一标段采购需求：

一、项目基本情况

《陕西省数字政府建设“十四五”规划》将“智慧黄河”列入生态保护重点应用清单，要求推动黄河流域一体化生态环境监测监管，构建黄河流域生态环境风险预警体系，构筑全要素生态保护能力。陕西省“智慧黄河”信息平台建设（一期）项目是省2022年省级政务信息化建设项目重点工作。陕西省“智慧黄河”信息平台建设（一期）项目依托陕西省政务云资源，构建实景三维子数据库、生态资源子数据库、经济社会子数据库、业务管理子数据库和平台运维子数据库5个数据库，开发平台门户、综合信息分析系统、督察监测系统3个业务系统。通过项目实施，初步汇聚陕西省黄河流域信息资源，提供统一的信息入口，实现各类数据资源的融合和动态更新，推动流域内数据资源整合共享，对各类督察问题的基本情况、处理结果及后续发展进行监测。

二、具体采购内容

1、数据资源建设及数据治理

（1）实景三维数据库：建设黄河流域9省（区）和陕西省黄河流域82个县（区、市）14.3万平方千米视觉缩放效果连续、数据无缝套合的宏观层级实景三维模型；对于重点自然地理实体与文化景观获取并制作生成不少于100平方千米5-10cm高精度实景三维模型；融合相关要素数据层，建立实景三维数据库。

（2）生态资源数据库：通过收集、分析、清洗自然资源、生态环境、水利、农业、林草等行业资料，建立包含自然资源、生态环境、水利、农业、林草等行业不少于20个空间数据图层的生态环境数据库。

（3）经济社会数据库：通过收集、分析、清洗发改、交通、教育、医疗、文化旅游、文物、统计等行业资料，建立包含发改、交通、教育、医疗、文化旅游、文物、统计等行业不少于20个空间数据图层的经济社会数据库。

（4）业务管理数据库：通过监管问题上图入库、提取遥感监测疑问图斑、无人机外业巡查、监测数据整理分析等工作，对2019年至2022年以来历年黄河流域各类督察问题整改落实情况进行卫星遥感及无人机巡查监测、对2022年省黄河流域涉水项目问题排查问题进行卫星遥感监测、对2022年省黄河流域尾矿

库及周边情况进行卫星遥感监测，建立2022年业务管理数据库。

（5）平台运维数据库：制定用户管理、角色管理、菜单管理、部门管理、数据字典、日志管理等各类表结构，并随着平台日常运行对其进行维护更新，建立平台运维数据库。

2、成品软件购置

购置业务流管理软件和GIS基础软件。

3、定制软件开发

（1）平台门户：实现平台内系统单点登录、统一密码服务、身份验证、角色权限控制、平台功能和资源管理，并展示陕西省黄河流域生态保护和高质量发展工作进展、政策法规、公开信息等内容。

（2）综合信息分析系统：实现省黄河流域相关自然资源、生态环境、经济发展、文化旅游、规划指标等信息定制化检索、统计、分析，并通过实景三维场景全方位展示其时空变化。

（3）督察监测系统：利用业务管理数据库，实现省黄河流域督察问题整改情况的上报、管理和展示；利用卫星遥感、无人机巡查、大数据分析等技术，全方位感知、实时监测督察问题处理结果及后续发展。

4、体系建设

开展标准规范体系、运维管理体系、安全保障体系建设，编写相关文本资料。

5、其他

配合开展第三方软件测试、等级保护测评、密码应用安全性评估等工作。

三、采购要求及成果形式

1、总体要求

（1）设计要求

设计思路清晰、整体方案完整、重点内容突出。方案总体架构和技术架构设计合理、层次清楚、特色鲜明、描述详细、无缺漏、思路清晰、存储安全、灵活。

（2）技术要求

1）项目设计及技术路线选择综合考虑实用、成熟、先进性、可扩展性，同时考虑系统的易用性、易维护性。项目总体技术路线是采用B/S（Browser/Server）架构，系统采用J2EE技术架构为基础，通过三层结构的设计实现各业务应用。

2）系统应支持主流的浏览器、操作系统（包括 Windows、Linux、兼容国产操作系统）；投标人应保证针对采购人所提供的操作系统、中间件、数据库及浏览器版本与其他分项系统版本集成具备兼容性，后续实施过程中因兼容性导致的问题投标人应给予解决。

3）除平台运维数据库外，其他数据库中的数据应为空间数据，属性字段设计应满足系统运行以及业务需求。对数据结构、类型以及数据属性项字段有详细说明。采用的数据库管理软件应为国产自主可控。

（3）性能要求

1）吞吐量指标：系统支持用户数不低于 2000 人，数据门户需满足 40 个并发用户数同时在线使用；

2）在满足并发访问的前提下，系统的响应时间应符合以下要求：

平台响应时间：≤1S；

稳定性指标：系统保证 7×24 小时不间断运行。

3） 系统应能保证长时期运行且积累相当数量的数据后，系统软件性能没有明显的下降。为保证软件的效率和性能，投标人应提出可行的系统数据库优化方案。建设期和维保期间，投标人均应负责性能优化，包括但不限于软件系统本身、所使用的数据库、中间件等。

（4）环境与部署要求

该系统的用户运行环境需支持 Windows XP、Windows 7、Windows10 等主流操作系统，以及兼容国产操作系统，支持 IE9 及以上、Chrome、搜狗、360、Firefox 等主流浏览器，支持 1024*768 及以上分辨率，内部插件支持 Microsoft Office 2003 及以上，支持查看 PDF 格式文件，支持查看 JPG、BMP、GIF、PNG 等常用格式图片。

陕西省“智慧黄河”一期平台按全省一级集中部署方式，整体拟部署于西咸云基地省级信创政务云，使用政务云平台提供的资源和服务。投标方应根据本期项目平台的功能和性能要求，提出完整合理的系统硬件和平台部署配置方案。

（5）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，在院方指定的具备等保三级硬件和网络环境下，系统平台应符合国家信息安全等级保护三级相关要求；

2）提供多租户大数据资源共享能力，提供安全保障共享集群资源的数据安全，提供丰富的授权管理手段满足跨部门数据共享需求；

3）在身份鉴别、访问控制、安全审计、剩余信息保护、通讯完整性、通讯保密性、抗抵赖、软件容错、资源控制、代码安全等方面，按照国家信息安全等级保护第三级规定和技术要求进行设计、建设，并通过三级等保测评，按要求完成整改工作，直至项目顺利通过测评；

4）为保证本项目的安全稳定运行，确保信息的保密性、可用性、完整性，数据安全得到保障。投标人需按照等级保护三级进行设计，从物理架构、网络安全设计、基础平台安全服务、数据安全服务等方面提出全面的信息安全体系设计方案，供招标人参考。

（6）接口要求

设计要充分考虑与现有软硬件系统（包括集中部署和分散部署的系统、不同网络上部署的系统等）的对接工作，并做好各种预案，保障对接工作的顺利进行。

1）应充分提供和预留相应接口，以满足各业务系统的认证、二次开发、各系统间无缝衔接、以及与各厅局数据交换的需求。投标方需提供开发接口及详细说明文档，具有二次开发能力以及与第三方应用系统的集成能力。

2）需与已有的接口进行对接，包括但不限于以下来源:省发改委、省测绘局接口能力等。

（7）项目管理要求

投标人必须成立项目管理组织，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。

2、数据资源要求

（1）需要收集的资料

根据综合信息分析系统和平台门户的业务需求，需要自主向省黄河流域领导小组成员单位收集相关专业数据，具体如下，

1）向发改部门收集黄河流域规划计划、领导批示、专家建议、会议纪要、

公务文件以及经济区、宏观经济、产业经济等数据；

2）向教育部门收集学校、教师、学生等数据；

3）向科技部门收集科研机构、科技人员等数据；

4）向工业信息化部门收集工业、信息化发展等数据；

5）向民族宗教部门收集民族、宗教场所等数据；

6）向民政部门收集行政区划、地名等数据；

7）向自然资源部门收集土地利用、国土空间规划、耕地保护、矿产资源、地下水资源、地质灾害等数据；

8）向生态环境部门收集大气质量、水质、土地面源污染、污染治理情况等数据；

9）向住建部门收集污水处理厂、垃圾处理厂、建筑业等数据；

10）向交通运输部门收集铁路、公路、汽车站等数据；

11）向水利部门收集水系、地表水资源、水文区划、行蓄滞洪区、饮用水水源地保护区、水工设施、灌区、水土保持等数据；

12）向农业部门收集高标准农田、农业等数据；

13）向商务部门收集对外贸易业等数据；

14）向文旅部门收集旅游景点、风景名胜区、历史文化名城、名镇、名村、非物质文化遗产、饮食文化、公共图书馆、群众艺术馆、文化馆等数据；

15）向卫生健康部门收集医院、医疗从业人员等数据；

16）向应急管理部门收集尾矿库、自然灾害等数据；

17）向林业部门收集林地资源、草地资源、国家公园、自然保护区、湿地公园、森林公园、地质公园等数据；

18）向体育部门收集体育馆、体育从业人员等数据；

19）向统计部门收集人口、宏观经济等数据；

20）向文物保护部门收集文物保护单位、博物馆等数据；

21）向能源部门收集油气输送管道、输电线等数据；

22）向气象部门收集气候资源、气象灾害等数据；

23）向测绘地理信息部门收集基础测绘数据；

24）向通信管理部门收集通讯线等数据；

25）向相关部门收集其他数据。

（2）数据库的建设

1）实景三维数据库：通过对数字高程模型（DEM）和数字正射影像（DOM）的空间配准、地理套合和一致性处理，构建视觉缩放效果连续的、数据无缝套合的宏观层级实景三维模型；对于重点自然地理实体与文化景观利用无人机获取5cm-10cm分辨率倾斜影像，通过空中三角测量、密集点云匹配、三维模型构建、纹理映射，生成不少于100平方千米高精度实景三维模型；融合数字线划图（DLG）数据相关要素层，建立实景三维数据库。

2）生态资源数据库：对自然资源、生态环境、水利、农业、林业等行业数据信息进行分析和分类整理，对图件、文本、表单等不同文件进行栅格化、矢量化等空间化处理，根据业务需求对数据库进行概念设计、逻辑设计，根据数据实际情况对数据进行坐标转换、采集、编辑等处理，建立生态资源数据库。

3）经济社会数据库：对发改、交通、教育、医疗、文化旅游、文物、统计等行业数据信息进行分析和分类整理，对图件、文本、表单等不同文件进行栅格化、矢量化等空间化处理，根据业务需求对数据库进行概念设计、逻辑设计，根据数据实际情况对数据进行坐标转换、采集、编辑等处理，建立经济社会数据库。

4）业务管理数据库：通过监管问题上图入库、提取遥感监测疑问图斑、无人机外业巡查、监测数据整理分析等工作，对2019年至2022年以来历年黄河流域各类督察问题整改落实情况进行卫星遥感及无人机巡查监测、对2022年省黄河流域涉水项目问题排查问题进行卫星遥感监测、对2022年省黄河流域尾矿库及周边情况进行卫星遥感监测，建立2022年业务管理数据库。

5）平台运维数据库：制定用户管理、角色管理、菜单管理、部门管理、数据字典、日志管理等各类表结构，并随着平台日常运行对其进行维护更新，建立平台运维数据库。

（3）数据资源安全要求

数据资源建库环境必须是采取物理隔离措施的独立涉密网，在机房环境、设备、介质、存储备份、应急响应、运行管理、病毒防治、访问控制、安全审计、信息加密与电磁泄露防护、端口接入管理、系统及网络安全监测等方面必须满足涉密信息系统运行网络环境的要求。

数据资源安全设计的目标包括三个方面：一是无授权情况下数据库系统中任何数据不被下载、复制；二是满足系统数据对不同级别、不同权限用户的合理使用，使系统正常运行、不被非法入侵、不受外界破坏；三是在系统出现故障（设备故障、运行环境故障或人为操作失误）造成数据的破坏时能及时通过系统数据的备份与恢复策略及时进行数据恢复，从而保障系统数据的准确无误，系统的稳定运行。

3、系统功能要求

陕西省“智慧黄河”信息平台（一期）的系统功能需求根据省发改委黄河办主要业务来分析，其目的是推动黄河流域生态保护和高质量发展领导小组办公室日常工作标准化、信息化、流程化管理，推动陕西省黄河流域生态保护和高质量发展战略顺利实施。

陕西省“智慧黄河”信息平台（一期）的主要业务为综合查询业务、督察问题监管业务和平台管理业务，对应需建设综合信息分析系统、督察监测系统和平台门户。各系统的功能需求分析如下：

（1）综合信息分析系统。根据省发改委黄河办业务分析，综合信息分析系统需具备数据实景三维场景浏览、增加、删除、查询、修改等功能。提供黄河流域生态保护、高质量发展、规划指标等数据的检索、统计、分析和管理功能；对部分地理信息数据提供二三维电子地图服务，通过实景三维场景全方位展示重点数据的时空变化。

（2）督察监测系统。根据省发改委黄河办业务分析，督察监测系统需具备问题和线索的导入、下发、增加、删除、查询、通知等功能，以及任务的接收、上报、反馈、填报、确认等功能。提供黄河流域相关督察监测任务的上报、下发、核实、管理、展示、整改、自查等功能；利用卫星遥感、无人机巡查、外业核查、大数据分析等技术，实现定期监测，支撑黄河办督察监管业务的开展。

（3）平台门户。根据省发改委黄河办业务分析，平台门户需具备平台登录服务、身份验证、角色权限控制、平台功能和资源管理等功能。能够基于陕西省政务云平台提供的统一身份认证、统一电子印章、统一密码服务实现平台登录服务、身份验证、角色权限控制、平台用户和资源统一管理，并提供陕西省政务服务网接入，展示陕西省黄河流域生态保护和高质量发展工作进展、政策法规、公

开信息等内容。

4、成品软件购置要求

平台基于成品软件建设，需购置的成品软件有如下要求：

（1）业务流管理软件。选用国产自主可控、先进成熟的技术，且与硬件实现同步；支持多远端工作站；分布式处理，模块化设计，高内聚，低耦合，故障隔离，无存储瓶颈和处理瓶颈，具有良好的可扩展性，可平滑扩容；具有良好的开放性，实现纵向和横向联网。

（2）GIS 基础软件。选用国产自主可控大型的平台软件，具有二三维一体化的空间数据采集、存储、管理、分析、处理、制图与可视化等核心功能，并且具备赋能各行业应用系统的应用开发能力。

5、平台部署要求

陕西省“智慧黄河”信息平台（一期）采用集约化建设，整体部署于西咸云基地省级信创政务云，使用政务云平台提供的资源和服务，应提供基于省级信创政务云的集约化建设方案、数据资源共享方案、灾备方案。

6、成果形式

（1）数据库

实景三维数据库、生态资源数据库、经济社会数据库、业务管理数据库、平台运维数据库等 5 个数据库。

（2）平台系统

平台门户、综合信息分析系统、督察监测系统等 3 个系统。

（3）成品软件

业务流管理软件、GIS 基础软件各 1 套。

（4）文档资料

标准规范体系文本、运维管理体系文本、安全保障体系文本、专业技术设计书、技术总结、质检报告等。

四、技术标准要求（依照标准、参照标准）

1、《中华人民共和国测绘法》（中华人民共和国主席令第 67 号，2017 年 4 月 27 日）；

2、《国务院关于印发政务信息资源共享管理暂行办法的通知》（国发〔2016〕

51 号）；

3、《国务院关于加快推进“互联网+政务服务”工作的指导意见》（国发〔2016〕55 号）；

4、《“互联网+政务服务”技术体系建设指南》（国办函〔2016〕108 号）；

5、《政务信息系统整合共享实施方案》（国办发〔2017〕39 号）；

6、《国务院办公厅关于加快“互联网+监管”系统建设和对接工作的通知》（国办函〔2018〕73 号）；

7、《国家政务信息化项目建设管理办法》（国办发〔2019〕57 号）；

8、《黄河流域生态保护和高质量发展规划纲要》（发布版）（2021 年 10 月 8 日中共中央、国务院印发）；

9、《国务院关于加强数字政府建设的指导意见》（国发〔2022〕14 号）；

10、《国务院办公厅关于印发全国一体化政务大数据体系建设指南的通知》（国办函〔2022〕102 号）；

11、《陕西省测绘成果管理条例》（2021 年 9 月 29 日陕西省第十三届人民代表大会常务委员会第二十八次会议修订）；

12、《陕西省测绘成果资源统筹应用管理办法》（陕财办建〔2018〕17 号）；

13、《陕西省测绘条例》（2019 年 9 月 27 日陕西省十三届人大常委会第十三次会议审议通过）；

14、《关于加强协作推动陕西省黄河流域生态环境保护的意见》（2020 年 9 月陕西省法院、省检察院、省公安厅、省生态环境厅、省自然资源厅、省水利厅、省林业局联合印发）；

15、《陕西省数字政府“十四五”规划》（陕政办发〔2021〕27 号）；

16、《陕西省黄河流域生态保护和高质量发展 2021 年工作要点》；

17、《陕西省黄河流域生态保护和高质量发展 2022 年工作要点》；

18、《国家电子政务工程建设项目管理暂行办法》（发展改革委令第 55 号）；

19、《陕西省省级政务信息化项目建设管理办法（暂行）》（陕政办发〔2022〕19 号）；

20、《实景三维中国建设技术大纲（2021 版）》（自然资办发〔2021〕56 号）；

21、《基础地理信息要素分类与代码》GB/T 13923-2006；

22、《基础性地理国情监测内容与指标》GQJC 03-2020；

23、《基础地理信息数据库基本规定》GB/T 30319-2013；

24、《公开地图内容表示要求》》GB/T 35764-2017；

25、《电子政务系统总体设计要求》GB/T 21064-2007；

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

27、《信息安全技术信息系统密码应用基本要求》GB/T39786-2021；

28、《信息安全技术 政府网站云计算服务安全指南》GB/T 38249-2019；

29、《计算机软件需求规格说明规范》GB/T 9385-2008；

30、其他测绘地理信息与信息化标准规范。

五、验收方法及标准

系统通过试运行，各项功能指标均达到招标文件、投标文件和合同约定，同时提交项目相关各类技术文档后，由采购人分别组织专家开展初级和终级验收。

1、采购人将依照国家相关系统开发建设的标准和规范，组织对本项目进行初级和终极验收。验收方案由采购人最终确定，验收工作由采购人负责，供应商配合。

2、初级和终级验收时，供应商应至少提供相关的纸质技术资料(三份)，包括：用户需求说明书、详细设计说明书、系统安装说明、系统使用手册、系统维护手册等;同时提供以上技术资料的电子文档以及所有自开发应用系统的源代码，其它验收文档由用户向开发商另行提出。

六、软件测试、密评、等保

供应商配合第三方机构进行软件测试、密码应用安全评估（三级系统）和等保测评（三级）。

七、知识产权

供应商应对所供服务具有或已取得合法知识产权，供应商应保证所供服务不会出现因第三方提出侵犯其专利权、商标权或其它知识产权而引发法律或经济纠纷，否则由供应商负责解决并承担全部责任；如因此影响到采购人的正常使用，采购人有权单方解除本合同，供应商应无条件向采购人退回已收取的全部合同价款，给采购人造成损失的，由供应商一并赔偿。采购人享有该项目所开发的所有应用软件的所有权，采购人和中标人共同享有著作权。

八、保密要求

中标供应商对项目工作中应无条件地对接触到的涉密数据做好保密工作，不得以任何方式泄露，否则，应承担相应的法律责任。项目完成或终止不免除供应商应承担的保密义务。

九、服务要求

所有参与陕西省“智慧黄河”信息平台建设（一期）的工作人员（包括数据资源建设和系统软件研发）必须全部驻场（办公场地、桌、椅、网络由采购人提供，其他办公设备自备），并且建设过程中不得随意更换人员，否则采购方有权解除合同。项目建设完成后提供 3 年免费服务（提供不少于 2 人驻场服务）。

二标段采购需求：

招标内容及要求

一）技术标准

本标段技术要求提供的是最低限度的技术要求，并未对一切技术细节做出规定，也未充分引述有关标准和规范的条文，投标人应遵循可靠、先进、经济、实用及环保的原则，保证提供符合本监理要求的优质服务。

本项目的监理服务须执行中华人民共和国国家标准、规范、办法。技术要求中所应用的标准和规范应使用现行最新版本。

监理单位应遵循科学、公正、遵纪、守法、诚信、守约的职业道德，以高度的责任心和丰富的专业技术经验，根据国家的有关法规、技术规范和标准以及业主与承建单位签订的合同，对项目实施有重点的、全面的、精线条的监理。同时帮助用户掌握工程进度，按期分段对工程验收，保证工程按期、高质量地完成。

二）监理目标

依照有关标准以及建设方的需求，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，对本项目建设实施全面的、按技术线条的监督管理。通过在项目实施的全过程中对项目建设的监管、实施进度的控制和质量管理，保证整个项目建设各部分、各环节和各个子系

统的质量符合设计要求和国家规范；从而保证项目高质量、按计划完成。

具体分解为如下目标：

（1）质量目标：符合国家有关技术标准和规范，满足设计文件与合同要求。

（2）进度目标：协助用户处理好设计单位、承建单位及相关参建方的关系。对施工过程中由于设计方案的漏洞或与实际情况的差异或质量问题等所引起的全部或部分工程的停工、窝工，有责任及时组织相关单位或人员进行沟通、协调，保证项目按工程计划分阶段全面完成。

（3）项目管理目标：对各种设计文档以及项目管理提供可靠的审核和质量保证。

（4）对承建单位的行为进行监控，保证项目建设行为符合国家标准规范要求，制止业务系统开发和实施行为的随意性和盲目性，监督和保证文明施工的实施，确保工程合法、科学、合理又经济。

（5）协助用户与承建单位的有效沟通，使承建单位能够全面准确了解用户的实际需求，随时为用户提供工程的进展情况。

（6）保证项目运行的全过程有一套明确、合理、可行的计划或者规程，以及与之相应的审核、监理机制和手段。

（7）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，及早预测和发现可能影响施工计划的各种因素，及时纠正可能影响工程质量的缺陷，实时控制工程计量与付款。

（8）如工程出现或需要变更，有责任对变更的合理性进行审核并协调或通知用户、设计单位或承建单位进行认可，对变更所产生的费用和对工程计划的影响进行把握和控制，对未经用户认可的变更一律不准实施。

三）监理服务范围

监理要正确理解本项目的建设目标和内容，要了解本项目相关的组织结构和业务特点，对项目管理单位、集成商等项目相关方在项目实施过程中涉及的项目实施、集成、应用开发、测试、初步验收、试运行、第三方测试、竣工验收和系统移交、培训等阶段进行全程的监理，配合项目建设单位对所有项目工作进行监督和管理。

四）服务内容

工程实施过程中的质量、进度、投资、变更控制，安全文明生产监督管理、合同、信息管理，参与项目建设各方关系的协调工作，配合招标人完成建设目标。

（一）合同签订阶段

合同签订阶段指自招标人与承建单位签订工程建设合同为止。此阶段监理主要的工作内容是：

（1）就招标文件实质性内容，结合招标人预期与成交服务商进行合同谈判；

（2）审核合同及附件文档，出具监理报告。

（二）实施准备阶段

准备阶段指项目合同签订之日起，至项目基准（建设范围、进度计划、实施方案）经三方（或监理方）确认后，总监理工程师签发开工令为止。

此阶段监理主要的工作内容是：

（1）由监理现场负责人对所建立管理制度进行培训，提出管理要求；

（2）与进场人员签订数据保密协议；

（3）审核承建单位进场人员资格；

（4）审查并实地复核设计方案，出具监理专题报告；

（5）审核承建单位提交的工程进度（实施）计划、施工方案、实施（管理）方案，出具监理专题报告；

（6）监督设计交底的组织；

（7）监督承建单位内部的技术交底和安全交底培训；

（8）签发开工令。

（三）实施阶段

施工阶段指项目开工令签发之日起，至单项工程完成子项验收为止，此阶段监理主要的工作内容是：

1.质量控制

（1）系统集成质量的控制

①系统集成方案的审核和确认；

②对采购的软硬件产品的质量进行检验、测试和验收；

③对系统软件的安装调试进行验收；

④对系统集成进行总体验收。

（2）软件开发质量的控制

①软件开发计划的审核和确认；

②对软件开发的需求分析、概要设计、详细设计、编码测试、应用测试等每个开发阶段进行把关；

③对承建单位的开发质量记录进行审核；

④源代码及应用程序的移交验收等；

⑤参与对应用软件的总体验收。

（3）培训的质量控制

①审核确认承建单位的培训计划；

②检查培训教材、使用说明书、维护手册等资料内容，检查培训文档是否与实际培训内容相符合；

③协助用户方组织培训；

④监督承建单位实施其培训计划，并征求用户的反馈意见；

⑤对培训效果进行考核；

⑥审核确认承建单位的培训总结报告。

2.进度控制

（1）根据已批准的工程实施计划，检查实际施工执行进度；

（2）对承建单位（施工方）提交的项目周报等内容进行进度真实性复核；

（3）根据当前实施进度，判断或预测项目执行的时间风险，并出具监理建议；

（4）定期以周报/月报形式向招标人量化汇报工程实际的执行状态。

3.投资控制

（1）审核合同或备忘录中关于工程款项支付的条件；

（2）收到承建单位/施工方提交付款申请，参照合同支付条件进行实际工程量核算，确定支付的符合性，出具监理支付意见（支付证书）；

（3）对于合同索赔进行造价评估；

（4）协助招标人梳理清查固定资产、进行子项的项目结算。

4.变更控制

（1）审核承建单位/施工方提出的变更申请，就其变更动机的合理性出具监

理专题报告，予以批准或否决；

（2）对初步批准的变更申请，组织三方审核变更方案，评估变更影响，并严格各方执行变更程序；

（3）对于工程款项变更进行造价评估；

（4）监督变更方案的实施，并评估变更影响效果，出具监理专题报告。

5.安全及数据保密管理

（1）协助建设单位审核安全施工方案和数据保密方案；

（2）定期/不定期对项目安全施工及数据保密管理方案执行情况进行检查；

（3）负责项目建设过程中所涉及的政府数据和资料的保护，保证不被非授权使用；

（4）负责项目建设施工过程中安全控制，确保不出现安全事故。

（5)对于危险施工的实施任务，监督承建单位/施工方安全交底工作的执行，安全交底包括方案编写、培训宣贯；监理人员应进行岗前检查和操作巡查。

6.文档管理

（1）批准承建单位/施工方提交项目文档管理计划，并根据计划及时敦促承建单位/施工方提交文档；

（2）审核承建单位/施工方提交的各类项目文档，并出具监理专题报告；

（3）负责对于工程过程产生的原始文档/文件进行收集，并定期整理；

（4）做好项目监理日记及项目大事记；

（5）做好合同批复等各类往来文件的存档；

（6）做好项目协调会、技术专题会的会议纪要工作；

（7）管理实施期间的各类技术文档；

（8）项目月报；

（9）监理工程师通知；

（10）阶段性项目总结。

7.合同管理

（1）协助审核项目合同，按照要求就项目合同征求意见并根据意见进行修改完善；

（2）跟踪检查合同的执行情况，确保项目建设单位按时履约；

（3）对合同的工期的延误和延期进行审核确认；

（4）对合同变更、索赔等事宜进行审核确认；

（5）根据合同约定，审核项目承建单位的支付申请，签发付款凭证；

（6）对项目变更控制，明确界定项目变更的目标，防止变更范围的扩大化，加强变更风险以及变更效果的评估；

（7）任何变更都要得到三方（建设单位、监理单位和承建单位）的书面确认。

8 沟通协调

（1）组织召开监理例会，并形成监理会议纪要；

（2）根据工程实际出现的建设问题，（协助招标人）及时召开工程专题例会，并形成监理会议纪要；

（3）对涉及多方的建设交互/协同问题，（协助招标人）及时召开工程协调会，并形成监理会议纪要。

（四）测试测评阶段

（1）协助建设单位系统测试工作，出具监理意见；

（2）协助建设单位系统安全测评工作，出具相应监理报告。

（五）验收阶段

（1）核查项目建设完成情况，出具是否具备验收条件的监理意见；

（2）协助建设单位确定验收程序、验收标准和验收方案；

（3）依据项目档案管理规范，协助整理工程验收文档；

（4）协助建设单位组织验收会议；

（5）协助项目和档案移交。

五）监理服务依据

1 国家相关部门、项目建设和监理的最新法律、法规、政策文件和管理规范，包括但不限于：

（1）国家及行业相关文件；

（2）国家有关标准和规范；

（3）招投标文件、合同书、实施方案等；

（4）经审批的变更方案。

2 本项目招投标文件及合同。

六）监理服务要求

（一）监理单位的责任

（1）监理单位有责任为建设单位提供项目顾问意见，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。

（2）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。

（3）由于承建单位在工程实施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。如承建单位人员工作不力，可提出调换有关人员。

（4）如果承建单位违反合同规定的质量要求和完工时限，监理单位应协助建设单位追究有关承建单位的责任。

（5）如果因监理单位监督不力，造成建设单位经济损失的，监理单位要向建设单位赔偿承建单位造成的损失。

（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按合同规定的时间和方式移交给建设单位。

（二）监理服务人员要求

为保障项目监理工作顺利实施，确保项目建设合法合规、规范有序，投标人应组建具有高度政治责任感、丰富从业经验、能够与招标人及承建单位进行良好沟通的高素质团队参与本项目监理工作。

（1）拟投入本项目的团队人员须为投标单位的正式员工，能够满足本项目监理工作需要，项目团队人员须配备合理，具有不同层次，应至少包括总监理工程师、总监理工程师代表、监理工程师等。

（2）总监理工程师、总监理工程师代表应承担过类似项目的监理工作。

（3）总监理工程师、总监理工程师代表不得随意更换，因重大原因确需调整的，须经招标人同意。投标人应根据项目实施阶段工作重点及时调整专业监理人员配置，人员调整必须经招标人同意，招标人有权要求更换人员。

（4）招标人有权要求投标人保证人员配置的合理性以及团队人员的稳定性，因人员的过失造成招标人的直接经济损失，应赔偿招标人的损失。

三标段采购需求：

一、项目概况

为保障各类业务系统上线后的安全稳定运行，验证系统在功能性、性能效率、可靠性等方面是否满足要求，需要在采购人提供的测试环境下进行检测。

二、服务期限

平台初验后 60 日历天。

三、采购内容

需检测的业务系统范围主要包括：综合信息分析系统、督察监测系统、平台门户等，测试内容主要是功能测试、性能测试、接口测试等。

（一）功能测试要求

1.目的

验证系统功能是否符合要求、是否覆盖系统需求文档、系统设计文档中的各个功能点、是否都实现正确。

2.范围

主要包含但不限于以下测试内容：

(1)基本功能类测试：主要验证各基础功能模块是否实现正确。

(2) 后台管理类测试：主要验证人员权限分配、参数设置、报表查询、数据统计、操作日志等功能是否实现正确。

(3) 核心业务流程类测试：主要验证数据信息流向是否正确。

(4) 渠道业务功能测试：主要验证渠道权限、渠道管理、渠道监控等功能是否正确。

(5) 身份认证及访问控制类测试：主要是验证系统用户的身份鉴别功能、访问控制功能是否正确。

(6) 人机交互类测试：主要验证人机操作、界面显示、消息提示等功能能否正确。

（二）性能测试要求

1.目的

验证系统技术文档中提出的各项性能指标是否满足性能需求。

2.范围

主要包含但不限于以下测试内容：

(1) 负载测试：验证的对象包括事务吞吐量、事务响应时间。

(2) 压力测试：通过长时间运行，验证系统资源使用情况是否稳定。

3.轮次要求

回归验证 1 轮。

4.通过标准（包括但不限于以下要求）

(1) 所有测试场景 100%测试完成；

(2) 给出所要求性能指标实际测试结果；

(3) 对于未达到要求之性能指标给予调优建议；

(4) 如调优仍然无法达到所要求之性能指标，则给出结论。

（三）接口测试要求

1.目的

验证系统对外提供的接口是否满足系统需求文档、系统设计文档中的要求，接口字段、接口请求处理及返回结果是否正确等，保证系统能够满足接口设计要求。

2.范围

主要包含但不限于以下测试内容：

(1) 接口通信协议；

(2) 接口传输字段；

(3) 接口请求数据；

(4) 接口应答数据；

3. 轮次要求

回归验证 1 轮。

4. 通过标准（包括但不限于以下要求）

(1) 所有测试脚本 100%运行完成

(2) 所有接口 100%测试完成；

(3) 测试发现的接口缺陷全部修复；

(4) 若存在特殊问题，经过协商处理，达成一致。

（四）测试标准

GB/T 25000.51-2016《系统与软件工程 系统与软件质量要求和评价（SQuaRE）第 51 部分：就绪可用软件产品（RUSP）的质量要求和测试细则》

（五）交付物要求

在提供测试服务的过程中，需向采购人提供的测试交付物为《陕西省“智慧黄河”信息平台建设项目（一期）软件测试报告》（纸质版和电子版）。

四、验收要求

供应商出具合格、完整、有效的软件测试报告。

四标段采购需求：

一、项目基本情况

《陕西省数字政府建设“十四五”规划》将“智慧黄河”列入生态保护重点应用清单，要求推动黄河流域一体化生态环境监测监管，构建黄河流域生态环境风险预警体系，构筑全要素生态保护能力。陕西省“智慧黄河”信息平台建设项目（一期）是省 2022 年省级政务信息化建设项目重点工作。陕西省“智慧黄河”信息平台建设项目（一期）依托陕西省政务云资源，构建实景三维子数据库、生态资源子数据库、经济社会子数据库、业务管理子数据库和平台运维子数据库 5 个数据库，开发平台门户、综合信息分析系统、督察监测系统 3 个业务系统。通过项目实施，初步汇聚陕西省黄河流域信息资源，提供统一的信息入口，实现各类数据资源的融合和动态更新，推动流域内数据资源整合共享，对各类督察问题的基本情况、处理结果及后续发展进行监测。

二、具体采购内容

（一）等级保护

信息安全等级保护工作共分为五步，分别是：“定级、备案、建设整改、等级测评、监督检查”。该项目主要完成系统的安全测评工作，依据安全技术和安全管理两个方面的测评要求，分别从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理十个安全类别进行安全测评。

1.定级

依据《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）、《人民法院非涉密重要信息系统安全等级保护定级工作指导意见》（法[2008]159号）确定系统等级。

2.备案

依据《网络安全等级保护测评过程指南》（GB/T 28449-2018），对该项目系统向陕西省网络安全保卫总队申请重要信息系统备案，完成备案的信息系统，获得公安机关颁发的《信息系统安全等级保护备案证明》。

3.等级保护测评

按照《信息安全技术 信息系统安全等级保护实施指南》（GB/T25058-2019）、《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）、《信息安全技术 网络安全等级保护测评过程指南》（GB/T28449-2018）等相关的标准规范开展等级测评工作，对系统的安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理共10个层面进行安全等级保护测评（三级）。测评内容包括但不限于如下指标：

等级保护技术要求（三级）

层面	控制点	测评项
安全物理环境	物理位置选择	1. 机房场地应选择在具有防震、防风和防雨等能力的建筑内； 2. 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	1. 机房出入口应安排专人值守，控制、鉴别和记录进入的人员； 2. 需进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围； 3. 应对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域； 4. 重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员。

	防盗器和防破坏	1. 应将主要设备放置在机房内； 2. 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； 3. 应将通信线缆铺设在隐蔽处，可铺设在地下或管道中； 4. 应对介质分类标识，存储在介质库或档案室中； 5. 应利用光、电等技术设置机房防盗报警系统； 6. 应对机房设置监控报警系统。
	防雷击	1. 应将各类机柜、设施和设备等通过接地系统安全接地； 2. 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	3. 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； 4. 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； 5. 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。
	防水和防潮	1. 水管安装，不得穿过机房屋顶和活动地板下； 2. 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透； 3. 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； 4. 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	1. 应采用防静电地板或地面并采用必要的接地防静电措施； 2. 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	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	1. 应在机房供电线路上配置稳压器和过电压防护设备； 2. 应提供短期的备用电力供应，至少满足主要设备在断电情况下的正常运行要求； 3. 应设置冗余或并行的电力电缆线路为计算机系统供电； 4. 应建立备用供电系统。
	电磁防护	1. 应采用接地方式防止外界电磁干扰和设备寄生耦合干扰； 2. 电源线和通信线缆应隔离铺设，避免互相干扰； 3. 应对关键设备和磁介质实施电磁屏蔽。
安全通信网络	网络架构	1. 应保证网络设备的业务处理能力满足业务高峰期需要； 2. 应保证网络各个部分的带宽满足业务高峰期需要； 3. 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； 4. 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； 5. 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	1. 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； 2. 应采用密码技术保证通信过程中数据的保密性。
	可信验证	3. 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。

	边界防护	1. 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； 2. 应能够对非授权设备私自联到内部网络的行为进行检查或限制； 3. 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； 4. 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。
	访问控制	1. 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； 2. 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； 3. 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； 4. 应能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； 5. 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。
	入侵防范	1. 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； 2. 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； 3. 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； 4. 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。

	恶意代码防范	1. 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； 2. 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。
	安全审计	1. 审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户； 2. 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件； 3. 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等； 4. 应能够根据记录数据进行分析，并生成审计报表； 5. 应保护审计进程，避免受到未预期的中断； 6. 应保护审计记录，避免受到未预期的删除、修改或覆盖等。
	可信验证	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。
安全计算环境	身份鉴别	1. 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； 2. 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施； 3. 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； 4. 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来实现。

	访问控制	1. 应对登录的用户分配账户和权限； 2. 应重命名或删除默认账户，修改默认账户的默认口令； 3. 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； 4. 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； 5. 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； 6. 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； 7. 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	1. 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； 2. 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； 3. 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； 4. 应对审计进程进行保护，防止未经授权的中断。
	入侵防范	1. 应遵循最小安装的原则，仅安装需要的组件和应用程序； 2. 应关闭不需要的系统服务、默认共享和高危端口； 3. 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； 4. 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； 5. 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； 6. 应能够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	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	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	1. 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，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； 2. 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，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。
	数据保密性	1. 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等； 2. 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。
	数据备份恢复	1. 应提供重要数据的本地数据备份与恢复功能； 2. 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份场地； 3. 应提供重要数据处理系统的热冗余，保证系统的高可用性。
	剩余信息保护	1. 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； 2. 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	1. 应仅采集和保存业务必需的用户个人信息； 2. 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	1. 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； 2. 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	1. 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； 2. 应通过审计管理员对审计记录应进行分析，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、管理和查询等。
	安全管理	1. 应对安全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管理操作，并对这些操作进行审计； 2. 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记，对主体进行授权，配置可信验证策略等。
	集中管控	1. 应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控； 2. 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； 3. 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； 4. 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； 5. 应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理； 6. 应能对网络中发生的各类安全事件进行识别、报警和分析。
	安全策略	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	1. 应对安全管理活动中的各类管理内容建立安全管理制度； 2. 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； 3. 应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。
	制定和发布	1. 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； 2. 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	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	1. 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； 2. 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； 3. 应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。
	人员配备	1. 应配备一定数量的系统管理员、审计管理员和安全管理员等； 2. 应配备专职安全管理员，不可兼任。
	授权和审批	1. 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；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； 2. 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。

	沟通和合作	1. 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； 2. 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； 3. 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	1. 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； 2. 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、安全配置与安全策略的一致性、安全管理制度的执行情况等； 3. 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	1. 应指定或授权专门的部门或人员负责人员录用； 2. 应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核； 3. 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	1. 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； 2. 应办理严格的调离手续，并承诺调离后的保密义务后方可离开。
	安全意识教育和培训	1. 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； 2. 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； 3. 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	1. 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； 2. 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； 3. 外部人员离场后应及时清除其所有的访问权限； 4. 获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。
安全建设管理	定级和备案	1. 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由； 2. 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； 3. 应保证定级结果经过相关部门的批准； 4. 应将备案材料报主管部门和相应公安机关备案。
	安全方案设计	1. 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； 2. 应根据保护对象的安全保护等级及与其他级别保护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； 3. 应组织相关部门和有关安全专家对安全整体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	1. 应确保网络安全产品采购和使用符合国家的有关规定； 2. 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； 3. 应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。

	自行软件开发	1. 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；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； 2. 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； 3. 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； 4. 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； 5. 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； 6. 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	1. 应在软件交付前检测其中可能存在的恶意代码； 2. 应保证开发单位提供软件设计文档和使用指南； 3. 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门和隐蔽信道。
	工程实施	1. 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； 2. 应制定安全工程实施方案控制工程实施过程； 3. 应通过第三方工程监理控制项目的实施过程。
	测试验收	4. 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； 5. 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测试相关内容。
	系统交付	1. 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； 2. 应对负责运行维护的技术人员进行相应的技能培训； 3. 应提供建设过程文档和运行维护文档。

	等级测评	1. 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； 2. 应在发生重大变更或级别发生变化时进行等级测评； 3. 应确保测评机构的选择符合国家有关规定。
	服务供应商选择	1. 应确保服务供应商的选择符合国家的有关规定； 2. 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； 3. 应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。
安全运维管理	环境管理	1. 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； 2. 应建立机房安全管理制度，对有关物理访问、物品带进出和环境安全等方面的管理作出规定； 3. 应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。
	资产管理	1. 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； 2. 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； 3. 应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。
	介质管理	1. 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； 2. 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，并对介质的归档和查询等进行登记记录。

	设备维护管理	1. 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； 2. 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； 3. 信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据应加密； 4. 含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，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	1. 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； 2. 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	1. 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； 2. 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； 3. 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； 4. 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； 5. 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、参数的设置和修改等内容； 6. 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； 7. 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，操作结束后应同步更新配置信息库； 8. 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； 9. 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； 10. 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的行为。
	恶意代码防范管理	1. 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； 2. 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	1. 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； 2. 应将基本配置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	1. 应遵循密码相关国家标准和行业标准； 2. 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	1. 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； 2. 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； 3. 应建立中止变更并从失败变更中恢复的程序，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	1. 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； 2. 应规定备份信息的备份方式、备份频度、存储介质、保存期等； 3. 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	1. 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； 2. 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；应在安全事件报告和响应处理过程中，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； 3. 对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。

	应急预案管理	1. 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、事后教育和培训等内容； 2. 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； 3. 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； 4. 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	1. 应确保外包运维服务商的选择符合国家的有关规定； 2. 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； 3. 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，并将能力要求在签订的协议中明确； 4. 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、存储要求，对 IT 基础设施中断服务的应急保障要求等。

五标段采购需求：

一、项目基本情况

《陕西省数字政府建设“十四五”规划》将“智慧黄河”列入生态保护重点应用清单，要求推动黄河流域一体化生态环境监测监管，构建黄河流域生态环境风险预警体系，构筑全要素生态保护能力。陕西省“智慧黄河”信息平台建设项目（一期）是省 2022 年省级政务信息化建设项目重点工作。陕西省“智慧黄河”信息平台建设项目（一期）依托陕西省政务云资源，构建实景三维子数据库、生态资源子数据库、经济社会子数据库、业务管理子数据库和平台运维子数据库 5 个数据库，开发平台门户、综合信息分析系统、督察监测系统 3 个业务系统。通过项目实施，初步汇聚陕西省黄河流域信息资源，提供统一的信息入口，实现各类数据资源的融合和动态更新，推动流域内数据资源整合共享，对各类督察问题的基本情况、处理结果及后续发展进行监测。

二、具体采购内容

1.测评概述

1.1 测评目的及范围

依据《信息系统密码应用基本要求》，针对目标系统从技术要求、密钥管理、安全管理三个角度出发，围绕信息系统的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全以及密钥管理、安全管理开展密码测评工作，以期发现信息系统与其相应安全等级要求之间的差距以及存在的安全隐患，为密码应用测评标准提供工作建议，保障信息系统密码合规、正确、有效地应用。

密码测评的目的是通过对目标系统在安全技术及管理方面的测评，对目标系统的安全技术状态及安全管理状况做出初步判断，给出目标系统在安全技术及安全管理方面与其相应安全等级要求之间的差距。测评结论作为委托方进一步完善系统安全策略及安全技术防护措施依据。

此次测评范围为：开发平台门户、综合信息分析系统、督察监测系统 3 个业务系统，拟测评等级均为三级。

供应商需提供整改建议咨询服务。

1.2 测评依据

法律法规：

- 《电子签名法》
- 《电子认证服务管理办法》
- 《信息安全等级保护商用密码管理办法》

行业标准：

- 新国标 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》
- GM/Y 5001-2017《密码标准应用指南》
- GM/Z 0001-2013《密码术语》
- GM/T 0028-2014《密码模块安全技术要求》
- GM/T 0039-2015《密码模块安全检测要求》
- GM/T 0036《采用非接触卡的门禁系统密码应用指南》
- GM/T 0060-2018《签名验签服务器检测规范》
- GM/T 0024-2014《SSL VPN 技术规范》

- GM/T 0025-2014《SSL VPN 网关产品规范》
- GM/T 0015-2012《基于 SM2 密码算法的数字证书格式规范》
- 《商用密码应用安全性评估管理办法》
- 《商用密码应用安全性测评机构管理办法》
- 《商用密码应用安全性评估测评过程指南（试行）》
- 《商用密码应用安全性评估测评作业指导书（试行）》

被测机构送审文档：

- 《支付机构国产密码应用试点实施方案》
- 《支付机构国产密码应用试点应用解决方案》
- 《国密试点项目技术方案概要设计》
- 《国密试点详细设计说明书》
- 《国产密码算法库接口使用说明文档》

术语和定义

下列术语和定义适用于本文件

（1）机密性 confidentiality

保证信息不被泄露给非授权的个人、进程等实体的性质。

（2）完整性 data integerity

数据没有遭受以非授权方式所做的篡改或破坏的性质。

（3）真实性 authenticity

确保主体或资源的身份正是所声称的特性。真实性适用于用户、进程、系统和信息之类的实体。

（4）国密算法

国密算法是由国家密码局发布的一系列商用密码算法标准。

（5）数字签名 digital signature

签名者使用私钥对待签名数据的杂凑值做密码运算得到的结果，该结果只能用签名者的公钥进行验签，用于确认待签名数据的完整性、签名者身份的真实性和签名行为的抗抵赖性。

1.3 测评原则

客观公正原则

测评人员保证在最小主观判断情形下，按照双方认可的测评方案，基于明确定义的测评方式和解释，实施测评活动。

经济性和可重用性原则

测评工作采信可重用已有测评结果中相同的检测项目，包括商用密码安全产品测评结果，信息系统密码测评结果和等级保护测评结果。所有重用结果都以结果适用于待测系统为前提，并能够客观反映目前系统的安全状态。

可重复性和可再现性原则

依照同样的要求，使用同样的测评方法，在同样的环境下，不同的测评机构对每个测评实施过程的重复执行应得到同样的结果。可再现性和可重复性的区别在于，前者关注不同测评者测评结果的一致性，后者则与同一测评者测评结果的一致性有关。

结果完善性原则

在正确理解《信息系统密码应用基本要求》各个要求项内容的基础之上，检测所产生的结果应客观反映信息系统的运行状态。测评过程和结果应服从正确的测评方法，以确保其满足要求。

1.4 密码应用安全性评估测评实施

测评目标和对象

通过对待测系统在商用密码技术应用、密钥管理及安全管理方面的分析，对系统商用密码应用的合规性、正确性、有效性作出判断，确定了测评目标和测评对象。

表 1 测评对象列表

序号	测评层面	测评对象
1	通用测评要求	密码管理员、密码算法、密码技术、密码产品、密码服务技术文档
2	物理和环境安全	物理安全负责人、系统管理员、机房监控系统、门禁系统、技术文档
3	网络和通信安全	交换机、堡垒机、应用系统、网络安全运维人员、技术文档
4	设备和计算安全	交换机、堡垒机、系统管理员、数据库管理员、

		业务服务器、数据库服务器、证书服务器、密钥管理服务器、技术文档
5	应用和数据安全	应用系统管理员、操作系统、存储各类密钥的管理系统、技术文档
6	安全制度	安全管理制度

1.5 测评方法

测评方式

本次密码测评的主要方式有：访谈、文档审查、配置审查、工具测试、实地察看。

- 访谈

检验人员与被测系统有关人员（个人/群体）进行交流、讨论等活动，获取相关证据，了解有关信息。在访谈范围上，不同等级信息系统在测评时有不同的要求，一般应基本覆盖所有的安全相关人员类型，在数量上可以抽样。

- 文档审查

检查《信息系统密码应用基本要求》和《信息系统密码测评要求》中规定的必须具有的制度、策略、操作规程等文档是否齐备。

检查是否有完整的制度执行情况记录和人员管理情况记录，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。

对上述文档进行审核与分析，检查他们的完整性和这些文件之间的内部一致性。

- 配置审查

根据测评结果记录表格内容，利用上机验证的方式检查应用系统、主机系统、数据库系统、密码设备以及网络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。

如果系统在输入无效命令时不能完成其功能，将要对其进行错误测试。

- 工具测试

根据测评指导书，利用技术工具对系统进行测试，包括网络协议分析、密码算法和密码协议的识别和验证等。

- 实地察看

根据被测系统的实际情况，检验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，测评其是否达到了相应等级的密码安全要求。

1.6 测评工具

对省局业务系统进行验证测试，涉及网络密码协议分析、密码算法检测等多种测评方式，测评工具类型列表见表 2 所示。

表 2　测评工具类型列表

序号	工具类型	测评对象
1	网络协议分析工具	实现对被测系统所在主机从应用安全\密码安全等方面进行评测分析。通过协议分析工具，对客户端与服务器之间的通信协议包进行抓取，并从应用安全、密码安全等方面进行评测分析。
2	数字证书合规性验证工具	对数字证书格式、数字证书签名值验证等方面进行合规性检测，分析证书使用是否合规，密码功能是否正确等。

针对被测系统的网络边界和抽查设备、主机和业务应用系统的情况，需要在被测系统及其互联网络中设置测试工具接入点。

1.7 风险分析及防范措施

测评阶段可能面临的风险以及风险规避措施如表 3 所示：

表 3　风险分析列表

风险概述	风险分析	风险规避
有效性风险	1、在商用密码应用安全性测评过程中首先要进行的是信息收集工作，在信息收集的过程中，经常会存在信息收集不完整、信息描述不准确等问题，而不准确的信息将会对测评方案编制工作中测评指标及测评对象的选择带来偏	1、信息收集过程中尽量确保信息收集完整、信息描述准确，测评机构应与被测评单位及时沟通。 2、测评过程中，测评实施人员应及时与被测评方就测评中发现的问题及时沟

风险概述	风险分析	风险规避
	差。 2、在现场测评中，不同工程师对标准要求的理解也会影响到测评工作的有效性和准确性。 3、在报告编制过程中测评师对测评结果的分析是否合理，对于测评结论的有效性也有较大影响。	通，避免因对标准理解的偏差导致的必须要问题出现。 3、报告编制过程中应指派至少两名及测评师负责测评结果的分析，确保对测评结果的分析正确、合理。
公正性风险	1、在测评过程中，测评工程师、测评机构通常会受到市场竞争压力、测评机构自身业务发展压力、被测评机构合同及财务压力等多方面的影响，从而导致测评结论的公正性问题。	1、加强测评人员测评素质培训，对测评机构的测评实施过程记性监督管理。 2、测评实施过程中，测评方应保证在符合国家密码主管部门要求及最小主观判断情形下，按照与被测单位共同认可的密评方案，基于明确定义的测评方式和解释，实施测评活动。
保密性风险	1、商用密码应用安全性测评工作，要求测评机构深入了解被测评系统的管理、技术及业务方面的信息。而这些信息大部分涉及到企业或机构的商业、工作秘密。如果测评工作中，测评机构泄漏了检测单位的系统状态信息，如网络拓扑、IP 地址、业务流程、安全机制、安全隐患和有关文档信息，将会对检测单位的信息系统带来极大的安全问题。	1、加强测评人员保密意识培训，测评人员与被测评单位签署安全保密协议，保密协议建议由被测单位提供。 2、被测评单位完善信息保密控制措施，根据“业务需要”和“最小权限”原则提供材料和系统使用权限。 3、在测评过程中，被测系统

风险概述	风险分析	风险规避
	2、在测评过程中，资料收集、现场测评记录、编制报告等活动都会使用到被测评单位系统相关信息，在信息的使用和交换过程中多存在着信息泄漏的风险。	的常规性资料以人员面对面形式进行递交，敏感性材料按照被测单位的相关要求，可采取现场查阅或访谈的方式进行；传递介质以光盘为主。
测评过程风险	1、验证测试可能影响被测信息系统正常运行：在现场测评时，需对设备和系统进行一定的验证测试工作，部分测试内容需上机查看信息，可能对被测信息系统的运行造成不可预期的影响。 2、工具测试可能影响被测信息系统正常运行：在现场测评时，根据实际需要可能会使用一些测评工具进行测试。测评工具使用时可能会产生冗余数据写入，同时可能会对系统的负载造成一定的影响，进而对被测信息系统中的服务器和网络通信造成一定影响甚至损害。 3、可能导致被测信息系统感信息泄露：测评过程中，可能泄露被测信息系统的敏感信息，如加密机制、业务流程、安全机制和有关文档信息等。 4、其他可能面临的风险：在测评过程中，也可能出现影响被测信息	1、签署委托测评协议书：在测评工作正式开始之前，测评方和被测单位需要以委托协议的方式，明确测评工作的目标、范围、人员组成、计划安排、执行步骤和要求以及双方的责任和义务等，使得测评双方对测评过程中的基本问题达成共识。 2、签署保密协议：测评相关方应签署合乎法律规范的保密协议，规定测评相关方在保密方面的权利、责任与义务。 3、签署现场测评授权书：现场测评之前，测评方应与被测单位签署现场测评授权书，要求测评相关方对系统及数据进行备份，采取适当的方法进行风险规避，并针对可能出现的事

风险概述	风险分析	风险规避
	系统可用性、机密性和完整性的风险。	件制定应急处理方案。 4、现场测评要求：需进行验证测试和工具测试时，应避开被测信息系统业务高峰期，在系统资源处于空闲状态时进行测试，或配置与被测信息系统一致的模拟/仿真环境，在模拟/仿真环境下开展测评工作；需进行上机验证测试时，密评人员应提出需要验证的内容，由被测单位的技术人员进行实际操作。整个现场测评过程，由被测单位和测评方相关人员进行全程监督。 5、测评工作完成后，密评人员应交回在测评过程中获取的所有特权，归还测评过程中借阅的相关资料文档，并将测评现场环境恢复至测评前状态。

1.8 测评指标

依据信息系统确定的业务信息安全保护等级和系统服务安全保护等级，选择《基本要求》中对应级别的安全要求作为密码测评的基本指标，以表格形式在表中列出。

此次测试从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、密钥管理、安全管理六个方面考虑罗列出本次测评指标范围,如表 4 所示。

测评范围内的测评指标：

表 4　测评范围内测评指标列表

序号	层面	测评指标
1	物理和环境安全	身份鉴别
2		电子门禁记录数据完整性
3		视频记录数完整性
4	网络和通信安全	身份鉴别
5		网络边界访问控制信息的完整性
6		通信数据完整性
7		通信数据机密性
8		安全接入认证
9	设备和计算安全	身份鉴别
10		远程管理通道安全
11		系统资源访问控制信息完整性
12		重要信息资源安全标记完整性
13		日志记录完整性
14		重要可执行程序完整性、重要可执行程序来源真实性
15	应用和数据安全	身份鉴别
16		访问控制完整性
17		数据传输机密性
18		数据存储机密性
19		数据传输完整性
20		数据存储完整性
21		日志完整性

序号	层面	测评指标
22		重要信息资源安全标记完整性
23		不可否认性
24	安全管理	制度安全
25		人员安全
26		实施安全
27		应急安全

1.9 通用测评要求

测评对象：密码管理员、密码算法、密码技术、密码产品、密码服务技术文档。

密码算法和密码技术合规性

信息系统中使用的密码算法应符合法律、法规的规定和密码相关国家标准、行业标准的有关要求。（第一级到第五级）

信息系统中使用的密码技术应遵循密码相关国家标准和行业标准。（第一级到第五级）

密钥管理

- 信息系统中使用的密码产品、密码服务应符合法律法规的相关要求。（第一级到第五级）
- 采用的密码产品，达到 GB/T 37092 一级及以上安全要求。（第二级）
- 采用的密码产品，达到 GB/T 37092 二级及以上安全要求。（第三级）
- 采用的密码产品，达到 GB/T 37092 三级及以上安全要求。（第四级）
- 采用的密码服务，符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格。（第一级到第四级）

1.10 测评内容和对象

物理和环境安全

测评对象：机房物理环境、物理安全负责人、电子门禁系统、视频监控系统、系统管理员、技术文档。

测评判定：对机房进行现场测评。符合程度根据被测信息系统实际保护状况判定为符合、部分符合、不符合。

表 5　物理和环境安全测评要求列表

测评项	测评指标	测评方法
身份鉴别	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。（第一级到第四级）	遵循物理和环境安全测评要求，对服务端设备所在机房环境进行测评（以核实新增记录的真实性、完整性为主）。
电子门禁记录数据完整性	采用密码技术保证电子门禁系统进出记录数据的存储完整性。（第一级到第四级）	
视频记录数完整性	采用密码技术保证视频监控音像记录数据的存储完整性。（第三级到第四级）	

网络和通信安全

测评对象：交换机、堡垒机、应用系统、网络安全运维人员、技术文档。

测评判定：对网络设备和通信进行现场测评。符合程度根据被测信息系统实际保护状况判定为符合、部分符合、不符合。

表 6　网络和通信安全测评要求列表

测评项	测评指标	测评方法
身份鉴别	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。（第一级到第三级） 采用密码技术对通信实体进行双向身份鉴别，保证通信实体身份的真实性。（第四级）	接入点 JA：在前置服务器前的外部接入交换机处接入，主要目的是捕获通信数据，分析数据交互双方是否加密、通信密码协议是否合规，分析密码服务是否合规、正确、有效。
通信数据完整性	采用密码技术保证通信过程中数据的完整性。（第一级到第四级）	

测评项	测评指标	测评方法
通信数据机密性	采用密码技术保证通信过程中重要数据的机密性。（第一级到第四级）	
网络边界访问控制信息的完整性	采用密码技术保证网络边界访问控制信息的完整性。（第一级到第四级）	
安全接入认证	采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入设备身份的真实性。（第三级到第四级）	

设备和计算安全

测评对象：交换机、堡垒机、系统管理员、数据库管理员、业务服务器、数据库服务器、证书服务器、密钥管理服务器、技术文档。

测评判定：对服务器和存储设备进行现场测评。符合程度根据被测信息系统实际保护状况判定为符合、部分符合、不符合。

表 7　设备和计算安全测评要求列表

测评项	测评指标	测评方法
身份鉴别	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。（第一级到第四级）	尝试正常登录和异常登录（包括错误的口令、不插入智能密码钥匙或插入未授权的智能密码钥匙等情况）情况下，是否按照预期结果完成身份鉴别。
远程管理身份鉴别信息机密性	远程管理设备时，采用密码技术建立安全的信息传输通道。（第三级到第四级）	在管理区 JA 交换机接入通信协议分析工具，查看用于设备管理涉及的管理员口令等鉴别数据和敏感数据在传输中是否进行了机密性保护。
访问控制信	采用密码技术保证系统资	在 JB 交换机接入通信协议分析工具

测评项	测评指标	测评方法
息完整性	源访问控制信息的完整性。（第一级到第四级）	捕获通信数据，分析业务服务器（内置密码模块）是否被有效调用。尝试修改访问控制信息和日志记录（或对应的 MAC），查看完整性保护机制的有效性。
敏感标记完整性	采用密码技术保证设备中的重要信息资源安全标记的完整性。（第三级到第四级）	核实“不适用”的论证依据。
重要可执行程序完整性、重要可执行程序来源真实性	采用密码技术对重要可执行程序进行完整性保护，并对其来源进行真实性验证。（第三级到第四级）	1.尝试修改访问业务服务器上重要程序和文件，查看完整性保护机制的有效性。 2.获取重要程序及其对应数字签名和数字证书（根据实际情况确定）。 3.不插入智能密码钥匙或插入未授权的智能密码钥匙（或其他鉴别设备、口令等），查看完整性保护机制的有效性。
日志记录完整性	采用密码技术保证日志记录的完整性。（第一级到第四级）	在 JB 交换机接入通信协议分析工具捕获通信数据，分析业务服务器（内置密码模块）是否被有效调用。尝试修改访问控制信息和日志记录（或对应的 MAC），查看完整性保护机制的有效性。

应用和数据安全

测评对象：应用系统管理员、数据库系统、待测系统业务应用、存储各类密钥的密钥管理平台、设计文档。

测评判定：对待测系统的应用和数据安全进行现场测评。符合程度根据被测信息系统实际保护状况判定为符合、部分符合、不符合。

表 8　应用和数据安全测评要求列表

测评项	测评指标	测评方法
身份鉴别	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。（第一级到第四级）	1）查看设计文档中身份鉴别采用的密码技术及实现机制； 2）访谈应用管理员，了解应用系统在对用户实施身份鉴别过程中是否使用了密码技术来实现用户身份信息的鉴别，具体采用了何种密码技术和安全设备。 3）核查专用密码产品，如密码算法模块、证书服务管理模块等是否具有国家密码管理部门批准的商用密码产品型号证书。 4）核查待测系统用户身份鉴别信息使用密码技术的正确性和有效性；在接入点 JA 使用网络协议分析工具，抓取报文，分析身份鉴别过程是否正确实现。
访问控制	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。（第一级到第四级）	1）核查是否使用密码技术对访问控制策略进行完整性保护（如使用支持 SM2/SM3/SM4 算法的密码机/密码算法模块执行密码运算，对数据库表访问控制信息、重要资源敏感标记进行保护）；
重要信息资源安全标记完整性	采用密码技术保证信息系统应用的重要信息资源安全标记的完整性。	1）核实“不适用”的论证依据； 2）检查重要信息资源安全标记的保护措施。

测评项	测评指标	测评方法
	（第三级到第四级）	
数据传输机密性	采用密码技术保证信息系统应用的重要数据在传输过程中的机密性。（第一级到第四级）	1）在接入点 JA 使用网络协议分析工具和密码算法合规性验证工具，捕获通信数据，分析系统是否使用 SM4 算法保证待测系统与 XXXX 之间交易数据传输机密性。 2） 查看系统所使用的密码算法、国密算法模块是否经过了国家密码管理部门核准；并截取相关关键数据，作为证据材料。
数据存储机密性	采用密码技术保证信息系统应用的重要数据在存储过程中的机密性。（第一级到第四级）	1）在接入点 JB 接入网络协议分析工具，捕获业务服务器发往数据库服务器的通信数据，分析数据存储是否进行机密性保护； 2）在接入点 JB（业务服务器和密钥管理平台之间）接入网络协议分析工具，捕获通信数据，分析密钥管理平台提供的加密功能是否被有效调用； 3） 查看系统所使用的密码算法、密码算法模块是否经过了国家密码管理部门核准；并截取相关关键数据，作为证据材料。
数据传输完整性	采用密码技术保证信息系统应用的重要数据在传输过程中的完整性。（第一级到第四级）	1）通过 JA 工具接入点接入网络协议分析工具和数字证书合规性验证工具，捕获通信数据，分析待测系统业务服务器与 XXXX 之间的通讯数据是否使用国密算法数字证书进行签名和完整性保护。

测评项	测评指标	测评方法
		2） 查看系统所使用国家密码管理局认可的密码算法、数字证书是否经过了国家密码管理部门核准；并截取相关关键数据，作为证据材料。
数据存储完整性	采用密码技术保证信息系统应用的重要数据在存储过程中的完整性。（第一级到第四级）	1）在接入点 JB 接入数据包捕获工具，捕获业务服务器发往数据库服务器的通信数据，分析数据存储是否进行完整性保护。
不可否认性	在可能涉及法律责任认定的应用中，采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性。（第三级到第四级）	1）核实应用是否存在不可否认性的需求； 2）检测不可否认性的实现方式和密码算法（SM2 算法）

安全管理

测评对象：安全管理制度

测评指标：对安全管理制度进行现场测评。符合程度根据被测信息系统实际保护状况判定为符合、部分符合、不符合。

表 9　安全管理测评要求列表

测评项	测评指标
人员安全	应了解并遵守密码相关法律法规。
	建立密码应用岗位责任制度
	建立上岗人员培训制度
	定期进行安全岗位人员考核
	建立关键岗位人员保密制度和调离制度
制度安全	具备密码应用安全管理制度

测评项	测评指标
	密钥管理规则
	建立操作规程
	定期修订安全管理制度
	明确管理制度发布流程
	制度执行过程记录留存
建设运行安全	制定密码应用方案
	制定密钥安全管理策略
	制定实施方案
	投入运行前进行密码应用安全性评估
	定期开展密码应用安全性评估及攻防对抗演习
应急安全	应急策略
	事件处置
	向有关主管部门上报处置情况

2.预期成果交付物及服务期：

密码测评工作结束后，根据测评内容记录各系统的密码应用现状，出具各系统的《信息系统密码测评报告》。测评报告中以密码应用基本要求为基准，逐项比对各被测系统密码应用的符合性、规范性和正确性，比对与标准存在差异的检查项，出具整改建议书。

序号	交付物名称	介质形式
1	《商用密码应用安全性评估报告》	电子、纸质
2	《整改建议书》	电子、纸质

同时，测评工作也可对现有密码应用测评标准测评内容的准确性进行验证，根据各信息系统密码应用现状和行业应用需求，总结共性问题，指出密码应用改造的难点、疑点和下一步工作计划。

服务期：平台初验后 60 日历天。