑人得1分；（2）演示在案件中对嫌疑人发起送拘送押业务，支持上传体检信息并同步办案区人员信息采集信息得2分；（3）演示违法犯罪人员信息系统接收政法协同办案系统推送的送拘送押人员信息得1分。</p> <p>4、违法犯罪人员信息预警：可动态配置预警信息项目，项目包含本次建设相关预警信息，可以通过预警信息实现多级钻取，最终能查看人员档案，并对该人员进行业务办理。（1）演示可动态配置本次建设相关预警信息功能得1分；（2）演示通过预警信息实现多级钻取和最终能查看人员档案的功能得2分；（3）演示钻取查看人员档案后支持对人员进行业务办理的功能得1分。</p> <p>注：演示通过在线视频会议软件线上进行双路视频演示，演示时间20分钟。</p>	16.0000	客观	商务应答表 服务方案
------	--------	---	---------	----	---------------

项目实施方案	<p>方案描述清晰、整体结构设计科学合理、针对性强具备可实施性，有针对性的细化方案，系统建设目标清晰明了，能全面涵盖项目总体要求，项目建设重点、难点分析透彻，工期、人员安排合理、保障45天内完成系统实施及可以上线试运行的得4分；方案描述较清晰，整体结构设计较合理，工期、实施人员安排较合理、保障60天内完成系统实施及可以上线试运行的得2分；方案描述基本清晰，整体结构设计基本可行，工期、实施人员安排相对合理、保障90天内完成系统实施及可以上线试运行的得1分；方案描述不清晰，整体结构设计难以实施，工期、实施人员安排不合理或无实施方案的不得分。</p>	4.0000	主观	商务应答表 服务方案
运维服务方案	<p>根据采购人要求编制运维服务方案（包括但不限于：运维团队安排、故障响应时间、保障计划等，以及有利于采购人的其他服务措施）：运维服务方案完整详细、运维团队人员充足且构成合理、有完善的保障计划、故障响应时间能满足需求、并提供本地运维服务的得3分；运维服务方案较为完整、运维团队人员较为充足、构成基本合理、有基本保障计划、故障响应时间能满足需求得2分；运维服务方案有缺漏、运维团队人员不足、缺乏基本的服务保障计划、故障响应时间基本满足需求，得1分；未提供运维服务方案不得分。</p>	3.0000	主观	商务应答表 服务方案

培训方案	根据招标要求编制详细培训方案（包含但不限于：培训人员情况、培训内容、培训时间）：培训内容完整详细、培训时长充足、有成熟的培训材料和课程安排的得3分；培训内容较完整、培训时长基本满足要求、已具备一定的材料和课程安排的得2分；培训内容有缺漏、培训时长不足、不具备现有的培训材料和课程安排得1分；不提供培训方案不得分。	3.0000	主观	商务应答表 服务方案
业绩	<p>（1）供应商提供2021年1月1日至今（以合同签订时间为准）具备本项目的省级平台类似业绩证明材料，业绩证明材料以合同+付款发票+验收证明为准（提供材料不全不得分），每份计1分，最高计3分。</p> <p>（2）供应商提供2021年1月1日至今（以合同签订时间为准）具备本项目的地市级平台类似业绩证明材料，业绩证明材料以合同+付款发票+验收证明为准（提供材料不全不得分），每份计1分，最高计2分。未提供不得分。</p>	5.0000	客观	商务应答表 服务方案
项目经理	项目经理具有国家人社部门认定的相关专业高级职称，并具备至少五年（2019年1月至开标当日）同类项目工作经验（提供职称证书复印件、个人简历和就职于投标单位的社保缴纳证明），同时提供的，得3分，否则不得分。	3.0000	客观	商务应答表 服务方案

	项目团队	项目实施团队（不包含项目经理）不少于 60 人，须提供人员清单、工作简历及就职于投标单位的社保缴纳证明，否则“项目团队人员”整体不得分；在此基础上：（1）项目实施团队（不包含项目经理）人员，具有信息系统项目管理师、系统分析师、系统架构设计师，每提供 1 个证书复印件得 1 分，最多得 3 分；（2）项目实施团队（不包含项目经理）人员，具有软件设计师、软件测评师、信息安全工程师、数据库系统工程师、信息系统管理工程师资格证书的，每提供 1 个证书复印件得 1 分，最多得 5 分。（同一人提供多个证书复印件的，不重复计分）	8.0000	客观	商务应答表 服务方案
	供应商服务实施能力	（1）供应商具有质量管理体系认证证书，得 1 分；（2）供应商具有信息技术服务管理体系认证证书，得 1 分；（3）供应商具有信息安全管理体系统认证证书，得 1 分（4）供应商具有ITSS证书，得 1 分；（5）供应商具有涉密信息系统集成服务证书（乙级）及以上，得 1 分；	5.0000	客观	商务应答表 服务方案
价格分	价格分	价格分统一采用低价优先法计算，即满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他投标供应商的价格分统一按照下列公式计算：投标报价得分= $(\text{评标基准价} / \text{投标报价}) \times 100$ 计算分数时四舍五入取小数点后两位。	10.0000	客观	开标一览表 标的清单

价格扣除

序号	情形	适用对象	比例	说明	关联格式
----	----	------	----	----	------

1	小型、微型企业，监狱企业，残疾人福利性单位	投标人或联合体成员均为小型、微型企业	10.0000 %	对于经主管预算单位统筹后未预留份额专门面向中小企业采购的采购项目，以及预留份额项目中的非预留部分采购包，对符合《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）规定的小微企业报价给予C1的扣除，用扣除后的价格参加评审。承接本项目的供应商符合相应条件时，给予C1的价格扣除，即：评标价=最后报价×（1-C1）；监狱企业与残疾人福利性单位视同小型、微型企业，享受同等价格扣除，当企业属性重复时，不重复价格扣除	开标一览表 中小企业声明函 残疾人福利性单位声明函 标的清单 监狱企业的证明文件
---	-----------------------	--------------------	-----------	--	--

采购包2:

评审因素		评审标准			
分值构成		详细评审70.0000分 报价得分30.0000分			
评审因素分类	评审项	详细描述	分值	客观/主观	关联格式

	技术指标	投标人所投产品的技术指标，参数完全满足招标文件规定相应技术指标、参数的得 45 分； 低于招标文件规定相应技术指标、参数的证明材料无法提供的；带▲项（重要技术指标）不满足的，每有一项减 2 分；非带▲项（一般技术指标）不满足的，每有一项减 1 分，扣完为止。注： 1、标★条款为实质性响应条款，负偏离或未响应按废标处理； 2、部分满足该技术指标的按不满足处理。	45.0000	客观	技术方案 商务应答表 技术偏离表
	类似业绩	投标人提供 2022年1月1日 至今类似规模类似项目业绩，每提供一个得 1 分，最高得 5 分。注：需提供合同（包含合同首页、关键内容页及签署页）复印件并加盖本单位公章有效证明文件。不符合上述要求或未按要求提供有效证明文件的业绩在评审时不得分。	5.0000	客观	商务应答表 技术方案
	方案完整性	根据对项目内容范围的理解以及实施方案、工作思路等阐述情况，专家提问答疑情况、服务承诺情况的完整性、科学性、专业性进行横向比较，综合评价。阐述范围必须包括：现状描述、风险分析、解决方案、方案价值： 1、针对技术设计方案的兼容性、合理性和科学性进行横向比较，方案内容完整无缺项，与项目需求相关具有针对性得 5 分； 2、方案无重大缺项，方案内容与需求相关，具有一定的可行性和合理性，得 3 分； 3、方案缺项较多，未能准确描述方案内容，得 1 分； 4、其他情形不得分。	5.0000	主观	商务应答表 技术方案

详细评审	产品实力	1、可信云认证：为保障云平台在自主可控的持续演进和管理能力，要求云平台在支持鲲鹏、飞腾、海光服务器的多芯架构下，云平台在供应链采购、规章制度、平台建设、稳定性故障演练、安全运行等平台韧性上满足业务稳定性成熟度模型评估，提供第三方专业测试机构证明材料，并加盖原厂商公章得2分。其他情形不得分； 2、为满足自主可控要求，所投云平台和大数据库产品应支持符合名录的操作系统（银河麒麟、统信UOS等）以及全自研国产数据库，提供证明材料并加盖原厂商公章得2分。其他情形不得分。	4.0000	客观	技术方案 商务应答表
	售后服务	1、投标人提供所有产品生产厂家的针对此项目提供原厂授权书和售后服务承诺函的得2分，未提供或提供不全的不得分； 2、根据项目实际需求提供售后服务方案：（1）售后服务范围和响应时间故障处理；（2）补救措施和定期回访及维护；（3）突发事件和重大活动应急保障能力，具有本地化服务团队。根据提供方案的完整性和可实施性进行打分，方案内容完整无缺项，与项目需求相关具有针对性得3分； 项目实施方案无重大缺项，方案内容与需求相关，具有一定的可行性和合理性，得1分； 其他情形不得分。	5.0000	主观	商务应答表 技术方案

	保密	投标人应承诺不得泄露采购单位一切敏感信息，包括但不限于技术情报、技术资料、商业秘密和商业信息等，提供保密措施方案，内容应包括：（1）保密管理制度和规章制度；（2）人员保密规划；（3）保密应急三个方面分别阐述。内容全面、符合本项目要求得3分；内容简单、不完全符合或有缺失不得分。	3.0000	主观	技术方案 商务应答表
	项目团队	1、投标人项目经理具有高级信息系统项目管理师证书及8年以上的工作经验，得1分； 2、投标人针对本项目人员配备投入情况（主要专业技术管理人员及项目组成员），项目团队有明确的组织形式、团队人员具有相关资质证书：高级系统架构师、高级信息系统项目管理师、高级工程师（通信或计算机类）、网络工程师、cisp注册信息安全工程师。全部齐备得2分，缺项或者未提供不得分。 以上证明文件要求提供证书复印件和2024年近三个月的社保缴纳证明复印件。（项目团队成员若一人持多种证书，不重复计算，需提供相关证书复印件、近三个月社保证明复印件并加盖投标人公章）	3.0000	客观	商务应答表 技术方案
价格分	价格分	价格分统一采用低价优先法计算，即满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他投标供应商的价格分统一按照下列公式计算：投标报价得分=(评标基准价 / 投标报价)×100计算分数时四舍五入取小数点后两位。	30.0000	客观	开标一览表 标的清单

价格扣除

序号	情形	适用对象	比例	说明	关联格式
----	----	------	----	----	------

1	小型、微型企业，监狱企业，残疾人福利性单位	投标人或联合体成员均为小型、微型企业	10.0000 %	对于经主管预算单位统筹后未预留份额专门面向中小企业采购的采购项目，以及预留份额项目中的非预留部分采购包，对符合《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）规定的小微企业报价给予C1的扣除，用扣除后的价格参加评审。承接本项目的供应商符合相应条件时，给予C1的价格扣除，即：评标价=最后报价×（1-C1）；监狱企业与残疾人福利性单位视同小型、微型企业，享受同等价格扣除，当企业属性重复时，不重复价格扣除	开标一览表 中小企业声明函 残疾人福利性单位声明函 标的清单 监狱企业的证明文件
---	-----------------------	--------------------	-----------	--	--

采购包3:

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	提供2021年1月1日至今的同类业绩合同，每提供1份业绩得2分，最高得10分。须提供业绩合同复印件或扫描件，不提供不得分。	10.0000	客观	商务应答表 服务方案

详细评审	人员团队配备方案	<p>投标人针对本项目的实施组织机构、人员安排等，有具体的方案。项目团队人数及专业能力满足招标文件要求，能确保项目顺利实施。 1、方案全面完整、切实可行、满足本项目实际需求得20分； 2、方案全面完整、可行性较高、基本满足本项目实际需求得15分； 3、方案基本完整、可行性较低得10分； 4、方案不完整、可行性低得5分； 5、缺项或无实质性响应内容不得分。</p>	20.0000	主观	商务应答表 服务方案
	测评实施方案	<p>测评实施方案应包含项目需求分析、技术服务方案、实施进度及人员安排等内容；应根据本项目实际需求情况，对本项目进行全面、准确、细致的需求分析，并针对服务内容进行综合描述，针对技术服务部分应依据国家等级保护2.0测评标准体系要求，并结合招标方要求，方案内容完整，应包括基线测评、漏洞扫描、渗透测试部分，且方案描述详细，测评指标选取合理，测评内容及方法明确，服务条理清晰，满足技术规范书要求；项目实施进度计划合理、项目执行过程管控到位、项目风险分析及处置措施完善、合理、指导性强： 1、针对测评实施方案的合理性和科学性进行横向比较，方案内容完整无缺项，与项目需求相关具有针对性得20分； 2、方案无重大缺项，方案内容与需求相关，具有一定的可行性和合理性，得15分； 3、方案缺项较多，未能准确描述方案内容，得5分； 4、其他情形不得分。</p>	20.0000	主观	商务应答表 服务方案

	风险管理和应急处置方案	<p>为防止项目实施中出现突发应急事件，服务方应在本次项目中提供风险管理和应急处置方案，以应对突发事件出现后可迅速解决，防止给采购人信息系统带来影响，提高采购人应对安全突发事件的处置能力。</p> <p>1.方案全面完整、切实可行、满足本项目实际需求得10分； 2.方案全面完整、可行性较高、基本满足本项目实际需求得6分； 3.方案基本完整、可行性较低得2分； 4.缺项或无实质性响应内容不得分。</p>	10.0000	主观	商务应答表 服务方案
	项目质量管控措施	<p>针对本项目具有严格的项目质量管控措施，过程控制及监控手段，能保证技术人员按照相应的操作指导规范实施测评。</p> <p>1、措施全面完整、切实可行、满足本项目实际需求得10分； 2、措施全面完整、可行性较高、基本满足本项目实际需求得7分； 3、措施基本完整、可行性较低得4分； 4、缺项或无实质性响应内容不得分。</p>	10.0000	主观	商务应答表 服务方案
	项目实施进度管理	<p>针对项目实施进度具有科学合理安排，进度安排科学紧凑，按照方案响应程度赋分。</p> <p>1、方案全面完整、切实可行、满足本项目实际需求得10分； 2、方案全面完整、可行性较高、基本满足本项目实际需求得7分； 3、方案基本完整、可行性较低得4分； 4、方案不完整、可行性低得1分； 5、缺项或无实质性响应内容不得分。</p>	10.0000	主观	商务应答表 服务方案

	售后服务	服务商应提供完善的售后服务，包括不限于安全咨询服务、安全培训服务、漏洞扫描服务、安全巡检等服务内容，能提供售后服务并做出相应说明。1、方案全面完整、切实可行、满足本项目实际需求得10分；2、方案全面完整、可行性较高、基本满足本项目实际需求得6分；3、方案基本完整、可行性较低得2分；4、缺项或无实质性响应内容不得分。	10.0000	主观	商务应答表 服务方案
价格分	价格分	价格分统一采用低价优先法计算，即满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他投标供应商的价格分统一按照下列公式计算：投标报价得分=(评标基准价 / 投标报价)×100计算分数时四舍五入取小数点后两位。	10.0000	客观	开标一览表 标的清单

价格扣除

序号	情形	适用对象	比例	说明	关联格式
----	----	------	----	----	------

1	小型、微型企业，监狱企业，残疾人福利性单位	投标人或联合体成员均为小型、微型企业	10.0000%	对于经主管预算单位统筹后未预留份额专门面向中小企业采购的采购项目，以及预留份额项目中的非预留部分采购包，对符合《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）规定的小微企业报价给予C1的扣除，用扣除后的价格参加评审。承接本项目的供应商符合相应条件时，给予C1的价格扣除，即：评标价=最后报价×（1-C1）；监狱企业与残疾人福利性单位视同小型、微型企业，享受同等价格扣除，当企业属性重复时，不重复价格扣除	开标一览表 中小企业声明函 残疾人福利性单位声明函 标的清单 监狱企业的证明文件
---	-----------------------	--------------------	----------	--	--

采购包4:

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

	人员团队配备方案	<p>投标人针对本项目的实施组织机构、人员安排等，有具体的方案。项目团队人数及专业能力满足招标文件要求，能确保项目顺利实施。1、方案全面完整、切实可行、满足本项目实际需求得20分；2、方案全面完整、可行性较高、基本满足本项目实际需求得15分；3、方案基本完整、可行性较低得10分；4、方案不完整、可行性低得5分；5、缺项或无实质性响应内容不得分。</p>	20.0000	主观	商务应答表 服务方案
	业绩	<p>供应商提供近三年（合同签订日期自2021年1月1日至今）已完成同类型成功案例。每个1分，最高得3分。提供的证明材料均不得遮挡涂黑，否则不予认定加分。项目业绩须提供有效的相关证明资料，未提供或提供不全的不得分。具体要求如下：①合同复印件，包括甲乙双方名称及盖章、服务内容、签订日期；②用户盖章的验收报告复印件。</p>	3.0000	客观	商务应答表 服务方案

项目测评方案	对投标供应商提供的针对本项目的测评方案进行综合评价，根据响应程度进行打分，具体标准如下： 1 、项目测评方案专业性强，对系统现状及需求理解准确，方案科学、合理，内容完整、可靠性强，实施方法和技术措施的可操作性和有效性强，完全满足招标文件要求，得 10分 ； 2 、项目测评方案专业性较好，对系统现状及需求理解较为准确，方案较为科学、合理，内容较为完整、可靠性较强，实施方法和技术措施的可操作性和有效性较好，较好满足招标文件要求，得 8分 ； 3 、项目测评方案专业性一般，对系统现状及需求理解一般，方案一般，内容一般，实施方法和技术措施基本得当，基本满足招标文件要求，得 6分 ； 4 、未提供方案或项目整体方案专业性较差的、存在重要缺陷，得 0分 。	10.0000	主观	商务应答表 服务方案
项目测评环境评价	对投标供应商为本项目配备的测评环境进行综合评价，按照响应程度赋分，具体标准如下： 1 、供应商针对本项目配有较为完善的测评环境，配备密评网络抓包、密码算法、协议分析工具、随机数检测工具以及常用密码设备，具有模拟以及验证被测评系统密码应用方案的能力，得 10分 ； 2 、供应商针对本项目的测评环境配置较好，具有一定的密码应用方案模拟与验证能力，得 8分 ； 3 、供应商针对本项目的测评环境配置一般，合理性较差，得 6分 ； 4 、未提供或其他，得 0分 。	10.0000	主观	商务应答表 服务方案

测评工具评价	<p>供应商承诺投入本项目的测评工具应为正版并保证测评工具产生的数据的可靠性，根据响应程度综合打分，具体标准如下： 1、测评工具科学、先进、可行，至少包括具有校准证明的网络传输密码检测仪，并提供上述工具采购合同，得10分； 2、投入工具较为齐全、充足，较好满足项目测评需求，得7分； 3、投入工具一般，基本满足项目测评需求，得4分； 4、未提供或其他，得0分。</p>	10.0000	主观	商务应答表 服务方案
保密管理方案评价	<p>根据本项目保密管理需求，对提供的针对本项目测评过程中涉及重要或敏感数据的安全保密管理方案进行评分，具体标准如下： 1、供应商配有相关能力支撑的保密办公区，具有很好的项目保密管理制度与安全保密管理能力，采取的安全管理措施得当，能够很好保障本项目测评的数据安全，得10分； 2、供应商具有较好的项目保密管理制度与安全保密管理能力，采取的安全管理措施较为得当，能够保障本项目测评的数据安全，得7分； 3、供应商具有较好的项目保密管理制度与安全保密管理能力，采取的安全管理措施较为一般，基本保障本项目测评的数据安全，得4分； 4、其他情形不得分。</p>	10.0000	主观	商务应答表 服务方案

项目质量管理方案评价	对提供的针对本项目测评过程中的质量管理方案进行评分，具体标准如下： 1、项目质量管理完备，项目质量保障措施科学、可行、完善，项目管理与风险控制合理，得10分； 2、项目质量管理较为完备，项目质量保障措施较为科学可行，项目管理与风险控制较为合理，得7分； 3、项目质量管理一般，项目质量保障措施一般，项目管理与风险控制一般，得4分； 4、其他情形不得分。	10.0000	主观	商务应答表 服务方案
进度控制	供应商针对本项目提供进度安排及保障措施，根据响应程度综合打分，具体标准如下： 1、有明确合理的项目实施周期和进度计划表，并有相应的进度保障措施，措施安排合理科学，可行性高的计10分； 2、方案可行、措施安排基本合理的计7分； 3、方案基本合理可行，但内容不全的计4分； 4、未提供不计分。	10.0000	主观	商务应答表 服务方案
风险防范	对整个评测项目实施过程中的风险有相应的防范措施，应急响应措施，根据响应程度综合打分，具体标准如下： 1、有完善的安全需求分析和安全方案设计，保证客户信息资料的安全性，并明确保密责任与赔偿承诺，各项措施分析切实可行的计7分； 2、措施分析基本可行，措施完整的计4分； 3、措施分析较差的计1分； 4、未提供不计分。	7.0000	主观	商务应答表 服务方案

价格分	价格分	价格分统一采用低价优先法计算，即满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他投标供应商的价格分统一按照下列公式计算：投标报价得分=(评标基准价 / 投标报价)×100计算分数时四舍五入取小数点后两位。	10.0000	客观	开标一览表 标的清单
-----	-----	---	---------	----	---------------

价格扣除

序号	情形	适用对象	比例	说明	关联格式
1	小型、微型企业，监狱企业，残疾人福利性单位	投标人或联合体成员均为小型、微型企业	10.0000 %	对于经主管预算单位统筹后未预留份额专门面向中小企业采购的采购项目，以及预留份额项目中的非预留部分采购包，对符合《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）规定的小微企业报价给予C1的扣除，用扣除后的价格参加评审。承接本项目的供应商符合相应条件时，给予C1的价格扣除，即：评标价=最后报价×（1-C1）;监狱企业与残疾人福利性单位视同小型、微型企业，享受同等价格扣除，当企业属性重复时，不重复价格扣除	开标一览表 中小企业声明函 残疾人福利性单位声明函 标的清单 监狱企业的证明文件

采购包5:

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

详细评审	实施方案	根据投标人提供的项目实施方案，服务内容、服务手段、服务计划安排、服务保障方案等方面进行评分。 1.内容深刻全面的得10分； 2.内容基本全面的得6分； 3.内容不够完善的得3分； 4.差的或不提供的不得分。	10.0000	主观	商务应答表 服务方案
	项目管理措施	根据投标人提供的项目质量管理过程控制及监控手段，能确保技术人员按照相应的操作指导规范实施，有完善的质量保证管理体系。 1.内容深刻全面的得10分； 2.内容基本全面的得6分； 3.内容不够完善的得3分； 4.差的或不提供的不得分。	10.0000	主观	商务应答表 服务方案
	项目风险防范措施	根据投标人提供的项目实施过程中的风险防范措施，并明确保密责任与赔偿承诺，根据方案的完整程度和优劣程度综合评分。 1.内容深刻全面的得10分； 2.内容基本全面的得6分； 3.内容不够完善的得3分； 4.差的或不提供的不得分。	10.0000	主观	商务应答表 服务方案
	进度控制	供应商针对本项目提供进度安排及保证措施。 1.有明确合理的项目实施周期和进度计划表，并有相应的进度保障措施，措施安排合理科学，可行性高的计5分； 2.方案可行、措施安排基本合理的计3分； 3.方案基本合理可行，但内容不全的计1分， 4.未提供不计分。	5.0000	主观	商务应答表 服务方案
	培训方案	供应商须针对本项目提供培训方案。 1.培训服务方案内容全面、安排合理，能完全满足本项目需要的，得10分； 2.培训方案内容设计一般的，得6分； 3.培训方案设计较差、部分满足本项目需要的，得3分； 4.未提供本项内容不得分。	10.0000	主观	商务应答表 服务方案

售后服务方案	投标人须针对本项目提供售后服务方案。 1.售后服务方案设计全面，能完全满足本项目需要的，得10分； 2.售后服务方案内容设计一般的，得6分； 3.售后服务方案设计较差、部分满足本项目需要的，得3分； 4.未提供本项内容不得分。	10.0000	主观	商务应答表 服务方案
服务保障方案	针对服务要求提供服务保障，保证项目的安全实施和售后维护；在项目服务期内提供培训、应急等服务。 1.服务保障方案内容完整，可行性高的得10分； 2.服务保障方案内容较完整，有一定可行性的得6分； 3.服务保障方案内容不完整，可行性较差的得3分； 4.未提供本项内容不得分。	10.0000	主观	商务应答表 服务方案
其他服务承诺及合理化建议	根据投标人可为招标人提供的其他相关服务内容、服务承诺及合理化建议赋分。 1.服务内容、服务承诺及合理化建议具体详细，与项目匹配度高且能够落到实处的得10分； 2.服务内容、服务承诺及合理化建议较详细，对项目开展有一定实际意义，但存在不完善的地方的得6分； 3.服务内容、服务承诺及合理化建议较为粗略的得3分； 4.未提供或其他情况不得分。	10.0000	主观	商务应答表 服务方案
业绩	投标人提供2021年1月1日至今（以合同签订时间为准）同类成功项目案例，每提供一个得3分，最多得15分。投标人需提供项目案例合同关键页（包括但不限于合同封面页、合同双方、服务内容、签字盖章、生效时间等）复印件或扫描件并加盖公章，否则该项目案例不得分。	15.0000	客观	商务应答表 服务方案

价格分	价格分	价格分统一采用低价优先法计算，即满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他投标供应商的价格分统一按照下列公式计算：投标报价得分=(评标基准价 / 投标报价)×100计算分数时四舍五入取小数点后两位。	10.0000	客观	开标一览表 标的清单
-----	-----	---	---------	----	---------------

价格扣除

序号	情形	适用对象	比例	说明	关联格式
1	小型、微型企业，监狱企业，残疾人福利性单位	投标人或联合体成员均为小型、微型企业	10.0000 %	对于经主管预算单位统筹后未预留份额专门面向中小企业采购的采购项目，以及预留份额项目中的非预留部分采购包，对符合《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）规定的小微企业报价给予C1的扣除，用扣除后的价格参加评审。承接本项目的供应商符合相应条件时，给予C1的价格扣除，即：评标价=最后报价×（1-C1）;监狱企业与残疾人福利性单位视同小型、微型企业，享受同等价格扣除，当企业属性重复时，不重复价格扣除	开标一览表 中小企业声明函 残疾人福利性单位声明函 标的清单 监狱企业的证明文件

采购包6:

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

	项目理解	根据对本项目的业务需求和系统建设进行需求分析： 1.分析清晰、合理、深入、准确的，得10分； 2.分析基本合理、存在部分内容理解不够准确的，得6分； 3.分析没有针对性或业务流程掌握不准确、分析与业务需求有较大偏差的，得3分。 4.未响应不得分。	10.0000	主观	商务应答表 服务方案
	项目团队	1、拟派项目总监具有信息系统监理师证书且有8年以上（含8年，以取得信息系统监理师证书时间计算）信息系统工程项目管理经验，得5分；拟派项目总监具有信息系统监理师证书且有8年以下（以取得信息系统监理师证书时间计算）信息系统工程项目管理经验，得2分。 本项最高得5分，不符合要求不得分。 2、团队其他成员（不含项目总监）具有信息系统监理师证书，每有1人计1分，最高得5分。（注：需将加盖公章的证书复印件或扫描件附在投标文件中，；总监理工程师必须为投标人单位职工，提供开标前近三个月社保证明，否则该项不得分。）	10.0000	客观	商务应答表 服务方案
	重点难点分析	对本项目关键点把控和重点难点分析符合项目实际情况： 1.分析清晰、合理、深入、准确的，得10分； 2.分析基本合理、存在部分内容理解不够准确的，得6分； 3.分析没有针对性或业务流程掌握不准确、分析与业务需求有较大偏差的，得3分。 4.未响应不得分。	10.0000	主观	商务应答表 服务方案
	合理化建议分析	对本项目关键点把控和重点难点分析提出的合理化建议，具有针对性与可行性： 1.符合项目实际情况的，得10分； 2.提出的建议可行性一般或不完全符合项目实际情况的，得6分； 3.提出的建议针对性较差的，得3分。 4.未响应不得分。	10.0000	主观	商务应答表 服务方案

详细评审	质量控制方法和措施	1.质量控制原则，描述内容详细完整，控制原则有针对性、切实可行，得2分；方案基本合理，内容基本完整，得1分；内容不合理或未响应不得分； 2.质量控制总思路，描述内容有完整，有详细的质量控制组织框架，得2分；方案基本合理，内容基本完整，得1分；内容不合理或未响应不得分； 3.质量控制方法，描述内容详细完整，质量控制方法科学、切实可行，得2分；方案基本合理，内容基本完整，得1分；内容不合理或未响应不得分； 4.质量控制措施，描述内容详细完整，质量控制措施完善、有针对性且可执行，得2分；方案基本合理，内容基本完整，得1分；内容不合理或未响应不得分。	8.0000	主观	商务应答表 服务方案
	进度控制方法和措施	1.进度控制原则，描述内容详细完整，进度控制原则符合项目需求，方案合理可行，得2分；方案基本合理，内容基本完整，得1分；内容不合理或未响应不得分； 2.进度控制方法，描述内容详细完整，进度控制方法科学、可执行，得2分；方案基本合理，内容基本完整，得1分；内容不合理或未响应不得分； 3.进度控制措施，描述内容详细完整，质量控制措施完善、有针对性且可执行，得2分；方案基本合理，内容基本完整，得1分；内容不合理或未响应不得分。	6.0000	主观	商务应答表 服务方案

投资控制方法和措施	1.投资控制原则，描述内容详细完整，投资控制原则规范、合理可行，得2分；方案基本合理，内容基本完整，得1分；内容不合理或未响应不得分； 2.投资控制方法，描述内容详细完整，投资控制方法符合项目控制目标，针对性强，得2分；方案基本合理，内容基本完整，得1分；内容不合理或未响应不得分； 3.投资控制措施，描述内容详细完整，质量控制措施完善、有针对性且可执行，得2分；方案基本合理，内容基本完整，得1分；内容不合理或未响应不得分。	6.0000	主观	商务应答表 服务方案
项目安全、合同、变更、信息管理方案	1.项目安全管理方案目标明确、措施方法合理可行，且具有针对性，符合本项目实际需求，得2分；方案基本合理，内容基本完整，得1分；内容不合理或未响应不得分。 2.项目合同管理方案目标明确、措施方法合理可行，且具有针对性，符合本项目实际需求，得2分；方案基本合理，内容基本完整，得1分；内容不合理或未响应不得分。 3.项目变更管理方案目标明确、措施方法合理可行，且具有针对性，符合本项目实际需求，得2分；方案基本合理，内容基本完整，得1分；内容不合理或未响应不得分。 4.项目信息管理方案目标明确、措施方法合理可行，且具有针对性，符合本项目实际需求，得2分；方案基本合理，内容基本完整，得1分；内容不合理或未响应不得分。	8.0000	主观	商务应答表 服务方案
组织协调方法和措施	协调难点分析准确，协调工作程序和会议制度等明确，措施方法合理可行，且具有针对性，得6分；方案基本合理，内容基本完整，得3分；内容不合理或未响应不得分。	6.0000	主观	商务应答表 服务方案

	项目实施和风险控制措施	<p>监理工作的组织实施与计划安排细致、周全、合理、详尽风险控制措施有力，得10分； 监理工作的组织实施与计划安排较细致、较周全、较合理、较详尽，风险控制措施较有力，得6分； 监理工作的组织实施与计划安排一般，风险控制措施一般，得3分； 未提供项目实施进度计划和安排的不得分。</p>	10.0000	主观	商务应答表 服务方案
	业绩	<p>投标人提供2021年1月1日至今（以合同签订时间为准）同类项目业绩，每提供一个得2分，最多得6分。 投标人需提供项目案例合同关键页（包括但不限于合同封面页、合同双方、服务内容、签字盖章、生效时间等）复印件或扫描件并加盖公章，否则不得分。</p>	6.0000	客观	商务应答表 服务方案
价格分	价格分	<p>价格分统一采用低价优先法计算，即满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他投标供应商的价格分统一按照下列公式计算： 投标报价得分=（评标基准价 / 投标报价）×100 计算分数时四舍五入取小数点后两位。</p>	10.0000	客观	开标一览表 标的清单

价格扣除

序号	情形	适用对象	比例	说明	关联格式
----	----	------	----	----	------

1	小型、微型企业，监狱企业，残疾人福利性单位	投标人或联合体成员均为小型、微型企业	10.0000 %	对于经主管预算单位统筹后未预留份额专门面向中小企业采购的采购项目，以及预留份额项目中的非预留部分采购包，对符合《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）规定的小微企业报价给予C1的扣除，用扣除后的价格参加评审。承接本项目的供应商符合相应条件时，给予C1的价格扣除，即：评标价=最后报价×（1-C1）；监狱企业与残疾人福利性单位视同小型、微型企业，享受同等价格扣除，当企业属性重复时，不重复价格扣除	开标一览表 中小企业声明函 残疾人福利性单位声明函 标的清单 监狱企业的证明文件
---	-----------------------	--------------------	-----------	--	--

说明：

- 1、评分的取值按四舍五入法，保留小数点后两位；
- 2、评分标准中要求提供的证明材料须清晰可辨。

（最低评标价法适用）采用最低评标价法的，投标文件满足招标文件全部实质性要求，且投标报价最低的投标人为中标候选人。采用最低评标价法评标时，除了算术修正和落实政府采购政策需进行的价格扣除外，不能对投标人的投标价格进行任何调整。

5.7废标

本次政府采购活动中，出现下列情形之一的，予以废标：

- 一、符合专业条件的投标人或者对招标文件作实质响应的投标人不足三家的；
- 二、出现影响采购公正的违法、违规行为的；
- 三、投标人的报价均超过了采购预算，采购人不能支付的；
- 四、因重大变故，采购任务取消的；

废标后，代理机构将在陕西省政府采购网上公告。对于评标过程中废标的采购项目，评标委员会应当对招标文件是否存在倾向性和歧视性、是否存在不合理条款进行论证，并出具书面论证意见。

5.8定标

5.8.1 定标原则

采购人在评标报告确定的中标候选人名单中按顺序确定1名中标人。中标候选人并列的，由采购人采取随机抽取的方式确

定中标人。

5.8.2定标程序

一、评标委员会在项目电子化交易系统中编制评标情况，生成评标报告。

二、代理机构在评标结束之日起2个工作日内将评标报告送采购人。

三、采购人在收到评标报告后5个工作日内，按照评标报告中推荐的中标候选人顺序确定中标供应商。逾期未确认的，又不能说明合法理由的，视同按评标报告推荐的顺序确定排名第一的中标候选人为中标供应商。

四、根据确定的中标供应商，代理机构在陕西省政府采购网上发布中标结果公告，通过项目电子化交易系统向中标供应商发出中标通知书。

5.9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。

5.10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）评标前，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）评标过程中，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）评标过程中，不得干预或者影响正常评标工作，不得发表倾向性、引导性意见，不得修改或细化招标文件确定的评标程序、评标方法、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标意见，不得拒绝对自己的评标意见签字确认。

（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6章投标文件格式

6.1 投标文件封面格式

采购包1:

分册名称：投标响应文件分册

详见附件：投标文件封面

详见附件：投标函

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：投标人应提交的相关资格证明材料

详见附件：商务应答表

详见附件：开标一览表

详见附件：标的清单

详见附件：服务方案

详见附件：法定代表人授权书

详见附件：非联合体不分包投标声明

详见附件：分项报价表

详见附件：近三年无重大违法、违纪书面声明

详见附件：书面声明

详见附件：保证金汇款声明函、保函

详见附件：控股管理关系

详见附件：技术偏离表

采购包2:

分册名称：投标响应文件分册

详见附件：投标文件封面

详见附件：投标函

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：投标人应提交的相关资格证明材料

详见附件：商务应答表

详见附件：开标一览表

详见附件：标的清单

详见附件：保证金汇款声明函、保函

详见附件：法定代表人授权书

详见附件：非联合体不分包投标声明

详见附件：分项报价表

详见附件：技术方案

详见附件：近三年无重大违法、违纪书面声明

详见附件：控股管理关系

详见附件：书面声明

详见附件：技术偏离表

采购包3：

分册名称：投标响应文件分册

详见附件：投标文件封面

详见附件：投标函

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：投标人应提交的相关资格证明材料

详见附件：商务应答表

详见附件：开标一览表

详见附件：标的清单

详见附件：服务方案

详见附件：保证金汇款声明函、保函

详见附件：法定代表人授权书

详见附件：非联合体不分包投标声明

详见附件：分项报价表

详见附件：近三年无重大违法、违纪书面声明

详见附件：控股管理关系

详见附件：书面声明

采购包4：

分册名称：投标响应文件分册

详见附件：投标文件封面

详见附件：投标函

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：投标人应提交的相关资格证明材料

详见附件：商务应答表

详见附件：开标一览表

详见附件：标的清单

详见附件：服务方案

详见附件：保证金汇款声明函、保函

详见附件：法定代表人授权书

详见附件：非联合体不分包投标声明

详见附件：分项报价表

详见附件：近三年无重大违法、违纪书面声明

详见附件：控股管理关系

详见附件：书面声明

采购包5：

分册名称：投标响应文件分册

详见附件：投标文件封面

详见附件：投标函

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：投标人应提交的相关资格证明材料

详见附件：商务应答表

详见附件：开标一览表

详见附件：标的清单

详见附件：服务方案

详见附件：保证金汇款声明函、保函

详见附件：法定代表人授权书

详见附件：非联合体不分包投标声明

详见附件：分项报价表

详见附件：近三年无重大违法、违纪书面声明

详见附件：控股管理关系

详见附件：书面声明

采购包6：

分册名称：投标响应文件分册

详见附件：投标文件封面

详见附件：投标函

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：投标人应提交的相关资格证明材料

详见附件：商务应答表

详见附件：开标一览表

详见附件：标的清单

详见附件：服务方案

详见附件：保证金汇款声明函、保函

详见附件：法定代表人授权书

详见附件：非联合体不分包投标声明

详见附件：分项报价表

详见附件：近三年无重大违法、违纪书面声明

详见附件：控股管理关系

详见附件：书面声明

第7章 拟签订采购合同文本

详见附件：合同文本.docx

