采购需求

采购包 1：

标的名称：信息化工程监理服务

监理工作服务要求

一、服务目标

实现项目实施过程中的质量、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，完成陕西省市场监督管理局市场经营主体综合业务系统升级改造及整合迁移项目“四控、三管、一协调”的监理服务目标。

二、服务内容

（一）准备阶段监理工作内容：

准备阶段指项目合同签订之日起，至项目进度计划、实施方案等经监理方确认后，总监理工程师签发开工令为止，监理标准应参考《GB/T 19668.1-2014 信息技术服务监理 第一部分：总则》以及相关分则等相关国家标准执行。此阶段监理主要的工作内容是：

1.协助采购方对建立管理制度，提出管理要求；

2.审核承建单位进场人员资格；

3.审查并实地复核计划方案，出具监理意见；

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)方案等，出具监理意见；

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。

（二）.实施阶段监理工作内容：

1.质量控制

（1）项目实施方案的审核和确认，并提出监理意见；

（2）对项目各参与单位提出的项目计划方案、服务方案等进行审核，对过程资料进行审查，并提出监理意见；

（3）在实施过程中确定质量控制基线，全程、实时地参与项目建设，检查、督促各参建单位严格按合同和规范、保密标准、相关技术标准、设计要求进行实施，监督各参建单位关键节点、重要质量控制点的现场监督；

（4）监督工程中所提供的产品和服务符合承建合同及国家相关法律、法规和标准，做好项目验收工作，

（5）对系统软件的安装调试和部署进行监督及管理，并提出监理意见；

（6）监督项目参建单位的系统集成工作，并提出监理意见；

（7）负责审核项目各参建单位、第三方测评机构提交的测试方案（计划）和报告，保证测试方案和报告的有效性和对功能点、各项验收指标的覆盖，并提出监理意见；

（8）负责监督项目各参建单位对应用系统进行测试工作，对测试报告内容进行检查，并审查部分测试结果，直至测试合格，并提出监理意见；

（9）进行各系统及服务交付成果的核实、软件质量检查及验收工作；

（10）协助采购人组织各项验收工作。

2.进度控制

（1）审核各参建单位的进度分解计划，确认分解计划可以保证总体计划目标；

（2）对项目实施进度进行实时跟踪，并要求各参建单位按项目总进度计划进行动态调整，以确保项目的阶段目标和总体进度目标的实现；

（3）配合采购方对项目实施过程中发生的需求变更进行分析、管理和认定，以确保项目的

阶段目标和总体进度目标的实现；

3.投资控制

（1）对项目实施中的设计优化方案或措施进行审核，对项目建设不可预见性造成风险性支出进行技术性审核，并提出意见；

（2）对因项目变更导致的费用变化进行审查；

（3）做好项目进度付款前的项目完成量确认。

4.变更控制

（1）建立符合本次项目实施及管理的变更管理机制，通过变更控制机制对项目计划、流程、预算、进度或可交付成果的变更申请进行评估，出具是否同意进行的变更审查意见；

（2）通过对项目计划、费用、质量和进度的影响进行分析，审核变更方案，并提出监理意见；

（3）根据变更方案及变更费用预算对变更的的费用进行造价审核；

（4）配合采购方和各参建单位完善及妥善保管有关的变更记录。

5.合同管理

（1）跟踪检查合同的执行情况，监督各参建单位按合同约定履约；

（2）对合同工期的延误和延期进行审核确认；

（3）对合同变更、索赔等事宜进行审核确认；

（4）根据合同约定，鉴定违约事件。

6.文档管理

（1）制订文档管理制度和流程、文档编制规范及项目各类文档模板；

（2）在项目实施过程中做好项目文档的收集、管理工作等，项目文档包括不限于纸质文件、电子文件等；

（3）督促各参建单位做好对所建项目文档的收集、整理和保管工作，确保各参建单位所提供的项目各阶段形成的技术、管理文档的内容和种类符合相关标准；

（4）做好监理记录及项目大事记；

（5）做好项目合同、技术方案、测试文档、验收报告、来往文档等各类文件收集、存档以及移交工作；

（6）做好项目专题会、项目例会等会议纪要；

（7）做好文档的版本控制。

7.安全管理

（1）明确工程的安全要求，协助采购方编制安全管理制度；

（2）促使项目各方所签订的合同中与安全相关的条款在技术、经济上有效；

（3）审核优化各参建单位的项目安全性设计方案，重点加强对实施方案中安全性、合法性、合理性、功能性的审查；

（4）督促各参建单位做好自身的信息安全和实施安全管理工作，并检查其具体工作的实施；

（5）协助对发生的安全问题进行处置。

8.组织协调

负责协调本项目所涉及的各方之间的工作关系，并协调解决项目建设过程中的各类纠纷。通过口头沟通、书面沟通、必要的会议制度来实施协调工作。

（三）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。

三、服务要求、周期与地点

（一）监理服务要求

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，监理单位应组建具有高度政治责任感、丰富从业经验、能够与采购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、监理工程师等。

2.总监理工程师应承担过类似项目的监理工作，具有信息系统监理师证书及软件造价评估师。

3.总监理工程师不得随意更换，因重大原因确需调整的，须经采购人同意。供应商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，人员调整必须经采购人同意，采购人有权要求更换人员。

4.采购人有权要求供应商保证人员配置的合理性以及团队人员的稳定性,因人员的过失造成采购人的直接经济损失，应赔偿采购人的损失。

（二）服务期限

自委托合同签订之日起，至履约验收合格止。

（三）服务地点

采购方指定地点

（四）考核（验收）标准和方法

1.服务必须等同或优于本项目招标文件“服务内容及要求”所述的标准。若乙方在其响应文件中承诺的技术标准优 于本项目招标文件“服务内容及要求”所述标准的，按投标的承诺执行。

2.中标供应商完成并交付的工作成果需经采购人验收合格，则视为接受。如果在验收时采购人表明不接受中标供应商提交的工作成果并明示不接受的原因,中标供应商应当采取合理之措施进行修改，以达到合同规定的要求。

（五）支付方式

付款条件说明：合同签订后 30 日内支付 100％ ，达到付款条件起 30 日内，支付合同总金额的 100.00%。

（六）违约责任与解决争议的方法

1.本合同履行期间，任何一方发生了不可抗力事件，以致不能履行或不能如期履行本合同，各方协商一致后，发生不可 抗力事件的一方可以免除履行本合同的责任或推迟履行本合同。

2.本合同约定的不可抗力事件包括以下范围：⑴自然原因引 起的事件，如地震、洪水、飓风、寒流、火山爆发、大雪、水灾、冰灾、暴风雨等；⑵社会原因引起的事件，如战争、罢工、政府禁令、封锁、疫情等；

3.发生不可抗力的一方，应于不可抗力发生后 5 天内以书面形式通知对方，通报不可抗力的详尽 情况，提交不可抗力影响履行程度的官方证明文件。未尽告知义务的，不免除违约责任。

（七）其他要求

1.本项目最高限价为 26.54 万元；

2.保证服务质量，本项目兼投不兼中，投标人可以参与多个采购包的投标，但最多只能成为1个采购包的中标单位。评标按采购包顺序进行，采购包1排名第一的中标候选人在后续采购包评审时不推荐为中标候选人。

采购包2：

标的名称：第三方软件测评项目

一、项目目标

1.按照GB/T25000.51-2016《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》及国家或行业相关要求、技术合同以及项目招标采购文件、承建方提供的响应文件、项目设计文档等资料中的技术要求对陕西省市场监督管理局市场经营主体综合业务系统升级改造及整合迁移项目进行检测。

2.测试机构所有检测服务完成后，出具第三方检测报告，报告的内容根据相关标准结合项目的设计文件、招投标文件和合同书，对各项指标合格与否作出评判。

3.测试机构对所出具的检验报告真实性及有效性负责。如因该报告失实或无效造成采购人损失，测试机构承担违约责任并赔偿相应损失。

二、服务原则

1.公平原则：实施方应遵循“面向应用、保证质量、客观公正、诚信守诺”的原则开展软件测试工作。

标准性原则：实施方应依据相关国家标准、行业标准开展测试工作。本测试要求所使用的标准和规范如与实施方所执行的标准不一致时，按较高标准执行。

2.优质服务原则：本测试要求实施方提供的是最低限度的要求，实施方应保证提供符合本测试要求和有关标准的优质服务，并确保测试报告符合项目验收的所有要求。

3.保密原则：对测试服务过程中接触到的各种信息，不得泄漏给任何单位和个人，未经允许不得利用这些信息从事与服务无关的活动。

三、服务要求

1.规范各系统文档资料，协调测试计划时间安排，组织完成测试业务需求分析，编写测试方案计划，并组织实施测试。根据测试结果，编写并提交测试报告，保证测试内容与测试方案一致。

2.严格管理项目参加人员，把控方案、计划、实施工作，确保测试工作按时保质完成；根据信息系统上线和部署要求，合理安排软件测试计划。

3.根据信息系统需求、系统设计编写测试方案、测试计划、测试用例、测试报告等相关文档，确保文档质量。

4.在测试过程中报告发现的缺陷并实时提出优化建议；在承建方完成整改后进行回归测试，验证缺陷和优化建议已得到正确处理且未引入新的缺陷；要求每次测试至少含一轮回归测试；为提高测试效率,应提供现场测试服务。

5.通过实施系统测试,发现和找出系统开发阶段未满足项目设计要求并且影响上线使用的开发设计缺陷，对被测试系统进行评估，为系统上线并最后总体验收使用提供质量保证。

6.根据项目各系统建设情况和系统测试目标，注重性能测试在整个测试过程中的重要性，需将项目设计文档、建设单位能够出具的相关行业标准和其他具体要求列为测试依据，避免漏测部分功能。

7.测评服务团队人数应不少于5人。

四、服务内容

依据国家标准及系统设计文档等要求,检验系统是否满足用户需求,保证信息系统工程质量、维护用户和项目承建方双方利益。通过评估系统的需求符合性，对系统功能、性能效率等方面进

行专业的测试，为项目验收提供重要依据。为了保证软件质量，投标供应商应从应用系统的功能、性能效率等质量特性方面开展软件测试，测试内容及描述具体如下：

（一）功能测试

通过设计测试用例、执行用例等获取结果，对系统的功能、业务流程等分别进行测试，保证系统功能正常使用。

（二）性能效率测试

依据招标文件中对相关平台性能要求的描述，考查信息系统关键业务在正常工作量、预期的峰值工作量下的效率情况，主要考虑系统容量特性、时间特性及资源利用状况等效率指标是否符合用户需求，并据此对系统的性能做出全面评价。

1.分析系统用户行为，依据性能需求验证分级部署的信息系统支持高并发处理业务的能力。

2.系统的关键业务，诸如数据采集、数据同步、数据统计等，具备快速响应能力。

3.系统资源利用在合理的数值范围，不超过资源指标的预警值。

4.测试在大用户量、大并发、大数据量和长时间连续运行等条件下，系统的 响应时间和稳定运行情况。

五、商务要求

（一）服务期限

自委托合同签订之日起，至履约验收合格止。

（二）服务地点

采购方指定地点。

（三）考核（验收）标准和方法

1.交付的服务必须等同或优于本项目招标文件“服务内容及要求”所述的标准。若乙方在其响应文件中承诺的技术标准优 于本项目招标文件“服务内容及要求”所述标准的，按投标的承诺执行。

2.测试机构完成并交付的工作成果需经采购人验收合格，则视为接受。如果在验收时采购人表明不接受测试机构提交的工作成果并明示不接受的原因，测试机构应当采取合理之措施进行修改，以达到合同规定的要求。

（四）支付约定

合同签订后 30 日内支付 100%，达到付款条件起 30 日内，支付合同总金额的 100.00%。

六、违约责任与解决争议的方法

1.本合同履行期间，任何一方发生了不可抗力事件，以致不能履行或不能如期履行本合同，各方协商一致后，发生不可 抗力事件的一方可以免除履行本合同的责任或推迟履行本合同。

2.本合同约定的不可抗力事件包括以下范围：⑴自然原因引 起的事件，如地震、洪水、飓风、寒流、火山爆发、大雪、水灾、冰灾、暴风雨等；⑵社会原因引起的事件，如战争、罢工、政府禁令、封锁、疫情等；

3.发生不可抗力的一方，应于不可抗力发生后 5 天内以书面形式通知对方，通报不可抗力的详尽 情况，提交不可抗力影响履行程度的官方证明文件。未尽告知义务的，不免除违约责任。

七、其他要求

1.本项目最高限价为 29.69 万元；

2.保证服务质量，本项目兼投不兼中，投标人可以参与多个采购包的投标，但最多只能成为 1 个采购包的中标单位。评标按采购包顺序进行，采购包 1 排名第一的中标候选人在后续采购包评审时不推荐为中标候选人。

采购包 3：

标的名称：网络安全等级保护测评项目

1、项目背景

为贯彻落实国家信息安全等级保护制度的相关规定,根据信息系统安全等级保护基本要求等技术标准和规范，提高信息系统安全防护水平，落实信息安全等级保护工作，加强信息系统的信息安全管理，防范黑客及恶意代码等对信息系统的攻击及侵害，保障信息系统的安全稳定运行，陕西省市场监督管理局组织开展信息系统等级保护测评项目工作。

2、项目内容

为保障陕西省市场监督管理局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，对陕西省市场监督管理局市场经营主体综合业务系统升级改造及整合迁移项目开展等级保护测评服务工作,本次等保级别为三级。

3，本次项目采购预算：8 万；**付款方式：**自合同签订后一个月内支付中标金额的 100%;

4、报价要求

总价报价：不超过采购预算金额。包括本次项目所需的人工费、所消耗材料、机械机具检测仪器设备、服务费、管理费、规费、利润、税金等所有费用。

5、服务依据及要求

5.1 测评依据

政策法规文件：

《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）

《中华人民共和国网络安全法》

《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）

《关于开展信息安全等级保护安全建设整改工作的指导意见》（公信安 【2009】1429 号）

《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安【2010】303 号）

《关于印发<陕西省信息安全等级保护安全建设整改工作指导意见>的通知》 （陕等保办【2011】2 号）

《陕西省公安厅重要信息系统和重点网站安全执法检查反馈意见》（陕公网字检字【2015】713 号）

标准规范文件：

《计算机信息系统安全保护等级划分准则》（GB 17859-1999）

《信息安全技术网络安全等级保护定级指南》（GB/T 22240-2020）

《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）

《信息安全技术网络安全等级保护测评要求》（GB/T 28448-2019）

《信息安全技术网络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测试评估技术指南》（GB/T 36627-2018）

《信息安全技术网络安全等级保护安全管理中心技术要求》（GB/T 36958- 2018）

《信息安全技术信息安全风险评估规范》（GB/T 20984-2007）

5.2 服务总体要求

5.2.1 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，通过静态分析、渗透测试、综合评估等程序对我单位信息系统的安全保护状况进行测评，找出其与《网络安全等级保护基本要求》对应级别的差距，及时发现系统存在的安全问题，针对等保测评中发现的各种安全风险，提出适宜的安全整改建议，提供整改技术支持。

等级测评分安全技术及安全管理两大方面共十个层面的单元测评,以及在此基础上进行的系统整体测评和后续的风险分析。

单元测评：

1）物理环境测评：包括位置、访问控制、防盗窃防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电磁防护等内容。

2）网络系统测评：包括网络架构、网络访问控制、网络安全审计、边界完整性检查、网络入侵防范、网络恶意代码防范、网络设备防护等内容。

3）主机与数据库测评：包括主机与数据库身份鉴别、主机与数据库访问控制、主机与数据库安全审计、主机与数据库入侵防范、主机恶意代码防范、信息资源安全、资源控制等内容。

4）应用系统测评：包括应用系统身份鉴别、应用系统访问控制、应用系统安全审计、剩余信息保护、通信完整性、通信保密性、抗抵赖、软件容错、资源控制等内容。

5）数据及备份恢复测评：包括数据完整性、数据保密性、备份和恢复等内容。

6）安全管理制度测评：包括管理制度、制定和发布、评审和修订等内容；

7）安全管理机构测评：包括岗位设置、人员配备、授权和审批、沟通和合作、审核和检查、资金保障等内容。

8）人员安全管理测评：包括人员录用、人员离岗、人员考核、安全意识教育和培训、外部人员访问管理等内容。

9）系统建设管理测评：包括系统定级、安全方案设计、产品采购、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、系统备案、等级测评、服务商选择等内容。

10）系统运维管理测评：包括环境管理、资产管理、介质管理、设备管理、监控管理和安全管理中心、网络安全管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理等内容。

整体测评：

整体测评是对单元测评中发现的问题进行系统整体测评分析,包括从安全控制点间、层面间、区域间和系统结构等方面进行安全测评。

5.2.2 渗透测试服务要求：

渗透性测试是通过模拟恶意黑客的攻击方法，来对计算机网络的安全性进行检测评估的过程。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给甲方，由此证实甲方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。

5.2.3 售后服务要求

- 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，收到陕西省市场监督管理局的服务请求，测评单位工程师在 2 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。
- 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，要与我局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。
- 电话支持服务：每天 24 小时不间断的电话支持服务，解答甲方在系统运行过程中遇到的安全问题，及时提出解决问题的建议和操作方法。电话响应时间不超过 10 分钟，到达现场时间不超过 3 小时，解决问题不超过 24 小时。

5.2.4 其他要求

- 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员书面报备，并供更换测评师资质证明。

- 服务商需在中标后，协助我局开展备案资料梳理工作，并协助我局取得公安部门办理的等级保护备案证。
- 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，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。
- 服务商须服从陕西省市场监督管理局业务信息系统的统一协调，且必须在项目实施期间由服务商派驻有丰富实施经验的测评师为项目实施团队，全程参与项目实施，现场检测工时必须符合国家相关标准。

5.3 测评指标

5.3.1 三级要求指标

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；
		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	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；
		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。
	访问控制	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；
		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。
	入侵防范	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。
	恶意代码和垃圾邮件防范	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；
		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。
	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、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。
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；
		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。
		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热冗余，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；
		b）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；
		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。
安全建设管理	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。
安全运维管理	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。
	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	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

	理	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。
	应急预案管理	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，事后教育和培训等内容；
		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。

5.4 测评原则

5.4.1 标准性

在项目实施过程中严格按照 GB/T22239-2019、GB/T28448-2019、GB/T28449-2018、GB/T36627-2018 等标准中规定的评测要求、评测方法等进行项目实施。

5.4.2 客观公正性

在没有偏见和最小主观判断情形下，按照测评双方相互认可的测评方案， 基于明确定义的测评方法和过程，实施测评活动。

5.4.3 规范行为

严格按照测评指导书的使用规范的测评技术进行测评， 准确记录测评证据； 不擅自评价测评结果；不将测评结果复制给非测评人员；对被测单位的敏感信息或工作秘密，在指定场所查看，查看后立即归还。

5.4.4 规避风险

充分评估测评可能对被测系统带来的影响，揭示风险，协助开展预防措施规避风险。签订现

场测评授权书、保密协议。及时与测评委托单位沟通，从而保证项目执行的效果。

5.4.5 结果完善性

测评所产生的结果是在对测评指标的正确理解下所取得的良好的判断。在测评实施过程中应当使用正确的方法以确保其满足了测评指标的要求。

6、项目验收

项目验收方法：乙方出具《信息安全等级保护测评报告》并协助取得《信息系统安全等级保护备案证明》。

7、保密要求

乙方承担被测评单位敏感信息的保密责任，在项目实施过程中，双方需要复制对方提供的相关资料时，应提交书面申请，在得到对方书面同意后方可复制，并将数据内容记录成表，签字确认。

未经双方书面同意，不得向第三方透露项目和涉及双方的信息安全、技术成果的任何内容。

项目结束后，双方必须互相确认测评过程中提供的相关资料，相互承担保密责任。

8、其他

1、供应商应根据上述因素结合其他方面因素自行考虑含入磋商报价中，采购人不因供应商磋商报价中的任何遗漏而予以增加或补偿费用，磋商报价表中标明的价格，在合同执行过程中，不得以任何理由变更。

2.保证服务质量，本项目兼投不兼中，投标人可以参与多个采购包的投标，但最多只能成为1个采购包的中标单位。评标按采购包顺序进行，采购包1排名第一的中标候选人在后续采购包评审时不推荐为中标候选人。

采购包4：

标的名称：密码应用性安全评估项目

一、测评方案

1.1.1 测评概述

为全面贯彻总体国家安全观和网络强国战略，做好国产密码应用推进工作，深入贯彻落实习近平总书记关于核心技术自主可控重要批示精神，需要加强商用密码应用的工作部署和推进普及，在保证商用密码应用大力推广和普及的同时，做好网络与信息系统的商用密码应用安全性评估，确保商用密码应用的合规、正确、有效。

1.1.2 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。测评结论作为省局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：陕西省市场监督管理局市场经营主体综合业务系统升级改造及整合迁移项目

供应商需提供整改建议咨询服务。

1.1.3 测评依据

法律法规：

- 《中华人民共和国密码法》
- 《中华人民共和国电子签名法》
- 《中华人民共和国网络安全法》
- 《中华人民共和国个人信息保护法》
- 《中华人民共和国数据安全法》
- 《商用密码管理条例》
- 《国家政务信息化项目建设管理办法》
- 《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》

行业标准及其他依据：

- GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》
- GB/T 43206-2023《信息安全技术 信息系统密码应用测评要求》
- 《商用密码应用安全性评估管理办法》
- 《商用密码检测机构管理办法》
- 《系统密码应用方案》
- 密码应用管理相关制度文件

术语和定义

下列术语和定义适用于本文件

（1）机密性

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

数据没有遭受以非授权方式所作的篡改或破坏的性质。

（3）真实性

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）不可否认性

证明一个已经发生的操作行为无法否认的性质。

（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

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。

1.1.4 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。

1.2 密码应用安全性评估测评实施

1.2.1 测评目标

对信息系统所使用的密码算法、密码技术、密码产品、密码服务进行合规性测评。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；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；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。从信息系统的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、管理制度、人员管理、建设运行、应急处置对其密码应用基本要求进行测评,验证信息系统的商用密码应用基本要求是否达到其所对应网络安全等级保护级别的密码应用安全保护能力，是否满足对应安全等级的保护要求。

1.2.2 测评方法

1.2.2.1 测评方式

本次密评的主要方式有：访谈、文档审查、配置审查、工具测试、实地察看。

1.2.2.2 测评工具

对省局业务系统进行验证测试，要求服务商具备专业的测评工具，测评工具需满足如下配置要求：

（1）采用的测评工具必须获得正版授权，并在有效期内，不得使用盗版软件；

（2）采用的测评工具应为正版、合法厂商提供，能够对产品进行持续更新并提供质量和安全保障；

（3）测评工具不会对采购人系统和网络产生破坏或负面影响。

1.2.2.3 风险分析及防范措施

服务商应制定风险防范措施，针对测评阶段可能面临的风险制定风险规避措施，应包含测评环节各类常见风险。

1.2.3 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 GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》中对应级别的安全要求作为密码测评的基本指标。

此次待测系统为三级，本次测评指标范围,如表 1 所示。

测评范围内的测评指标：

表 1　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
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	管理制度
25		人员管理
26		建设运行

27		应急处置

1.2.4 测评内容

依据《信息安全技术信息系统密码应用基本要求》（GB/T39786-2021）《信息安全技术信息系统密码应用测评要求》（GB/T43206-2023）和系统自身的安全性需求分析，对待测系统进行密评工作，服务内容包括：物理和环境安全测评、网络和通信安全测评、设备和计算安全测评、应用和数据安全测评，密钥管理测评、安全管理测评、整体测评与风险评估、提出系统整改建议等，结合量化评估准则，输出测评结果。

根据项目内容要求,以电子版或纸版形式按需求输出成果,并针对省局的咨询进行及时反馈，方式不限于现场支撑、邮件、电话或报告。

密评现场工作完成后，立足于测评获取的数据记录、证据文件、信息资料等，对评估发现的问题提出整改建议,并按照国家密码管理局要求包含的内容或参考模板编制交付正式的密码应用安全性评估报告。

该项目提交的文档包括但不限于：

（1）提交相关系统的《商用密码应用安全性评估报告》；

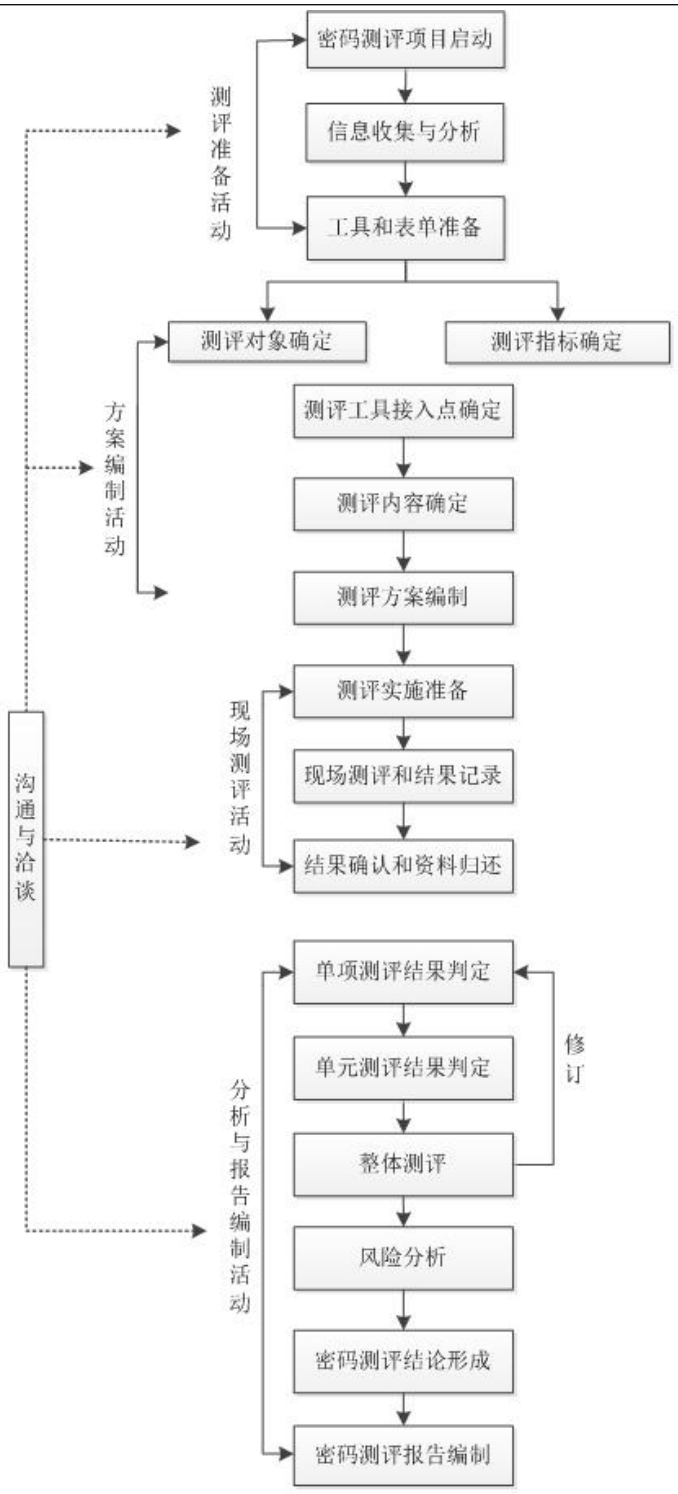
（2）整改建议书；

（3）其他服务资料等。

提交形式：纸质资料一式三份，电子版资料一份。

服务期限内，提供密码应用安全性评估相关问题的咨询；若有需要，辅助省局进行密码应用安全性评估相关备案、培训等工作。

1.3 测评实施流程



密码应用安全性测评实施流程图

1.4 测评实施计划

1.4.1 项目组构成

1.4.1.1 工作实施组

工作实施组负责具体项目的实施与测评工作，工作实施组由省局、测评机构组成工作实施组具体负责测评工作推进实施并向主管部门汇报沟通，测评机构成立测评实施小组，负责省局的商用密码应用安全性测评工作。

1.4.1.2 项目协调小组

项目协调组由省局委派相关人员组成，能够在必要时有效调动其他部门人员。测评机构与省局分别成立项目协调小组协助测评实施小组做好测评工作。

1.4.2 项目实施计划

表 2　项目实施计划表

阶段	任务	
测评准备阶段	实施方案制定	内部项目启动会议
		根据系统规模成立项目组、编制项目计划书
		与被测方沟通，填写信息采集表
		实施方案编写
	测评对象确定	被测系统整体结构、边界、网络区域、重要节点、测评对象等
	测评指标确定	选择相应等级的安全要求作为测评指标
	测评工具接入点确定	结合网络拓扑图，选择测试路径
	测试内容确定	确定单元测评
	测评方案编制	测评内容、测评实施计划
现场测评阶段	现场测评准备	召开现场首次会议。授权书、确认资源、必要的测评程序更新
	现场测评和结果记录	人员访谈、文档审查、上机验证、工具测试
	结果确认和资料归还	召开现场结束会议，确认现场问题。
非现场综合	结果判断、整体测评、风险分析	
报告出具阶段	综合评估及报告生成	

二、预期成果交付物及服务期限、付款方式

1、密码测评工作结束后，根据测评内容记录系统的密码应用现状，出具系统的《商用密码应用安全性评估报告》。测评报告中以密码应用基本要求为基准，逐项比对被测系统密码应用的符合性、规范性和正确性，对与标准存在差异的检查项。

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》	电子和纸质
2.	《整改建议书》	电子和纸质

2、服务期限：自甲方通知入场评测之日起 30 个自然日内出具《商用密码应用安全性评估报告》和《整改建议书》。

3、付款方式：自合同签订后一个月内支付中标金额的 100%

4、保证服务质量，本项目兼投不兼中，投标人可以参与多个采购包的投标，但最多只能成为 1 个采购包的中标单位。评标按采购包顺序进行，采购包 1 排名第一的中标候选人在后续采购包评审时不推荐为中标候选人。