报名二维码

采购需求

一、项目背景

为进一步做好网络安全等级保护、商用密码应用安全性评估、信息安全风险评估及数据安全风险评估工作，现需要采购具有相关资质的专业测评机构（以下简称投标人）对采购人相关信息系统开展等级保护测评、商用密码应用安全性评估、信息安全风险评估及数据安全风险评估服务，提出整改建议并协助采购人完成中、高风险问题整改，提供符合采购人要求的相关测评报告，协助采购人完成信息系统等保系统（含等保一级系统）的备案更新，对商用密码应用安全性评估发现的问题进行改造。

二、项目内容

（一）采购内容

★本项目涉及的服务内容主要包括但不局限于以下内容,投标文件应包含项目技术方案和项目实施方案，项目实施参照标准及依据（详见三、项目需求）。

序号	服务名称	服务内容	服务期限
1	等级保护测评服务	投标人对青岛市税务局等保三级系统、二级系统进行等级保护测评，并协助完善整改。	自合同签订之日起一年
2	应用系统商用密码应用安全性评估服务项目	投标人对青岛市税务局等保三级系统的关键基础设施、重要应用、网络进行商用密码应用安全性评估,并协助完善整改。	自合同签订之日起一年
3	信息安全风险评估服务项目	投标人对青岛市税务局等保三级系统进行信息安全风险评估，并协助进行整改。	自合同签订之日起一年
4	数据安全风险评估服务项目	投标人对青岛市税务局所有信息系统进行数据安全风险评估，并协助进行整改。	自合同签订之日起一年
5	应用密码安全性改造服务	投标人对青岛市税务局 7 个重要网络与信息系统的基础设施、重要应用、网络商用密码应用安全存在的问题进行改造。	自合同签订之日起一年

（二）项目实施要求

#1. 等级保护测评服务实施范围包含但不限于采购人采购人 7 个等保三级,2 个等保二级网络与信息系统的基础设施、应用、网络。

#2. 应用系统商用密码应用安全性评估服务范围包含但不限于采购人 7 个重要网络与信息系统的基础设施、重要应用、网络行商用密码应用安全性评估，并协助完善整改。

#3. 信息安全风险评估服务实施范围包含但不限于采购人采购人 7 个网络与信息系统的基础设施、应用、网络进行信息安全风险评估，并协助进行整改。

#4.数据安全风险评估服务项目包含但不限于采购人7个重要网络与信息系统的基础设施、重要应用、网络信息系统进行数据安全风险评估，并协助进行整改。

#5.应用密码安全性改造服务实施范围包含但不限于采购人7个重要网络与信息系统的基础设施、重要应用、网络商用密码应用安全存在的高风险问题。

（三）其他要求

★1.投标人应具有有效期内公安部三所颁发的《网络安全等级测评与检测评估机构服务认证证书》或《网络安全服务认证证书等级保护测评服务认证》。（需提供复印件，并由投标方盖章确认）

★2.投标人应具有有效期内国家密码管理局颁发的《商用密码检测机构资质证书》（业务范围包括但不限于商用密码应用安全性评估）。（需提供复印件，并由投标方盖章确认）

三、项目需求

（一）网络安全等级保护测评要求

#投标人对不少于7个三级系统和2个二级系统，按照《信息安全技术网络安全等级保护基本要求》（等保2.0）标准开展等级保护测评工作，找出系统现状与相关标准要求之间的差距和问题，提出切实可行的整改建议，协助开展相关的安全整改工作，并对整改结果进行复测，直至测评通过。根据采购人需要，在2025年11月30日前出具正式等级保护测评报告，若新增系统或系统重大变更需要等保测评或重新出具报告的一并包含在本项目范围内。具体评测内容详见以下内容：

#（1）物理安全测评

物理安全测评涉及的测评对象主要为采购人网络信息设施部署机房和相关的安全文档；测评主要关注机房在物理位置选择、物理访问控制、供电等方面的安全保护能力，具体测评指标至少包含下表内容。投标人提供的服务方案要求包含：“物理安全测评涉及的测评对象主要为采购人网络信息设施部署机房和相关的安全文档；测评主要关注机房在物理位置选择、物理访问控制、供电10等方面的安全保护能力”等内容。

序号	安全子类	测评指标描述

1	物理位置的选择	机房物理场所在位置上是否具有防震、防风和防雨等多方面的安全防范能力。
2	物理访问控制	信息系统在物理访问控制方面的安全保护能力。
3	防盗窃和防破坏	信息系统是否采取了必要的安全措施预防设备、介质等丢失和被破坏。
4	防雷击	信息系统是否采取相应的措施预防雷击。
5	防火	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	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	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	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	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	信息系统是否具备一定的电磁防护能力。

#（2）网络安全测评

网络安全测评主要关注采购人信息系统的结构安全、访问控制、安全审计等6方面的安全保护能力，具体测评指标至少包含下表内容。投标人提供的服务方案要求包含:“网络安全测评主要关注采购人信息系统的结构安全、访问控制、安全审计等6方面的安全保护能力”等内容。

序号	安全子类	测评指标描述
1	结构安全	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	访问控制	测试系统对外暴露漏洞情况等，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	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。
4	边界完整性检查	测评分析信息系统私自联到外部网络的行为。

5	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。
6	网络设备防护	测评网络设备自身的安全防范能力。

#（3）主机安全测评

主机安全测评关注采购人信息系统的服务器操作系统(包括安全性增强软件系统，如防病毒软件）和数据库管理系统在身份鉴别、访问控制、安全审计等 6 个方面的安全保护能力，具体测评指标至少包含下表内容。投标人提供的服务方案要求包含“采购人信息系统的服务器操作系统（包括安全性增强软件系统，如防病毒软件）和数据库管理系统在身份鉴别、访问控制、安全审计等 6 个方面的安全保护能力”等内容。

序号	安全子类	测评指标描述
1	身份鉴别	服务器的身份标识与鉴别和用户登录的配置情况。
2	自主访问控制	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	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	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	服务器的恶意代码防范情况。
6	资源控制	服务器对单个用户的登录方式、网络地址范围、会话数量等的限制情况。

#（4）应用安全测评

应用安全测评关注采购人信息系统的业务应用软件在身份鉴别、访问控制、安全审计等 7 个方面的安全保护能力，具体测评指标至少包含下表内容。投标人提供的服务方案要求包含“采购人信息系统的业务应用软件在身份鉴别、访问控制、安全审计等 7 个方面的安全保护能力”等内容。

序号	安全子类	测评指标描述

1	身份鉴别	应用系统的身份标识与鉴别功能设置和使用配置情况;应用系统对用户登录各种情况的处理,如登录失败处理、登录连接超时等。
2	访问控制	应用系统的访问控制功能设置情况,如访问控制的策略、访问控制粒度、权限设置情况等。
3	安全审计	应用系统的安全审计配置情况,如覆盖范围、记录的项目和内容等; 检查应用系统安全审计进程和记录的保护情况。
4	通信完整性	应用系统客户端和服务器端之间的通信完整性保护情况。
5	通信保密性	应用系统客户端和服务器端之间的通信保密性保护情况。
6	软件容错	应用系统的软件容错能力,如输入输出格式检查、自我状态监控、自我保护、回退等能力。
7	资源控制	应用系统的资源控制情况,如会话限定、用户登录限制、最大并发连接以及服务优先级设置等。

#（5）数据安全及备份恢复测评

数据安全及备份恢复测评主要关注采购人信息系统的数据完整性、数据保密性和备份和恢复等 3 个方面，具体测评指标至少包含下表内容。投标人提供的服务方案要求包含“采购人信息系统的数据完整性、数据保密性和备份和恢复等 3 个方面”等内容。

序号	安全子类	测评指标描述
1	数据完整性	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。
2	数据保密性	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。

3	数据备份和恢复	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。

#（6）安全管理制度测评

安全管理制度测评主要关注采购人管理制度体系、制定与发布以及评审和修订等 3 方面，涉及安全主管、安全管理人员、管理制度文档、各类操作规程文件和操作记录等，具体测评指标至少包含下表内容。投标人提供的服务方案要求包含“采购人管理制度体系、制定与发布以及评审和修订等 3 方面，涉及安全主管、安全管理人员、管理制度文档、各类操作规程文件和操作记录等”等内容。

序号	安全子类	测评指标描述
1	管理制度	信息系统管理制度在内容覆盖上是否全面、完善。
2	制定与发布	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。
3	评审和修订	信息系统管理制度定期评审和修订情况。

#（7）安全管理机构测评

安全管理机构测评主要关注采购人信息系统岗位设置、人员配备、授权和审批等 5 个方面，涉及安全主管、相关管理制度以及相关工作/会议记录等测评对象，具体测评指标至少包含下表内容。投标人提供的服务方案要求包含“采购人信息系统岗位设置、人员配备、授权和审批等 5 个方面，涉及安全主管、相关管理制度以及相关工作/会议记录等测评对象”等内容。

序号	安全子类	测评指标描述
1	岗位设置	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	信息系统各个岗位人员配备情况。
3	授权和审批	信息系统对关键活动的授权和审批情况。
4	沟通和合作	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	信息系统安全工作的审核和检查情况。

#（8）人员安全管理测评

人员安全管理测评实施过程关注采购人信息系统的人员录用、人员离岗、人员考核等5个方面，涉及安全主管、人事管理人员、相关管理制度以及相关工作记录等对象，具体测评指标包括至少包含下表内容。投标人提供的服务方案要求包含“采购人信息系统的人员录用、人员离岗、人员考核等5个方面，涉及安全主管、人事管理人员、相关管理制度以及相关工作记录等对象”等内容。

序号	安全子类	测评指标描述
1	人员录用	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	信息系统人员离岗时是否按照一定的手续办理。
3	人员考核	是否对人员进行日常的业务考核和工作审查。
4	安全意识教育和培训	是否对人员进行安全方面的教育和培训。
5	外部人员访问管理	对第三方人员访问（物理、逻辑）系统是否采取必要控制措施。

#（9）系统建设管理测评

系统建设管理测评涉及采购人信息系统的系统定级、安全方案设计和产品采购和使用等9个方面，涉及系统建设负责人、各类管理制度、操作规程文件和执行过程记录等测评对象，具体测评指标至少包含下表内容。投标人提供的服务方案要求包含“采购人信息系统的系统定级、安全方案设计和产品采购和使用等9个方面，涉及系统建设负责人、各类管理制度”等内容。

序号	安全子类	测评指标描述
1	系统定级	是否按照一定要求确定系统的安全等级。
2	安全方案设计	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	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	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	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	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	系统运行前是否对其进行测试验收工作。
8	系统交付	是否采取必要的措施对系统交付过程进行有效控制。
9	安全投标人选择	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。

#（10）系统运维管理测评

系统运维管理测评主要关注采购人信息系统的环境管理、资产管理和介质管理等 12 个方面，主要涉及安全主管、各类运维人员、各类管理制度、操作规程文件和执行过程记录等测评对象，具体测评指标至少包含下表内容。投标人提供的服务方案要求包含“采购人信息系统的环境管理、资产管理和介质管理等 12 个方面，主要涉及安全主管、各类运维人员、各类管理制度、操作规程文件和执行过程记录等测评对象”等内容。

序号	安全子类	测评指标描述
1	环境管理	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	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	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	设备管理	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	系统安全管理	是否采取必要的措施对网络的安全配置、网络用户权限和审计日志等方面进行有效的管理，确保网络安全运行。
6	网络安全管理	是否采取必要的措施对系统的安全配置、系统账户、漏洞扫描和审计日志等方面进行有效的管理。
7	恶意代码防护管理	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	密码管理	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。
9	变更管理	是否采取必要的措施对系统发生的变更进行有效管理
10	备份和恢复管理	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。
11	安全事件处置	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。
12	应急预案管理	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。

（二）信息安全风险评估要求

#投标人依据《信息安全技术 信息安全风险评估方法》等国家法律法规要求，针对采购人不少于7个信息系统开展信息安全风险评估工作并出具《信息系统风险评估报告》，发现问题隐患，排查安全风险，根据评估结果和问题风险，提出加强信息安全管理的措施建议等。评估过程中要评价采购人信息系统的整体安全保护能力有没有缺失，是否能够对抗相应等级的安全威胁。信息系统整体测评应从安全控制点间、层面间和区域间等方面进行安全分析和测评，并最后从系统结构安全方面进行综合分析，对系统结构进行安全测评。

#1. 安全控制点安全分析和测评

安全控制点间安全测评主要对同一区域同一层面内的两个或者两个以上不同安全控制点间的关联进行测评分析，其目的是确定这些关联对信息系统整体安全保护能力的影响。

#2. 层面间安全分析和测评

层面间安全测评主要对同一区域内的两个或者两个以上不同层面安全控制点间的关联进行测评分析，其目的是确定这些关联对信息系统整体安全保护能力的影响。

#3. 区域间安全分析和测评

区域间安全测评主要对两个或者两个以上不同物理或逻辑区域间安全控制点间的关联进行测评分析,其目的是确定这些关联对信息系统整体安全保护能力的影响。

通过对采购人信息系统的单元测评、安全控制点之间的测评、层面分析和区域分析，从而评价信息系统面临的主要安全风险，并提出整改建议，协助进行整改方案的评审，最终使其符合信息系统所定等级应达到的安全防护要求，将信息系统的安全风险降至最低。

#4.系统结构安全测评

系统结构安全测评主要考虑信息系统整体结构的安全性和整体安全防范的合理性。

在掌握系统的物理布局、网络拓扑、业务逻辑（业务数据流）、系统实现和集成方式等基础上，结合系统的业务数据流分析物理布局与网络拓扑之间、网络拓扑与业务逻辑之间、物理布局与业务逻辑之间、不同信息系统之间存在的各种关系，明确物理、网络和业务系统等不同位置上可能面临的威胁、可能暴露的脆弱性等，综合判定系统的整体布局是否合理、主要关系是否简单、整体是否安全有效等。

在熟悉系统安全保护措施的具体实现方式和部署情况后,结合其业务数据流分析不同区域和不同边界与安全保护措施的关系、重要业务和关键信息与安全保护措施的关系等，参照纵深防御的要求，识别系统的安全防范是否突出重点、层层深入，综合判定系统的整体安全防范是否恰当合理等。

（三）商用密码应用安全性评估要求

#投标人按照《信息安全技术-信息系统密码应用基本要求》（GB/T 39786-2021），和国家密码管理局和税务系统密码应用安全性基本要求，对不少于 7 个等保三级系统开展密码应用安全性评估，从密码算法合规性、密码技术合规性、密码产品合规性、密码服务合规性四个方面开展测评工作，找出系统现状与相关标准要求之间的差距和问题，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、管理制度、人员管理、建设运行、应急处置等方面提出安全整改建议，协助采购人落实整改，对整改结果进行复测，直至测评通过。根据采购人需要，在规定时间前出具正式密码应用安全评估报告。

#1. 物理和环境安全

物理和环境安全主要关注采购人信息系统的身份鉴别、电子门禁记录数据完整性、视频记录数据完整性等评估对象，具体测评指标至少包含下表内容。投标人针对“身份鉴别、电子门禁记录数据完整性、视频记录数据完整性等”内容提供评估方案，对测评常见问题及解决方案。

序号	评估名称	评估内容描述
1	身份鉴别	是否使用密码技术的真实性服务来保护物理访问控制身份鉴别信息，保证重要区域进入人员身份的真实性。
2	电子门禁记录数据完整性	检查使用密码技术的完整性服务来保证电子门禁系统进出记录的完整性情况。
3	视频记录数据完整性	检查使用密码技术的完整性服务来保证视频监控音像记录的完整性情况。

#2. 网络和通信安全

网络和通信安全主要关注采购人信息系统的身份鉴别、访问控制信息完整性、通信数据完整性、通信数据机密性等评估对象，具体测评指标至少包含下表内容。投标人针对“身份鉴别、访问控制信息完整性、通信数据完整性、通信数据机密性等”内容提供评估方案，对测评常见问题及解决方案。

序号	评估名称	评估内容描述
1	身份鉴别	检查网络和通信设备的身份标识与鉴别和用户登录的配置情况。
2	访问控制信息完整性	通过抓包分析及验证的方式对访问控制信息的完整性进行分析检查。
3	通信数据完整性	通过抓包分析及验证的方式对通信数据的完整性进行分析检查。
4	通信数据机密性	通过抓包分析及验证的方式对通信数据的机密性进行分析检查。

5	集中管理通道安全	对采用密码技术建立的信息安全通道集中管理网络中安全设备或安全组件的情况进行分析检查。

#3. 设备和计算机安全

设备和计算机安全主要关注采购人信息系统的身份鉴别、远程管理身份鉴别信息机密性、访问控制信息完整性、敏感标记完整性等评估对象，具体测评指标至少包含下表内容。投标人针对“身份鉴别、远程管理身份鉴别信息机密性、访问控制信息完整性、敏感标记完整性等”内容提供评估方案，对测评常见问题及解决方案。

序号	评估名称	评估内容描述
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	远程管理身份鉴别信息机密性	检查系统在用户实施身份鉴别的过程中是否采用密码技术对设备标识信息进行密码保护。
3	访问控制信息完整性	检查各主机相应操作系统或数据库的自主访问控制设置情况，包括安全策略覆盖、访问控制信息完整性情况等。
4	敏感标记完整性	通过访谈系统管理员和安全管理员关于信息系统重要信息资源的敏感标记设置，并且通过相关技术手段进行强制访问控制措施有效性，同时检查敏感标记的完整性。
5	重要程序文件完整性	对重要程序及文件的完整性进行分析检查。
6	日记记录完整性	检查各主机服务器相应操作系统或数据库的日志记录的配置情况，如覆盖范围、记录的项目和内容等；检查安全审计记录的保护及完整性验证情况。

#4. 应用和数据安全

应用和数据安全主要关注采购人信息系统的身份鉴别、访问控制、数据传输安全、数据存储安全等评估对象，具体测评指标至少包含下表内容。投标人针对

“身份鉴别、访问控制、数据传输安全、数据存储安全等”内容提供评估方案，对测评常见问题及解决方案。

序号	评估名称	评估内容描述
1	身份鉴别	检查业务应用系统的身份标识与鉴别功能设置和使用配置情况；
2	访问控制	检查业务应用系统的访问控制功能设置情况，如访问控制的策略、访问控制粒度、权限设置情况等。
3	数据传输安全	检查业务应用系统的数据传输机制、加密算法等信息。
4	数据存储安全	检查数据存储的环境及安全性。
5	日志记录完整性	检查业务应用系统的日志配置情况及完整性保证措施。
6	重要应用程序的加载和卸载	检查重要应用程序的加载与卸载情况。
7	抗抵赖	检查业务应用系统客户端和服务器端之间的不可抵赖性情况。

#5. 密钥管理应用

密钥管理应用主要关注采购人信息系统的密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等环节，具体测评指标至少包含下表内容。投标人针对“密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等环节”内容提供评估方案。

序号	评估名称	评估内容描述
1	密钥生成	分析密码中的随机数的产生是否符合 GM/T 0005 要求
2	密钥存储	密钥的存储是否加密

3	密钥分发	密钥分发是否采取身份鉴别、完整性、机密性的防护措施
4	密钥导入与导出	是否采取安全措施防护非法获取
5	密钥使用	是否明确用途
6	密钥备份与恢复	是否明确密钥的备份策略，及可靠的恢复机制
7	密钥归档	是否采取有效安全的措施保证归档密钥的安全性和正确性
8	密钥销毁	是否具有紧急情况下销毁密钥的措施

#6. 安全管理

安全管理主要关注采购人信息系统的密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等环节，具体测评指标至少包含下表内容。投标人针对“制度、人员、建设、应急”内容提供评估方案。

序号	评估名称	评估内容描述
1	制度	检查密码安全管理制度的制订情况。
2	人员	通过访谈安全主管，检查人员名单等文档，检查关于密码管理的相关规定及岗位设置、职责情况。
3	建设	通过检查相关密码项目文档对密码项目的规划、建设及运行情况进行检查。
4	应急	通过访谈系统运维负责人，检查安全事件的应急预案、记录分析文档、安全事件报告和处置管理制度等过程，评估被评估单位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。

（四）数据安全风险评估要求

#投标人依据《网络安全标准实践指南-网络数据安全风险评估实施指引》等国家法律法规要求，针对采购人不少于 7 个信息系统开展数据安全风险评估工作

并出具《数据安全风险评估报告》，发现问题隐患，排查安全风险，根据评估结果和问题风险，提出加强数据安全管理的措施建议等。投标人应提供全面的数据安全风险评估服务，对重要信息系统的数据对象进行全面梳理探查，并且深入进行数据安全风险检查与分析。

#1.服务内容要求

投标人需负责对重要信息系统数据处理者基本情况、业务和信息系统情况、数据资产情况、数据处理活动情况进行调研，对数据对象梳理和安全评估，主要包括数据安全管理风险识别、数据处理活动风险识别、数据安全技术风险识别、个人信息处理风险识别等方面评估，数据对象的评估范围应覆盖信息系统全安全层面，包括主机操作系统、数据库系统、业务应用软件、网络通信系统、安全防护设施配置、物理环境设施以及数据相关安全管理制度等多个层面，以识别并量化评估系统在数据安全保护上的潜在风险点。

#2.风险识别与分析

投标人须具备成熟的风险评估方法论和检测经验，通过现场访谈、资料查阅、系统测试、数据取证等方式，深入挖掘重要信息系统的数据在数据生命周期安全方面的内外部威胁、技术脆弱性及管理短板，并对数据安全管理问题、数据处理活动问题、数据安全技术问题、个人信息保护问题进行详细的风险识别与量化分析，形成整改总结和建议。

#3.风险评估报告提交

投标人在完成风险评估工作后，需提交一份详尽、客观、具有高度参考价值的数据安全风险评估报告，明确列出各类数据所存在的各类风险，标明风险等级，并阐述可能带来的安全后果，为后续的风险管理工作提供科学依据。

4.重要数据对象检测要求

#（1）数据安全管理风险识别

评估名称	评估点	评估内容描述
1.安全管理制	数据安全制度体系	a）数据安全总体策略、方针、目标和原则制定情况；
		b）数据安全管理工作规划或工作方案制定情况；

度		c）数据分类分级、数据安全评估、数据访问权限管理、数据全生命周期管理、数据安全应急响应、数据合作方管理、数据脱敏、数据加密、数据安全审计、数据资产管理、大数据平台安全等制度建设情况；
	数据安全制度落实	a）网络安全责任制、数据安全责任制落实情况，网络安全和数据安全事件责任查处情况；
		b）数据安全制度落实情况，是否具备操作规程、记录表单等制度落实证明材料；
		c）制度落实监督检查机制。
		d）对数据处理活动定期开展数据安全风险评估的情况；
2.安全组织机构	数据安全组织架构	a）数据安全管理机构和职能设置情况；
		b）数据安全负责人和职能设置情况；
		c）对组织内部的数据安全管理执行情况、数据操作行为等进行安全监督的情况；
		d）数据安全人员和资源投入情况与组织数据安全保护需求适应性。
	数据安全岗位设置	a）数据库管理员、操作员及安全审计人员、安全运维人员等数据安全关键岗位设置情况，及职责分离、专人专岗等原则落实情况；
		b）业务部门、信息系统建设部门、信息系统运维部门数据安全人员设置情况，数据安全管理要求执行情况；
		c）特权账户所有者、关键数据处理岗位等数据安全关键岗位设立双人双岗情况。
3.分类分级管理	数据分类分级保护	a）是否对处理的个人信息和重要数据进行明确标识；
		b）按照数据级别建设覆盖全流程数据处理活动的安全措施情况；
		c）数据分类分级识别或数据资产管理工具建设情况，

		是否具有自动化标识能力，是否具有数据标识结果发布、审核等能力； d）按照相关重要数据目录或规定，评估重要数据并进行重点保护的情况； e）按照相关核心数据目录或规定，评估核心数据并进行严格管理的情况。
4.人员安全管理	人员录用	a）员工录用前背景调查情况； b）数据处理关键岗位人员录用，对其数据安全意识或专业能力进行考核的情况。
	保密协议	a）员工工作纪律和工作要求中是否明确规定员工禁止的数据安全相关行为； b）是否与所有涉及数据服务的人员签订安全责任承诺或保密协议，与数据安全关键岗位人员签订数据安全岗位责任协议； c）在重要岗位人员调离或终止劳动合同前，是否明确并告知其继续履行有关信息的保密义务要求，并签订保密承诺书。
	转岗离岗	a）在人员转岗或离岗时，是否及时终止或变更完成相关人员数据操作权限； b）对终止劳动合同的人员，是否及时终止并收回其系统权限及数据权限，明确告知其继续履行有关信息的保密义务要求。
	数据安全培训	a）对全体人员开展数据安全意识教育培训，并保留相关记录情况；
5.安全威胁和应急管理	安全威胁和事件	a）近 3 年发生的网络安全或数据安全事件信息及其处置、记录整改和上报情况，如事件名称、影响对象、发生时间和频次、发生原因、外部威胁、事件级别、处置措施、整改措施等，重大事件需提供事件调查评

		估报告； b）近 1 年通过安全工具、日志审计、安全测评、合规自查等发现的安全威胁、违规行为及其频率统计； c）实际环境中通过监测系统、检测工具等发现的攻击威胁情况； d）近期公布或曝光的同行业、类似业务模式的威胁事件、威胁预警。
	安全应急管理	a）数据安全事件应急预案制定和修订情况，是否定义数据安全事件类型，明确不同类别事件的处置流程和方法； b）数据安全应急响应及处置机制建设情况，发生数据安全事件时是否立即采取处置措施，是否按照规定及时告知用户并向有关主管部门报告； c）数据安全事件应急演练情况； d）数据处理活动安全风险监测情况，发现数据安全缺陷、漏洞等风险时，是否立即采取补救措施；
6.开发运维管理	开发运维管理	a）新应用开发审核流程建设情况，进行数据处理需求安全合规审核情况； b）开发程序的修改、更新、发布的批准授权和版本控制流程； c）工程实施、验收、交付的安全管理情况； d）对开发代码、测试数据的安全管理情况； e）产品或业务上线前进行安全评估的情况； f）开发测试环境和实际运行环境的隔离情况、测试数据和测试结果的控制情况；

#（2）数据处理活动风险识别

评估名称	评估点	评估内容描述

1.数据收集	数据收集合法正当性	a）数据收集的合法性、正当性，是否存在窃取、超范围收集、未经合法授权收集或者以其他非法方式获取数据的情况，数据收集目的和范围是否合法；
		b）违反法律、行政法规关于收集使用数据目的、范围相关要求，收集数据的情况。
	通过第三方收集数据	a）通过合同协议等合法方式，约定从外部机构采集的数据范围、收集方式、使用目的和授权同意情况；
		b）对外部数据源和外部收集数据进行鉴别和记录的情况；
		c）数据的真实性及来源的可靠性；
		d）对外部数据源和外部收集数据的合法性、安全性和授权同意情况进行审核的情况。
	数据收集方式	a）采用自动化工具访问、收集数据的，违反法律、行政法规或者行业自律公约情况，侵犯他人知识产权等合法权益情况；
		b）采用自动化工具收集时，对数据收集范围、数量和频率的明确情况，收集与提供服务无关数据的情况；
		c）采用自动化工具收集数据以及该方式对网络服务的性能、功能带来的影响情况；
		d）通过人工方式采集数据的，是否对数据采集人员严格管理，要求将采集数据直接报送到相关人员或系统，采集任务完成后及时删除采集人员留存的数据。
	数据收集设备及环境安全	a）采集终端数据泄露风险，检测采集终端或设备的安全漏洞，是否存在数据泄露风险；
		b）人工采集数据泄露风险，通过人员权限管控、信息碎片化等方式，对人工采集数据环境进行安全管控情况；
		c）客户端敏感信息留存风险，检测 App、Web 等客户

		端完成相关业务后，是否及时对缓存数据进行清理，是否留存敏感个人信息或重要数据。
2. 数据存储	数据存储适当性	a）数据存储安全策略和操作规程的建设落实情况；
		b）存储位置、期限、方式的适当性；
		c）永久存储数据类型的必要性；
	逻辑存储安全	a）数据库的账号权限管理、访问控制、日志管理、加密管理、版本升级等方面要求的落实情况；
		b）检测逻辑存储系统安全漏洞，查看安全漏洞修复、处置情况；
		c）实施限制数据库管理、运维等人员操作行为的安全管理措施情况；
		d）脱敏后的数据与可用于恢复数据的信息分开存储的情况；
		e）对敏感个人信息、重要数据进行加密存储情况及加密措施有效性；
		f）数据存储在第三方云平台、数据中心等外部区域的安全管理、访问控制情况；
	存储介质安全	a）存储介质（含移动存储介质，下同）的使用、管理及资产标识情况；
		b）存储介质安全管理规范建设情况，是否明确对存储介质存储数据的安全要求；
		c）对存储介质进行定期或随机性安全检查情况；
		d）存储介质访问和使用行为的记录和审计情况。
3. 数据	传输链路安	a）数据传输安全策略和操作规程的建设落实情况；

传输	全性	b）敏感个人信息和重要数据传输加密情况及加密措施有效性，是否选用安全的密码算法；
		c）个人信息和重要数据传输进行完整性保护情况；
		d）数据传输通道部署身份鉴别、安全配置、密码算法配置、密钥管理等防护措施情况；
		e）数据传输、接收的记录和安全审计情况；
		f）采取安全传输协议等安全措施情况；
	传输链路可靠性	a）网络传输链路的可用情况，包括对关键网络传输链路、网络设备节点实行冗余建设，建立容灾方案和宕机替代方案等情况；
		b）点对点传输中是否存在传输经过第三方、被第三方缓存情况。
4.数据使用和加工	数据使用和加工合法性	a）使用和加工数据时，遵守法律、行政法规，尊重社会公德和伦理，遵守商业道德和职业道德等情况；
		b）是否存在危害国家安全、公共利益的数据使用和加工行为，损害个人、组织合法权益的数据使用和加工行为；
		c）是否制作、发布、复制、传播违法信息；
		d）应用算法推荐技术、深度合成技术提供互联网信息服务的、生成式AI技术提供服务的，是否按照《互联网信息服务算法推荐管理规定》《互联网信息服务深度合成管理规定》等规定开展相关工作。
	数据正当使用	a）数据使用加工安全策略和操作规程的建设落实情况；
		b）数据使用是否获得数据提供方、数据主体等相关方授权；
		c）数据使用行为与承诺或用户协议的一致性；

		d）数据使用加工目的、方式、范围，与行政许可、合同授权等的一致性；
	数据导入导出	a）数据导出安全评估和授权审批流程建设情况；
		b）导入导出审计策略和日志管理机制建设情况；
		c）导出权限管理、导出操作记录情况；
		d）导出数据的存储介质的标识、加密、使用、销毁管理情况；
		e）定期对个人信息和重要数据导出行为进行安全审计情况；
5. 数据提供	数据提供合法正当必要性	a）数据对外提供的目的、方式、范围的合法性、正当性、必要性；
		b）数据提供的依据和目的是否合理、明确；
		c）数据提供是否遵守法律法规和监管政策要求，是否存在非法买卖、提供他人个人信息或重要数据行为；
		d）对外提供的个人信息和重要数据范围，是否限于实现处理目的的最小范围。
	数据提供管理	a）数据提供安全策略和操作规程的建设落实情况；
		b）数据对外提供的审批情况；
		c）签订合同协议情况，是否在合同协议中明确了处理数据的目的、方式、范围、数据安全保护措施、安全责任义务及罚则；
		d）开展共享、交易、委托处理、向境外提供数据等高风险数据处理活动前的安全评估情况；
		e）监督数据接收方到期返还、删除数据的情况；
	数据提供技术措施	a）对外提供的敏感数据是否进行加密及加密有效性；
		b）对外提供数据及数据提供过程的监控审计情况；
		c）对外提供数据时采取签名、添加水印、脱敏等安全

		措施情况； d）跟踪记录数据流量、接收者信息及处理操作信息情况，记录日志是否完备、是否能够支撑数据安全事件溯源； e）数据对外提供的安全保障措施及有效性；

#（3）数据安全技术风险识别

评估名称	评估点	评估内容描述
1.网络安全防护	网络安全防护情况	a）网络拓扑结构、网络区域划分、IP 地址分配、网络带宽设置等网络资源管理情况； b）网络隔离、边界防护等措施的有效性； c）安全策略和配置核查情况； d）网络访问控制、安全审计情况； e）安全漏洞发现及常见漏洞修复、处置情况； f）异常流量、恶意代码和钓鱼邮件发现及处置情况；
2.身份鉴别与访问控制	身份鉴别	a）建立用户、设备、应用系统的身份鉴别机制情况，身份标识是否具有唯一性； b）身份鉴别信息是否具有复杂度要求并定期更换； c）是否存在可绕过鉴别机制的访问方式； d）登录失败时采取结束会话、限制非法登录次数、设置抑制时间和网络登录连接超时自动退出等措施的情况； e）处理重要数据的信息系统，采用口令技术、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鉴别的情况。
	访问控制	a）建立与数据类别级别相适应的访问控制机制情况，是否限定用户可访问数据范围；

		b）是否在数据访问前设置身份认证等措施，防止数据的非授权访问；
		c）数据访问权限与访问者的身份关联情况；
		d）数据访问权限申请、审批机制的建设落实情况；
		e）是否以满足业务实际需要的最小化权限原则进行授权。
	授权管理	a）数据权限授权审批流程建设落实情况，是否明确用户账号分配、开通、使用、变更、注销等安全保障要求，是否对数据权限申请和变更进行审核，
		b）系统管理员、安全管理员、安全审计员等人员角色分离设置和权限管理情况；
		c）系统权限分配表建设及更新情况，用户账号实际权限是否满足最少够用、职权分离原则；
		d）是否存在与权限申请审批结果不一致的情况；
		e）是否存在多余、重复、过期的账户和角色；
3. 监测预警	数据安全风险监测预警	a）安全监测预警和信息报告机制的建设落实情况，是否明确对组织内部各类数据访问操作的日志记录要求、安全监控要求；
		b）异常行为监测指标建设情况，包括 IP 地址、账号、数据、使用场景等，对异常行为事件进行识别、发现、跟踪和监控等；
		c）对批量传输、下载、导出等敏感数据操作的安全监控和分析的情况，是否实现对数据异常访问和操作进行告警；
4. 数据脱敏	数据脱敏	a）数据脱敏规则、脱敏方法和脱敏数据的使用限制情况；
		b）需要进行数据脱敏处理的应用场景、处理流程及操作记录情况；

		c）静态数据脱敏和动态数据脱敏技术能力建设情况；
		d）开发测试、人员信息公示等应用场景的数据脱敏效果验证情况；
5. 数据防泄漏	数据防泄漏	a）数据防泄漏技术手段部署情况，能否对网络、邮件、终端等关键环节进行监控并报告敏感信息的外发行为；
		b）市场上售卖组织业务数据的情况，查看是否能通过公开渠道、开源网站查询到组织业务信息，如代码、数据库信息等；
		c）数据防泄漏技术措施有效性。
6. 数据备份恢复	数据备份恢复	a）数据备份恢复策略和操作规程的建设落实情况；
		b）数据备份的方式、频次、保存期限、存储介质等情况；
		c）提供本地或异地数据灾备功能情况；
		d）定期开展数据备份恢复工作情况；
7. 安全审计	审计执行	a）审计的实施情况；
		b）审计策略和要求的合理性、有效性；
		c）对数据的访问权限和实际访问控制情况进行定期审计的情况，审核用户实际使用权限与审批时的目的是否保持一致，并及时清理已过期的账号和授权；
	日志留存记录	a）对数据授权访问、收集、批量复制、提供、公开、销毁、数据接口调用、下载、导出等重点环节进行日志留存管理情况；
		b）日志记录内容，是否包括执行时间、操作账号、处理方式、授权情况、IP 地址、登录信息等；
		c）日志记录是否能够对识别和追溯数据操作和访问行为提供支撑；
		d）是否定期对日志进行备份，防止数据安全事件导致

		日志被删除； e）日志保存期限是否符合法律法规要求，如网络日志是否保存六个月以上。
	行为审计	a）对网络运维管理活动、用户行为、网络异常行为、网络安全事件等审计情况； b）对数据库、数据接口的访问和操作行为审计情况； c）对数据批量复制、下载、导出、修改、删除等高风险行为的审计情况； d）对个人信息处理活动的合规审计情况。

#（4）个人信息处理风险识别

评估名称	评估点	评估内容描述
1.个人信息处理基本原则	合法、诚信原则	a）通过误导、欺诈、胁迫等方式处理个人信息的情况； b）非法收集、使用、加工、传输他人个人信息的情况； c）非法买卖、提供或者公开他人个人信息的情况； d）是否从事危害国家安全、公共利益的个人信息处理活动； e）个人信息处理活动是否具备《个人信息保护法》规定的合法性事由；
2.个人信息告知	个人信息告知	a）在处理个人信息前，是否以显著方式、清晰易懂的语言真实、准确、完整地公开个人信息处理规则； b）是否告知个人信息处理者的名称或姓名、联系方式，有法律、行政法规规定应当保密或者不需要告知的情形除外； c）个人信息处理规则是否告知个人信息的处理目的、处理方式，处理的个人信息种类、保存期限； d）个人信息处理规则是否告知个人行使《个人信息保护法》规定权利的方式和程序；

		e）告知事项发生变更的，是否将变更部分告知个人；
3.个人信息同意	个人信息同意	a）处理个人信息前是否取得个人同意，同意是否由个人在充分知情的前提下自愿、明确作出，法律规定的例外情形除外；
		b）基于个人同意处理个人信息的，个人信息处理者是否提供便捷的撤回同意的方式，个人是否有权撤回其同意，个人撤回同意是否不影响撤回前基于个人同意已进行的个人信息处理活动的效力；
		c）个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，是否重新取得个人同意。
4.个人信息处理	个人信息保存	a）个人信息的保存期限是否为实现处理目的所必要的最短时间，法律、行政法规另有规定除外；
		b）是否将个人生物识别信息与个人身份信息分开存储。
	个人信息委托处理	a）是否与受托人约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，是否对受托人的个人信息处理活动进行监督；
		b）个人信息受托人是否按照约定处理个人信息，是否超出约定的处理目的、处理方式等处理个人信息；
		c）委托合同不生效、无效、被撤销或者终止的，受托人是否将个人信息返还个人信息处理者或者予以删除，是否违规保留个人信息；
		d）未经个人信息处理者同意，受托人是否转委托他人处理个人信息。
5.敏感个人信息处理	通用规则	a）敏感个人信息处理是否具有特定的目的和充分的必要性，是否对敏感个人信息采取严格保护措施；
		b）处理敏感个人信息是否取得个人的单独同意；

		c）法律、行政法规规定处理敏感个人信息应当取得书面同意的，是否取得个人的书面同意；
	人脸识别数据安全	a）在公共场所安装图像采集、个人身份识别设备，是否为维护公共安全所必需，是否遵守国家有关规定，并设置显著的提示标识；
		b）所收集的个人图像、身份识别信息，是否只用于维护公共安全的目的，未用于其他目的，取得个人单独同意的除外；
		c）开展业务活动时是否限定使用人脸识别技术作为身份鉴别的唯一方式，并且当用户拒绝人脸识别方式时，是否频繁申请授权干扰用户正常使用；

（五）应用密码安全性改造服务要求

#投标人对采购人 7 个重要网络与信息系统的关键基础设施、重要应用、网络商用密码应用安全性评估存在的问题进行改造。服务方案至少包含：网络及通信安全加固，设备和计算安全加固，应用及数据安全加固内容，提供包括但不限数据库透明加密、应用国密传输安全加固、远程管理运维通道加固、国密浏览器，应用身份鉴别加固等，协助对我局对应用密码安全性不合规项进行整改完善，改造完所有系统应满足密评要求。具体内容包括但不限于下表：

序号	服务名称	服务期限
1	数据库加固服务（对不少于三个应用系统的数据库数据存储机密性、完整性内容进行改造，改造完满足密评要求）	自合同签署之日起为期一年
2	应用国密传输信道安全加固服务，针对采购人应用系统的传输信道进行改造，确保传输信道满足国密要求。	自合同签署之日起为期一年
3	远程管理运维通道改造服务，针对采购人运维通道信道进行改造，确保远程管理运维通道满足国密要求。	自合同签署之日起为期一年
4	应用身份鉴别改造服务，针对采购人应用身	自合同签署之日起为期一年

	份鉴别高风险项进行改造，确保应用身份鉴别满足国密要求。	

（六）其他要求

#1.根据采购人需要，等级保护测评报告及风险评估报告需在 2025 年 11 月 30 日前出具正式报告。

★2.本项目若新增系统或系统重大变更导致等保测评、应用系统商用密码应用安全性评估、信息安全风险评估、数据安全风险评估项目需要出具或重新出具报告情况的，一并包含在本项目范围内。

★3.服务期内每年针对采购人内部开展 3 次网络安全培训，培训内容包含以下内容：网络安全政策法规培训，解读网络安全法等相关政策法规的背景、法律条目、深刻含义和应对措施等；网络安全竞赛实战知识培训；有针对性地对重要信息系统管理和运维部门技术人员进行相关培训；等级保护基础知识培训，介绍等级保护相关法律、法规、标准，以及等级保护工作流程、注意事项和典型案例；数据安全及商用密码应用知识培训。

#4.项目实施过程中应服从采购方的统一领导和协调，采购方有权裁决实施方的责任范围，实施方必须执行，在采购方限定的时间内解决问题。如果实施方不能按时完成测评内容，采购方有权中止项目、索赔或拒付款项；

#5.实施方需根据自己的工程实施经验结合采购方的实际需求进一步细化和完善工作任务书，对采购人所有信息系统继续梳理，开展测评，测评完成后出具测评报告及整改建议，并协助落实整改，针对整改结果协助出具整改结果报告。测评报告、整改建议方案、整改结果报告需要同时提供书面纸质版本和电子版本。

#6.在整改过程中，如需现场服务，实施方技术人员应赶到现场协助处理。

#（七）测评依据

投标人应依据国家信息系统网络安全等级保护、商用密码应用安全性评估和数据安全风险评估相关标准和要求开展测评，依据标准包括但不限于如下标准：

GB/T 22239-2019：《信息安全技术 网络安全等级保护基本要求》

GB/T 22240-2019：《信息安全技术 网络安全等级保护定级指南》

GB/T 28448-2019：《信息安全技术 网络安全等级保护测评要求》

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

GB/T 25058-2019：《信息安全技术 网络安全等级保护实施指南》

GB/T 39786-2021 《信息安全技术 信息系统密码应用基本要求》

GB/T 41479-2022：《信息安全技术 网络数据处理安全要求》

GB/T 35273-2020：《信息安全技术—个人信息安全规范》

GB/T 31509-2015 《信息安全技术 信息安全风险评估实施指南》

GB/T 20984-2022 《信息安全技术 信息安全风险评估方法》

GB/T 33132-2016 《信息安全技术 信息安全风险处理实施指南》

GB/T 37988-2019：《信息安全技术 数据安全能力成熟度模型》

TC260-PG-20212A：《网络安全标准实践指南——网络数据分类分级指引》

T/ISEAA 001-2020：《网络安全等级保护测评高风险判定指引》

TC260-PG-2023XX：《网络安全标准实践指南——网络数据安全风险评估实施指引》

四、人员要求

#（一）总体要求

为保障项目按质、按量、按时及有序实施，投标人应承诺对本项目建立稳定的项目团队、管理机构及执行流程。

投标人应详细描述测评人员的组成、资质及各自职责的划分。项目实施人员不少于 8 人，投标人应配置有一定资历及经验的测评人员进行本次测评工作，具体要求如下：

（二）管理团队

★1.项目负责人要求（1 人）

测评负责人具有 3 年以上的等级保护测评或商用密码应用安全性评估从业经验，需提供工作履历等证明材料；

投标文件中提供包括但不限于相应的资格证书复印件;工作经验要求需提供相关佐证材料，包括但不限于人员简介、项目工作经历、合同、社保、应得投标/响应文件复印件等。

2.技术团队

★（1）驻场人员要求（1 人）

提供1名驻场人员，全职服务于本项目且服务时长不少于6个月。驻场人员具有本行业1年以上的等级保护测评或商用密码应用安全性评估从业经验，熟悉数据库透明加密等密码设备操作及部署，在本公司工作满6个月，需提供工作履历、社保等证明材料。

驻场人员结合系统现状，对采购人等保系统进行梳理；参照主管部门要求对采购人备案信息进行更新；参照整改建议协助采购人开展应用系统密码安全性改造升级工作；对评测发现的问题组织复测。

投标文件中提供包括但不限于相应的资格证书复印件；工作经验要求需提供相关佐证材料，包括但不限于人员简介、项目工作经历、合同、社保、应得投标/响应文件复印件等。

★（2）项目组成员要求

项目成员人数至少为6人；

项目组成员具有本行业1年以上的等级保护测评或商用密码应用安全性评估从业经验，并在本公司工作满6个月，需提供工作履历、社保等证明材料；

投标文件中提供包括但不限于相应的资格证书复印件；工作经验要求需提供相关佐证材料，包括但不限于人员简介、项目工作经历、合同、社保、应得投标/响应文件复印件等。

#3.考核要求

中标人需接受采购人对现场安全服务人员的考核要求，按照采购人考核要求制定相关规章制度，对采购人各项考核要求提供实质性响应。

4.★其他要求

投标人须保证实际投入的主要人员（包括项目负责人、项目组成员、驻场人员）与投标时提供的人员一致，且驻场人员应全职服务于本项目，如需变更，须提出书面申请并经采购人同意，且应提供资质和能力比投标时提交的人员相当或更高的人员，若投标人违反本条款，经采购人书面警告后依然不予改正的，采购人有权单方解除合同。

若所派人员不称职，采购人可要求增加或调换人员，投标人应当在收到采购人要求之日起3日内响应，且由此造成的损失由投标人承担。如投标人拒不配合，且经采购人书面警告后依然不予改正的，采购人有权单方解除合同。

投标人首次进场的服务人员在进场后30天内不得更换。投标人首次进场的服务人员在30天内出现人员更换情况的，采购人有权要求投标人每更换1个人员支付合同总价5%的违约金，投标人支付的违约金累计达到或超过合同总价30%的，采购人有权解除合同；投标人造成采购人损失的，仍应承担全部的赔偿责任。

五、管理实施要求

#（一）测评工具要求

安全测评服务过程中所需要的各类工具由投标人负责提供，并向采购人列示。名录最少应包括以下几个方面：检测工具类型（如：端口扫描工具、数据库扫描工具、漏洞扫描工具等）、检测工具名称、检测工具来源（开源、自主研发、采购）等。投标人为了完成工作任务，使用非采购人提供的软硬件产品时，须征得采购人同意，满足采购人正版化要求，并自行承担相应的法律后果。

测评过程中可能使用的安全测评工具包括：

1. 高效率自动化等保测评工具类；

2. 加密算法安全检查工具类；

3. 基于网络传输协议的自动化密码协议分析工具类；

4. 网络安全自动化渗透测试工具类；

5. 综合密评自动化测评工具类；

6. 数据库漏洞扫描工具类；

注：投标人需在投标文件中提供取得上述工具的合法证明材料，如原厂承诺函。

（二）测评实施要求

#1. 本次等级保护测评和商用密码应用安全性评估实施过程中所使用到的工具软件由投标人推荐，经采购人确认后由投标人提供并在测评中使用。投标人应在投标文件中详细描述所使用的安全测评工具使用的方式和时间、对环境和平台的要求以及使用可能对系统造成的风险等；项目实施过程前，应给与详细的风险说明及风险规避措施，确保有效安全开展测评工作。重点阐述内容及响应方案。

#2. 需要时，投标人应承诺指派测评工作经验5年以上的安全技术顾问，为测评工作提供咨询服务，承诺测评过程按照国家相关标准进行，确保项目有质量完成。重点阐述内容及响应方案。

#3. 投标人应具有科学完整的项目管理与风险控制要求，确保项目顺利进行以及达到采购人预期要求。重点阐述内容及响应方案。

#六、保密要求

投标人与采购人签订网络安全保密协议，投标人测评人员签订网络安全保密承诺书。投标人需针对本次实施评估服务过程中收集的数据资料的保密性提供相应的保证措施。

投标人对本规范书中的内容及在应标过程中接触的设备信息、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。

评估的过程数据和结果数据严格保密，确保所有的阅读和使用均得到用户的授权，项目结束后用户提供的所有项目资料和与用户信息资产相关的资料均安全销毁。对由于实施方泄密带来的后果承担相应责任。投标人的保密义务不因合同的终止而终止。

#七、知识转移要求

中标人须按照国家税务总局相关管理规程和要求，将项目执行过程所涉及的相关知识和工作文档按照采购人提出的质量、数量、提供方式、提供时间等要求进行整理，并按照要求转移给采购人。具体要求如下：

1. 中标人须将项目功能优化部分的源代码、需求文档、设计文档、安装使用文档等知识通过文档等形式转移给采购人，并将项目所涉及的其他各类工作文档按照要求进行移交归档。

2. 项目实施过程中，为确保移交文档的一致性和完整性，中标人须按照项目实施计划，分层次、分阶段进行项目文档提交。

3. 项目结束时，中标人须按照项目要求及时向采购人移交项目所有相关文档。

八、履约验收要求

#（一）总体要求

验收名称	验收要求
第 1 次验收	按照《中华人民共和国网络安全法》和税务总局有关文件要求，结合《信息安全技术信息系统密码应用基本要求》

	（GBT/39786-2021）等标准，针对青岛市税务局的信息系统开展网络安全等级保护测评、商用密码安全性评估、信息安全风险评估、数据安全风险评估，对商用密码应用安全性高危问题进行整改，并协助中高危问题完善整改。测评服务完成后，要求提供包括但不限于交付物如下： 《信息系统安全整改建议书》; 《信息系统等级保护测评报告》; 《信息系统安全等级保护备案表》; 《信息系统安全等级保护定级报告》; 《信息系统风险评估报告》; 《信息系统数据安全风险评估报告》; 《商用密码应用安全性评估报告》; 《应用密码安全性改造服务实施方案》。

#（二）项目验收标准及交付物

采购人以本项目需求中相关内容为依据，作为项目验收标准。中标人是否按照本项目需求中定义的各项服务内容和服务管理开展各项工作，工作流程和结果是否符合采购人质量管理要求，是否在规定时间内提交相关工作文档。

按照《中华人民共和国网络安全法》和税务总局有关文件要求，结合《信息安全技术信息系统密码应用基本要求》（GBT/39786-2021）等标准，针对青岛市税务局的信息系统开展网络安全等级保护测评、商用密码安全性评估、信息安全风险评估、数据安全风险评估，对商用密码应用安全性高危问题进行整改，并协助完善整改。

测评服务完成后，要求提供包括但不限于交付物如下：

《信息系统安全整改建议书》；

《信息系统等级保护测评报告》；

《信息系统安全等级保护备案表》；

《信息系统安全等级保护定级报告》；

《信息系统风险评估报告》；

《信息系统数据安全风险评估报告》；

《商用密码应用安全性评估报告》；

《应用密码安全性改造服务实施方案》。

九、其他要求

（一）★税收信息化项目开发和应用管理工作要求

投标人在采购以及后续项目实施过程中，应严格遵守税务总局税收信息化项目开发和应用管理工作要求。对于违反合同约定的，依据合同约定及政府采购有关规定，采购人可采取要求限期改正、在应付合同金额中扣除违约金、解除合同等措施；对于存在严重违法失信行为的，由采购人按规定推送财政部纳入政府采购严重违法失信行为记录名单。

（二）★供应链安全管理要求

1、人员资格要求

（1）签订承诺书。投标人应严格落实国家税务总局网络安全和保密管理要求，承担技术支持人员的网络安全和保密管理责任，按采购人要求签订协议和承诺书。

（2）开展背景审查。投标人承担技术支持人员背景审查工作，提供其身份证明、履历、家庭成员及主要社会关系、无犯罪记录证明等材料，并提交采购人进行备案。

（3）设置网络安全负责人（由驻场运维人员兼任）。投标人为本项目配备一名网络安全负责人，该负责人具备独立决策能力并保持相对稳定，在项目实施的全过程负责网络安全工作，组织落实各项网络安全要求。

2、日常行为规范要求

（1）工作能力要求。投标人负责对技术支持人员进行资格条件、工作胜任力以及网络安全能力评估，对技术支持人员承担的工作进行安全保密风险分析，明确技术支持人员工作范围和边界，重点防范设备和资料失窃、误操作导致的软硬件故障、工作秘密和税费数据等信息泄露、信息系统越权访问和网络攻击等风险。

（2）教育培训要求。投标人负责对技术支持人员进行网络和数据安全法律法规、网络安全意识、网络安全管理、网络安全技能、保密意识以及网络安全警示教育等培训，上岗前对其进行考核。

3、违约惩戒措施

投标人对供应链安全管理责任落实不到位，造成安全事件或产生不良影响的，采购人按照法律法规及合同约定进行处理。

（三）★信息化服务运维人员要求

本项目涉及信息化服务运维人员的，运维人员应当是运维单位的正式人员，或者是与运维单位签订1年以上劳动合同且实际工作满1年的人员，常驻运维人员应当为技术骨干。

#（四）应急响应要求

当现场测评人员不能很好解决问题或发生紧急事件，需要二线支持人员到采购人现场进行事件处理时，必须5分钟内组织线上应急小组就位，在2小时内到达故障现场并提出故障解决方案，3小时内恢复系统正常运行，应急响应不再收取任何服务费用。

（五）★廉政要求

为进一步落实全面从严治党要求，构建亲清新型政商关系，加强税务信息化项目建设过程中的党风廉政建设和反腐败工作，确保项目建设规范、廉洁推进，投标人在参与税务部门信息化项目工作过程中，需严格遵守法律法规、规范履行合同，积极协助税务部门开展廉政风险防控工作。请严格遵守并落实如下要求：

1. 积极发挥廉政风险防控正向作用。投标人有义务配合税务部门在信息化项目工作中加强廉政风险防控，执行有关措施。

2. 健全廉政风险防控机制。投标人有责任在项目管理机制中健全内部廉政防控措施，包括但不限于：对参与本项目的员工提出廉洁行为规范；指定专人对项目实施各环节进行廉政监督；在项目验收过程中提交本项目廉政情况报告等。

3. 杜绝违纪违法行为。投标人及相关项目人员必须严格遵守党纪国法，坚守职业道德，杜绝任何形式的利益输送、权力寻租等违纪违法行为，对甲方工作人员不得实施以下行为：

（1）以各种形式和名义提供礼品、礼金、电子红包、支付凭证、商业预付卡、名贵特产、有价证券、股权、其他金融产品等财物。

（2）以各种形式和名义提供宴请、旅游、健身、娱乐、私人会所等活动安排；代付加班餐费、打车费等。

（3）以讲课费、咨询费等名义，提供或变相提供报酬。

（4）借款、借房、借车，报销应由个人负担的费用。

（5）以无偿、象征性地收取费用等方式提供家政、司机等服务劳务。

（6）其他通过任何形式行贿或输送利益的行为。

4. 信守承诺。投标人应承诺在项目实施过程中，严格遵守国家法律法规合法、诚信经营，杜绝商业贿赂、规范经营活动、公开透明合作、严格内部管理，并签订《税务信息化项目服务商廉洁承诺书》提交甲方负责项目实施的单位。

5. 自觉接受监管。投标人有义务配合税务机关的正常业务监管以及纪检监察、外部审计、督察内审等监督机构对税务信息化项目全过程的监督检查工作，如实提供相关资料和信息，不得隐瞒、篡改或销毁与项目建设有关的文件、数据等资料。

6. 举报和反馈意见。项目执行过程中，投标人有权举报、反馈甲方索贿受贿、吃拿卡要、违反中央八项规定精神等违纪违法行为。项目验收前，应填写《税务信息化项目服务商廉政反馈书》，提交甲方税务机关网络安全和信息化领导小组办公室。

7. 投标人在中标（成交）后需签署《税务信息化项目服务商廉洁承诺书》（附后），并提交至甲方项目实施单位。

8. 信息化项目终验前，投标人需向甲方税务机关网络安全和信息化领导小组办公室提交《税务信息化项目服务商廉政反馈书》。

9.《税务信息化服务商廉洁承诺书》（模版）

税务信息化服务商廉洁承诺书

为深入贯彻落实党中央关于全面从严治党的决策部署，进一步加强税务信息化项目合作中的廉政建设，防范廉政风险发生，确保项目公开、公平、公正推进，我司郑重承诺如下：

一、合法合规经营。严格遵守国家法律法规及税务部门的相关规定，坚持廉洁从业、诚信经营的原则。在合作过程中不以任何形式进行利益输送，维护良好的政商关系。

二、杜绝商业贿赂。加强内部管理，我司及我司员工均不对甲方工作人员实施以下行为：

（一）以各种形式和名义提供礼品、礼金、电子红包、支付凭证、商业预付卡、名贵特产、有价证券、股权、其他金融产品等财物。

（二）以各种形式和名义提供宴请、旅游、健身、娱乐、私人会所等活动安

排；代付加班餐费、打车费等。

（三）以讲课费、咨询费等名义，提供或变相提供报酬。

（四）借款、借房、借车，报销应由个人负担的费用。

（五）以无偿、象征性地收取费用等方式提供家政、司机等服务劳务。

（六）其他通过任何形式行贿或输送利益的行为。

三、规范经营活动。严格按照合同约定履行义务，保证项目质量，按时完成建设任务；在合作过程中不以任何借口拖延工期、虚报成本或谋取私利。

四、公开透明合作。我司承诺在项目实施过程中保持公开透明，主动接受税务部门及纪检监察机构的全程监督，并积极配合任何有关廉洁从业的调查工作。

五、严格内部管理。加强企业内部廉洁教育，确保员工知晓并遵守相关法律法规及廉洁要求；加强项目实施全过程廉洁监督；对于违反廉洁承诺的员工，将严肃处理，并承担相应责任。

六、积极参与监督。在税务信息化项目实施过程中，如发现任何违纪违法行为，将如实反馈问题和意见。

承诺单位（盖章）：_____

法定代表人或授权代表签字：_____

日期：XX 年 XX 月 XX 日

10.税务信息化廉政情况反馈书

税务信息化廉政情况反馈书

项目基本情况	
项目名称（编号）	XXX 税务信息化项目　项目编号
服务商名称	XXX 公司
联系人及电话	联系人：　职务：　电话：123-4567890
项目情况概述	
廉洁承诺履行情况	

反馈项	反馈内容
杜绝商业贿赂	向税务工作人员及其家属赠送礼品、礼金或提供任何形式的宴请、娱乐活动情况。
规范经营活动	按照合同要求，按时完成各阶段任务，确保项目质量和进度情况。
公开透明合作	在项目实施过程中保持信息公开透明，主动接受相关部门的监督和检查情况。
税务人员履职期间廉政情况	
税务人员履职过程存在违纪违规行为	否
	是（说明具体情况）

提交单位（盖章）：XXX 公司

法定代表人或授权代表签字：_____

日期：XX 年 XX 月 XX 日

备注：各单位可结合自身工作实际予以细化补充。

十、商务条件

（一）服务的地点：采购人指定地点。

★（二）服务期限：自合同签订之日起一年。

（三）付款方式：合同服务期满且经验收合格后，中标人提供合格发票，采购人在 10 个工作日内支付合同金额。

（四）履约保证金：不要求提供。

注：★为实质性条款，投标人必须做出响应，如未响应为无效投标。