第三章 技术、服务及其他要求

（注：本章的技术、服务及其他要求中，带“★”的要求为实质性要求。采购人、代理机构应当根据项目实际要求合理设定，并在第五章符合性审查中明确响应要求。）

3.1.采购内容

采购包1:

采购包预算金额（元）: 660,000.00

采购包最高限价（元）: 660,000.00

序号	采购品目名称	标的名称	数量(计量单位)	标的金额（元）	所属行业	是否涉及核心产品	是否涉及采购进口产品	是否涉及强制采购节能产品	是否涉及优先采购节能产品	是否涉及优先采购环境标志产品
1	C16060000 测试评估认证服务	信息安全等保（三级）评测	1.00（项）	660,000.00	软件和信息技术服务业	否	否	否	否	否

是否适用本国产品标准:

采购包1：否

报价要求

采购包1:

序号	报价内容	数量（计量单位）	最高限价	价款形式	报价说明
1	信息安全等保（三级）评测	1.00（项）	660,000.00	总价	无

★注：本采购包涉及采购货物的，供应商响应产品应当明确品牌和规格型号并指向唯一产品，不能指向唯一产品的，应通过报价表唯一产品说明栏补充说明。

本项目涉及核心产品：

采购包1:

序号	采购品目名称	标的名称	产品名称
不涉及			

注：涉及核心产品的，具体评审规定见第五章。

本项目涉及采购进口产品：

采购包1:

序号	采购品目名称	标的名称	产品名称
不涉及			

★注：不涉及采购进口产品时，供应商不得提供进口产品进行响应；涉及采购进口产品时，如国产产品满足采购需求，也

可提供国产产品进行响应。

本项目涉及强制采购节能产品：

采购包1：

序号	采购品目名称	标的名称	产品名称
不涉及			

★注：响应产品属于《节能产品政府采购品目清单》中政府强制采购的产品，供应商应当提供由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的原件扫描件或“全国认证认可信息公共服务平台”（http://cx.cnca.cn）的认证信息截图，否则作无效响应处理。具体要求详见第五章符合性审查表。

本项目涉及优先采购节能产品：

采购包1：

序号	采购品目名称	标的名称	产品名称
不涉及			

注：响应产品属于《节能产品政府采购品目清单》中优先采购的产品，供应商提供由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的原件扫描件或“全国认证认可信息公共服务平台”（http://cx.cnca.cn）的认证信息截图，可以享受优先采购政策。具体要求详见第五章规定。

本项目涉及优先采购环境标志产品：

采购包1：

序号	采购品目名称	标的名称	产品名称
不涉及			

注：响应产品属于《环境标志产品政府采购品目清单》中的产品，供应商提供由国家确定的认证机构出具的、处于有效期之内的环境标志产品认证证书的原件扫描件或“全国认证认可信息公共服务平台”（http://cx.cnca.cn）的认证信息截图，可以享受优先采购政策。具体要求详见第五章规定。

3.2.技术要求

采购包1：

标的名称：信息安全等保（三级）评测

序号	符号标识	技术要求名称	技术参数与性能指标
			一、项目需求 按照《中华人民共和国网络安全法》和《信息安全等级保护管理办法》等相关要求，采购网络安全等级保护测评服务供应商，对采购人相关信息系统安全等级状况开展等级测评工作，并出具等级保护测评报告。 1、测评内容包括技术和管理测评： （1）技术安全性测评包括：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。 （2）管理安全测评包括：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。 2、测评对象及范围 本次等级保护测评系统包括：

序号	系统名称	级别
1	四川省骨科医院OA系统	三级
2	四川省骨科医院微信公众号	三级
3	四川省骨科医院互联网医院系统	三级
4	四川省骨科医院SPD智能物资运输系统	三级
5	四川省骨科医院门户网站系统	三级
6	四川省骨科医院集成平台系统	三级
7	四川省骨科医院PACS系统	三级
8	医院检验科信息系统（LIS）	三级
9	医院信息系统（含EMR）	三级

3、依据标准

（1）《中华人民共和国网络安全法》

（2）GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》

（3）GB/T28448-2019《信息安全技术 网络安全等级保护测评要求》

（4）GB/T28449-2018《信息安全技术 网络安全等级保护测评过程指南》

（5）GB/T36627-2018《信息安全技术 网络安全等级保护测试评估技术指南》

4、项目具体要求

对信息系统安全等级保护状况进行测试评估，应包括两个方面的内容：一是安全控制测评，主要测评信息安全等级保护要求的基本安全控制在信息系统中的实施配置情况；二是系统整体测评，主要测评分析信息系统的整体安全性。其中，安全控制测评是信息系统整体安全测评的基础。

对安全控制测评的描述，使用工作单元方式组织。工作单元分为安全技术和安全管理两大类。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、安全管理中心五个方面；安全管理测评包括：安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理五个方面。

系统整体测评涉及到信息系统的整体拓扑、局部结构，也关系到信息系统的具体安全功能实现和安全控制配置，与特定信息系统的实际情况紧密相关。测评人员应根据特定信息系统的具体情况，结合本标准要求，确定系统整体测评的具体内容，在安全控制测评的基础上，重点考虑安全控制间、层面间以及区域间的相互关联关系，测评安全控制间、层面间和区域间是否存在安全功能上的增强、补充和削弱作用以及信息系统整体结构安全性、不同信息系统之间整体安全性等。

供应商根据国家对信息安全等级保护工作的相关法律和技术标准要求，结合本项目的系统保护等级开展实施与之相应的检查、访谈、测试工作。

二、测评要求

1、安全物理环境

序号	工作单元名称	工作单元描述

1	物理位置选择	通过访谈、检查机房信息系统物理场所在位置上是否具有防雷、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、检查机房出入口、机房分区域情况等过程，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、检查机房的设备、介质和防盗报警系统等过程，测评信息系统是否具备预防设备、介质等丢失和被破坏的能力。
4	防雷击	通过访谈、检查机房的设计/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、检查机房的设计/验收文档，检查机房防火设备等过程，测评信息系统是否具备防止火灾的发生的能力。
6	防水和防潮	通过访谈、检查机房的除潮设备等过程，测评信息系统是否具备防止水灾和机房潮湿的能力。
7	防静电	通过访谈、检查机房是否具备防止静电的产生的能力。
8	温湿度控制	通过访谈、检查机房温、湿度情况，是否具备对机房内的温湿度进行控制的能力。
9	电力供应	通过访谈、检查机房供电线路、设备等过程，是否具备提供电力供应的能力。
10	电磁防护	通过访谈、检查是否具备电磁防护能力。

2、安全通信网络

序号	工作单元名称	工作单元描述
1	网络架构	通过访谈、检查、测试网络拓扑情况、抽查核心交换机、接入交换机和接入路由器等网络互联设备，测试系统访问路径和网络宽带分配情况等过程，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，以及通信线路、设备硬件冗余，系统可用性保证情况。
2	通信传输	通过访谈、检查、测试通信传输过程的数据完整性和保密性保护情况。

3	可信验证	通过访谈、检查通信设备的系统引导、系统程序、配置参数和通信应用程序等进行可信验证及应用程序的关键执行环节进行动态可信验证的保护情况。

3、安全区域边界

序号	工作单元名称	工作单元描述
1	边界防护	通过访谈、检查、测试边界完整性检查设备，测评分析跨域边界的访问控制和数据流通过边界设备的控制措施，非法内联、外联、无线准入控制的监测、阻断等能力。
2	访问控制	通过访谈、检查、测试网络访问控制设备策略部署，测试系统对外暴露安全漏洞情况等过程，测评分析对进出网络的数据流量控制以及基于应用协议和应用内容的访问控制能力。
3	入侵防范	通过访谈、检查、测试网络边界处、关键网络节点检测、防止或限制从内部和外部发起网络攻击行为的防护能力，以及网络行为分析、监测、报警能力，特别是新型网络攻击行为的分析，对攻击行为的检测是否涉及攻击源、攻击类型、攻击目标、攻击事件、入侵报警等方面的防范能力。
4	恶意代码和防垃圾邮件	通过访谈、检查、测试关键网络节点处对恶意代码、垃圾邮件进行检测、防护和清除、恶意代码防护机制的升级和更新维护等情况。
5	安全审计	通过访谈、检查网络边界、网络节点安全审计情况等，测评分析信息系统审计配置和审计记录保护，审计内容等情况。
6	可信验证	通过访谈、检查边界设备的系统引导、系统程序、配置参数和边界防护应用程序等进行可信验证及应用程序的关键执行环节进行动态可信验证的保护情况。

4、安全计算环境

序号	工作单元名称	工作单元描述
1	身份鉴别	通过访谈、检查、测试对登录的用户进行身份标识和鉴别，是否具有不易被冒用的特点，口令应有复杂度要求并定期更换，以及远程管理安全、双因素鉴别等内容。

1	★	一、技术参数	2	访问控制	通过访谈、检查、测试是否启用访问控制功能，依据安全策略控制用户对资源的访问；是否根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限等内容。
			3	安全审计	通过访谈、检查安全审计范围及内容。
			4	入侵防范	通过访谈、检查、测试是否能够检测到对网络节点进行入侵的行为，能够记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警，是否遵循最小化安全装原则、系统服务、默认共享和高危端口、终端接入限制、数据有效性检验、已知漏洞防护等内容。
			5	恶意代码防范	通过访谈、检查、测试是否具有防恶意代码攻击的技术措施或主动免疫可信验证机制，能否及时识别入侵和病毒行为并将其阻断等内容。
			6	可信验证	通过访谈、通过访谈安全员，检查计算设备的系统引导、系统程序、配置参数和应用程序等进行可信验证及应用程序的关键执行环节进行动态可信验证的保护情况。
			7	数据完整性	通过访谈、检查、测试数据在传输和存储过程中的完整性保护情况，包括鉴别数据、业务数据、审计数据、配置数据、视频数据和个人信息等。
			8	数据保密性	通过访谈、检查、测试数据在传输和存储过程中的保密性保护情况，包括鉴别数据、业务数据、审计数据、配置数据、视频数据和个人信息等。
			9	数据备份恢复	通过访谈、检查、测试数据本地备份与恢复功能，异地实时备份功能，以及数据处理系统的热冗余和高可用性保证等。
			10	剩余信息保护	通过访谈、检查、测试边界信息在存储空间被释放或重新分配前是否有效清除，存有敏感数据的存储空间被释放或重新分配前是否有效清除等。
			11	个人信息保护	通过访谈、检查、测试是否仅采集和保存业务必须的用户个人信息，对用户个人信息的访问和使用等。

5、安全管理中心

序号	工作单元名称	工作单元描述
1	系统管理	通过访谈、检查、测试对系统管理员身份鉴别、命令或操作管理、操作审计，以及是否通过系统管理对系统资源和运行进行配置、控制和管理等。

2	审计管理	通过访谈、检查、测试对审计管理员身份鉴别、命令或操作管理、操作审计，以及是否通过审计管理员对审计策略、审计记录进行分析、处理等。
3	安全管理	通过访谈、检查、测试对安全管理员身份鉴别、命令或操作管理、操作审计，以及是否通过安全管理员对安全策略、参数进行配置等。
4	集中管控	通过访谈、检查、测试是否具有特定的管理区域，对分布在网络中的安全设备或安全组件进行集中管控，对网络链路、安全设备、网络设备和服务的运行进行集中监测，对分散在各设备上的审计数据进行收集汇总和集中分析，并确保记录留存符合法律法规要求，对安全策略、恶意代码、升级补丁等安全相关事项进行集中管理，对网络中发生的各类安全事件进行识别、报警和分析等。

6、安全管理制度

序号	工作单元名称	工作单元描述
1	安全策略	通过访谈、检查网络安全工作的总体方针及安全策略是否全面、完善。
2	管理制度	通过访谈、检查管理制度在内容覆盖上是否全面、完善。
3	制定和发布	通过访谈、检查管理制度的制定和发布过程是否遵循规定流程。
4	评审和修订	通过访谈、检查管理制度定期评审和修订情况。

7、安全管理机构

序号	工作单元名称	工作单元描述
1	岗位设置	通过访谈、检查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	通过访谈、检查各个岗位人员配备情况。
3	授权和审批	通过访谈、检查对关键活动的授权和审批情况。
4	沟通和合作	通过访谈、检查内部部门间、与外部单位间的沟通与合作情况。
5	审核和检查	通过访谈、检查安全工作的审核和检查情况。

8、安全管理人员

序号	工作单元名称	工作单元描述

1	人员录用	通过访谈、检查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	通过访谈、检查人员离岗时是否按照规定手续办理。
3	安全意识教育和培训	通过访谈、检查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	通过访谈、检查对第三方人员访问（物理、逻辑）系统是否采取必要控制措施。

9、安全建设管理

序号	工作单元名称	工作单元描述
1	定级和备案	通过访谈、检查是否按照规定要求确定系统的安全等级。
2	安全方案设计	通过访谈、检查整体的安全规划设计是否按照规定流程进行。
3	产品采购和使用	通过访谈、检查是否按照规定的要求进行系统的产品采购。
4	自行软件开发	通过访谈、检查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	通过访谈、检查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	通过访谈、检查建设的实施过程是否采取规定措施使其在机构可控的范围内进行。
7	测试验收	通过访谈、检查系统运行前是否对其进行测试验收工作。
8	系统交付	通过访谈、检查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	通过访谈、检查等级测评、整改情况。
10	服务商选择	通过访谈、检查是否选择符合国家“一：项目需求（3）依据标准”安全服务单位进行相关的安全服务工作。

10、安全运维管理

序号	工作单元名称	工作单元描述
1	环境管理	通过访谈、检查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	通过访谈、检查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	通过访谈、检查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	通过访谈、检查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	通过访谈、检查安全漏洞和隐患识别、处理情况，以及是否定期开展安全测评以及安全问题的应对措施。
6	网络和系统安全管理	通过访谈、检查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。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。
7	恶意代码防范管理	通过访谈、检查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	通过访谈、检查基本配置信息管理情况
9	密码管理	通过访谈、检查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	通过访谈、检查是否采取措施对系统发生的变更进行有效管理。
11	备份与恢复管理	通过访谈、检查是否采取必要的措施对业务信息，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	通过访谈、检查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	通过访谈、检查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	通过访谈、检查外包运维服务商、外包运维保密、服务内容管理是否选择符合国家要求的。

11、安全扩展要求

按照所测评系统的具体情况选用云计算安全扩展要求、移动互联安全扩展要求、物联网安全扩展要求、工业控制系统安全扩展要求。

12、验证测试相关要求

按照等级保护测评要求，测评过程中应配备工具、仪器/设备对信息系统进行验证测试，采用的测评工具的生产商应为正版软件、不得使用盗版软件。

三、测评工作步骤及要求

供应商对信息系统的初次等级测评可以分为：系统梳理、准备活动、方案编制、现场测评、整改加固协助、分析与报告编制。供应商应对等级保护测评各阶段具体工

			作内容进行描述。 1、系统梳理：协助采购人完成待测信息系统梳理工作。 2、准备活动阶段：对被测系统进行调研分析，明确测评对象、测评方法等工作。 3、方案编制阶段：制定信息安全等级保护测评项目计划书、测评实施具体方案，并提交采购人确认。 4、现场测评阶段：对本项目所涉及信息系统进行现场测评，按照等级保护相关标准规范要求从访谈、检查、测试几方面进行测试评估并出具《网络系统安全等级保护整改建议》，并在整改过程中提供技术咨询服务。 5、整改加固协助：协助对测评过程中发现的安全问题进行技术整改加固工作，并进行整改后的回归测评。 6、分析与报告编制：向采购人提交被测信息系统安全等级保护测评报告以及相应文档（包括纸质及电子文档）。 四、项目管理与实施保障 对项目进行管理，通过系统计划、有序组织、专业指导和质量控制，促进项目全面顺利实施，供应商成交后必须提供完整的项目管理方案，并符合以下要求： 1、供应商及其测评人员应当严格执行有关国家信息安全等级保护相关标准和有关规定，提供客观、公平、公正、有效的等级保护测评服务，并承担相应的法律责任。 2、供应商须保证测评活动的公正性和独立性，确保测评结果不受到商业、财务、健康、环境等方面的影响。 3、供应商在对被采购人开展等级保护测评服务之前需与被测评单位签订保密协议，测评过程中向被测评单位借阅的文档资料应在测评工作结束后全部归还被测评单位，未经被测评单位允许，不得擅自复制、保留。 4、供应商的岗位配置要至少配置项目经理、技术负责人、质量主管、测评工程师和渗透测试工程师，其中项目经理、技术负责人、质量主管、测评工程师和渗透测试工程师应独立配置，不能有兼任的情况。 5、测评人员要求 参与此次等级保护测评的供应商其测评人员应具备并符合以下要求： （1）开展此次等级保护测评工作的人员仅限于中华人民共和国境内的中国公民，且无犯罪记录。 （2）测评项目组人员在对开展等级保护测评工作之前需签订保密协议。

3.3.服务要求

3.3.1服务内容要求

采购包1:

序号	符号标识	服务要求名称	服务要求内容

1		其他要求	一、项目技术服务方案 供应商为本项目提供的项目技术服务方案，包括：①项目需求分析；②项目实施流程；③项目实施人员安排；④项目实施时间计划安排；⑤项目实施管理。 二、售后服务方案 供应商为本项目提供售后服务方案，包括，（1）售后服务保障措施；（2）售后服务组织及人员安排；（3）售后服务流程。 三、实施人员能力 （1）拟派本项目的项目经理，具有信息（或网络）安全等级测评师（高级）证书、重要信息系统保护人员CIIP-A（可信计算）证书、注册密码安全专业人员（NSATP-CSP）证书、个人信息保护专业人员认证证书（CCRC-PIPP） （2）拟派本项目的技术负责人，具有信息（或网络）安全等级测评师（高级）证书、信息系统项目管理师证书（高级）、计算机技术与软件专业技术资格证书（软件评测师）、CISP注册信息安全专业人员证书 （3）拟派本项目的质量主管，具有信息（或网络）安全等级测评师（中级）证书、DSO数据安全官证书、商用密码应用安全性评估从业人员考核成绩合格证明、CCSC网络安全能力认证证书（网络安全管理II级或以上） （4）拟派本项目的测评工程师，具有信息（或网络）安全等级测评师（中级）证书、CCSS-M网络安全服务能力评价证书（安全管理能力认证）、注册密码安全专业人员（NSATP-CSP）证书、重要信息系统保护人员（CIIPT-D）证书 （5）拟派本项目的渗透测试工程师，具有信息（或网络）安全等级测评师（高级）证书、注册渗透测试工程师证书（CISP-PTE）、CCSS-R网络安全服务能力评价证书（应急响应能力认证） 四、履约经验 供应商2023年1月1日（含1日）(以合同签订时间为准)至提交响应文件截止日提供类似项目业绩（类似项目业绩指：安全等保评测业绩）
2	★	质量保修范围和保修期	1.质量保修范围：被测系统完成测评后，对被测系统的相关安全问题，供应商需提供7*24小时的电话咨询服务。 2.质量保修期：1年。
3	★	培训要求	采购人在使用前，供应商应对采购人相关操作人员进行有针对性的培训，并保证正常使用（费用均包含在报价中）
4	★	服务期限 （说明:因系统固化原因，3.3.2.商务要求中“服务期限 ”不适用本项目。“交货时间 ”以此为准）	1.合同履行期限：自合同生效之日起 150 日历天 2.履约时间要求：自合同生效之日起40日历天内成交供应商出具《网络系统安全等级保护整改建议》，经采购人整改完成后通知服务单位进行复测，自复测进场后40日历天内出具《网络系统安全等级保护测评报告》）

5	★	付款进度安排 （说明：因系统固化原因，3.3.2商务要求中“付款进度安排”不适用本项目。“付款进度安排”以此为准）	1.自合同签订之日起40日历天内，成交供应商出具《网络系统安全等级保护整改建议》后，达到付款条件起20日历天内，采购人向成交供应商支付合同总金额50%。 2.待成交供应商出具《网络系统安全等级保护测评报告》后，达到付款条件起20日历天内，采购人向成交供应商支付合同总金额50%。

3.3.2.商务要求

采购包1:

序号	符号标识	商务要求名称	商务要求内容
1		服务期限	1.合同履行期限：自合同生效之日起 150 日 2.履约时间要求：自合同生效之日起40日内成交供应商出具《网络系统安全等级保护整改建议》，经采购人整改完成后通知服务单位进行复测，自复测进场后40日内出具《网络系统安全等级保护测评报告》）
2	★	服务地点	四川省骨科医院
3	★	验收、交付标准和方法	详见第二章“履约验收方案”（以供应商提供的《投标（响应）函》中“我单位完全接受和理解本项目采购文件规定的实质性要求”即视为响应）
4	★	支付方式	分期付款
5		付款进度安排	1、进度款，自合同生效之日起40天内成交供应商出具《网络系统安全等级保护整改建议》后，达到付款条件起15日内，支付合同总金额的50.00% 2、尾款，成交供应商出具《网络系统安全等级保护测评报告》后，达到付款条件起15日内，支付合同总金额的50.00%
6	★	违约责任与解决争议的方法	（一）违约责任 1.采购人、供应商双方必须遵守本合同并执行合同中的各项规定，保证本合同的正常履行。 2.采购人逾期支付服务费的，除应及时付足服务外，应向供应商偿付欠款总额万分之三/天的违约金；逾期付款超过60天的，供应商有权终止合同。采购人承担的违约责任最多不超过合同总金额的百分之二十。供应商未按时提供服务或提供的服务未按照本合同及附件约定的，采购人有权要求供应商改正，供应商应向采购人偿付合同总额的万分之三/天的违约金；如供应商在采购人催告后的15日内仍未改正，采购人有权终止合同，供应商则应按合同总价的百分之二十的款额向采购人偿付违约金，并须全额退还采购人已经付给供应商的货款及其利息。 3.如因供应商工作人员在履行职务过程中的疏忽、失职、过错等故意或者过失原因给采购人造成损失或侵害，包括但不限于采购人本身的财产损失、由此而导致的采购人对任何第三方的法律责任等，供应商对此均应承担全部的赔偿责任。 4.任何一方有其他违反本合同情形的，应赔偿守约方全部损失，该损失包括但不限于对守约方所造成的直接损失、可得利益损失、守约方支付给第三方的赔偿费用/违约金/罚款、调查取证费用/公证费、诉讼费用、律师费用以及因此而支付的其他合理费用。 （二）解决争议的方法 争议友好协商解决，如果无法解决，应向采购人所在地的人民法院提起诉讼。

3.4.其他要求

采购包1:

【说明1:“★注:投标人响应产品应当明确品牌和规格型号并指向唯一产品,不能指向唯一产品的,应通过报价表唯一产品说明栏补充说明。”不适用于本项目。】【说明2(本说明无需供应商进行响应):评分标准中所涉及的响应内容,供应商编制于对应的“关联格式”中。若编制投标文件过程中,涉及提供证明材料或单独提供承诺函等,供应商将前述材料编制于第六章响应文件格式-《其他资料》中】【说明3(本说明无需供应商进行响应):因系统原因,无法调整格式,提交响应文件的截止之日起不少于 90 天。响应文件未明确响应有效期或者少于前述规定天数的,其响应文件按无效处理。”不适用于本项目,不作为评审依据。评审依据以此为准:“提交响应文件的截止之日起不少于 90 天”】