**浦东新区“一网统管”项目密码测评服务采购需求**

一、说明

**1 总则**

1.1 供应商应具备国家或行业管理部门规定的，在本市实施本项目所需的资格（资质）和相关手续（如果有），由此引起的所有有关事宜及费用由供应商自行负责。

1.2 供应商提供的服务应当符合磋商文件的要求，并且其质量完全符合国家标准、行业标准或地方标准。

1.3 供应商在磋商前应认真了解项目的实施背景、应提供的服务内容和质量、项目考核管理要求等，一旦成交，应按照磋商文件和合同规定的要求提供相关服务。

1.4供应商对所提供的服务应当享有合法的所有权，没有侵犯任何第三方的知识产权、商业秘密、技术秘密等权利，而且不存在任何抵押、留置、查封等产权瑕疵。如采购人使用该服务构成上述侵权的，则由成交供应商承担全部责任。

★1.5供应商提供的服务必须符合国家强制性标准。

1.6供应商认为磋商文件（包括磋商补充文件）存在排他性或歧视性条款，可在收到或下载磋商文件之日起七个工作日内提出，并附相关证据。

二、项目概况

**2磋商范围与内容**

2.1 项目背景及现状

根据《上海市人民代表大会常务委员会关于进一步促进和保障城市运行“一网统管”建设的决定》和《关于“加快推进城市运行‘一网统管’，提高城市治理现代化水平”的若干建议》等相关文件要求，本项目旨在根据上海市“一网统管”建设要求，结合浦东新区实际情况，围绕智慧城市政府建设中城市运行和政务服务两个关键，聚集城市大脑认知、感知和行动三大能力提升，以全面提升浦东新区城市运行综合管理智能化应用水平为目标，实现“一屏观全域、一网管全城”的总体建设目标。

本项目主要建设内容包括“一网统管”数字基座、“一网统管”三级智能应用等软件开发及配套硬件设备、系统软件、信息安全、密码应用等采购。具体如下：

（一）“一网统管”数字基座

包括数据汇聚系统、数据治理系统、数据指标计算系统、视频汇聚系统、物联感知使能系统、AI 视频智慧感知系统和数据管理系统等功能模块开发。

（二）“一网统管”三级智能应用

包括区城市日常指挥管理、区城市运行体征、区协同事项监管、区城运数字底图、区市民热议事件感知、区重大节日保障、区民情民意智慧感知系统、区城运中心孪生应用、区视频融合展示、区城运单兵、街镇智能综合管理系统和居村联勤联动系统等功能模块开发。

（三）硬件设备

主要包含系统配套的视频汇聚设备、分布式编码器及算力服务器等硬件设备采购及安装。

（四）系统软件、信息安全及密码应用

包括操作系统、数据库、中间件等系统软件采购；政务云区域、本地网络机房等信息安全产品采购；安全认证网关、加密存储服务、数据安全中间件等密码应用产品采购。

2.2 项目磋商范围及内容

本项目是为浦东新区“一网统管”项目提供商用密码应用测评服务，并出具符合规范的《密码应用测评报告》，并协助被测评单位及相关技术支撑单位落实密码应用安全整改工作

2.3 本项目服务期限为自合同签订之日起至项目通过最终验收，并向采购人完整提供相关服务文档之日止。

**3承包方式**

3.1 依照本项目的磋商范围和内容，成交供应商以保质保量的方式实施项目承包。

3.2 本项目不允许分包。

**4合同签订方式**

4.1 本项目合同的标的、价格、质量及验收标准、考核管理、履约期限等主要条款应当与磋商文件和成交供应商响应文件的内容一致，并互相补充和解释。

**5结算原则和支付方式**

5.1 结算原则

5.1.1 本项目合同结算价以审计价为准，供应商的成交价和结算下浮率（如果有）不变，实际工作量以采购人或第三方按照磋商文件规定的验收标准核定为准。

5.2 支付方式

5.2.1 本项目合同金额采用**分期付款**方式，在采购人和成交供应商合同签订后按下款要求支付相应的合同款项。

5.2.2 分期付款的时间进度要求和支付比例具体如下：

（1）项目合同签订，且成交供应商完成全部测评内容并正式提交符合规范的《密码应用测评报告》后30日内，采购人向成交供应商支付合同金额的80%。

（2）项目完成审计后30日内，采购人向成交供应商支付合同尾款。

5.3成交供应商因自身原因造成返工的工作量，采购人将不予计量和支付。

5.4采购人不得以法定代表人或者主要负责人变更，履行内部付款流程，或者在合同未作约定的情况下以等待竣工验收批复、决算审计等为由，拒绝或者延迟支付中小企业款项。如发生延迟支付情况，应当支付逾期利息，且利率不行低于合同订立时1年期贷款市场报价利率。

三、技术质量要求

**6适用技术规范与规范性文件**

（1）《中华人民共和国密码法》；

（2）《商用密码应用安全性评估管理办法》；

（3）《关于规范和加强我市重要网络和信息系统密码应用与安全性评估工作的通知》；

（4）《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）；

（5）《信息安全技术 信息系统密码应用测评要求》（GB/T 43206-2023）；

（6）《信息系统密码应用测评过程指南》（GM/T 0116-2021）；

（7）《信息系统密码应用高风险判定指引》；

（8）《商用密码应用安全性评估量化评估规则》。

各供应商应充分注意，凡涉及国家或行业管理部门颁发的相关规范、规程和标准，无论其是否在本磋商文件中列明，供应商应无条件执行。标准、规范等不一致的，以要求高者为准。

**7磋商内容与要求**

7.1 工作目标与总体要求

依据《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）标准，参照《商用密码应用安全性评估管理办法》、《信息安全技术 信息系统密码应用测评要求》（GB/T 43206-2023）、《信息系统密码应用测评过程指南》（GM/T 0116-2021）、《信息系统密码应用高风险判定指引》、《商用密码应用安全性评估量化评估规则》等技术要求，逐一对信息系统进行密码应用的合规性、正确性、有效性进行安全性评估，通过商用密码应用安全性评估深入查找密码应用的薄弱环节和安全隐患，分析面临的风险，为提升信息系统安全奠定基础。

7.2 本项目磋商内容与具体质量要求（但不仅限于）详见下表。

**服务内容一览表**

项目名称及包件号：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **服务内容** | **具体要求** | **备注** |
| 1 | 安全技术测评 | 包括物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等四个方面的安全测评 |  |
| 2 | 安全管理测评 | 包括安全管理（分为制度、人员、建设和应急四个子模块）的安全测评。 |  |

**说明：此表所列内容为本次磋商核心工作内容，供应商不得缩减。**

7.3具体服务内容

**7.3.1 测评服务总体要求**

（1）供应商应详细描述本次项目的整体实施方案，包括项目概述、密码应用测评方案、测试过程中需使用测试设备清单、时间安排、阶段性文档提交和验收标准等。

（2）供应商应详细描述实施人员的组成、资质及各自职责的划分。供应商应配置有经验的技术人员进行本次项目实施。

（3）本次项目实施过程中所使用到的各种工具软件由供应商推荐，经采购人确认后由供应商提供并在项目中使用。在响应文件中应详细描述所使用的安全技术工具（软硬件型号、功能和性能描述）、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。

（4）本次项目实施过程中所使用到的测评工具，应包括自主密码专用检测工具、 漏洞扫描工具等获得许可的检测工具，对系统数据进行分析，并以分析结果辅证评估报告。

（5）安全技术工具软件运行可能需要的硬件平台（如笔记本电脑、PC、工作站等） 和操作系统软件等由供应商推荐，经采购人确认后由供应商提供并在项目中使用。

（6）项目实施需要的运行环境（如场地、网络环境等）由采购人提供，供应商应详细描述需要的运行环境的具体要求。

**7.3.2测评工作原则**

遵循以下若干原则，是评估结论真实、准确、可信的基础，也是评估组在独立实施评估时，在相似的情况下得出相似结论的前提。本次商用密码应用安全性测评实施方案设计与具体实施应满足以下原则：

（1）客观公正原则：评估实施过程中评估人员应保证在最小主观判断情形下，按照评估双方认可的评估方案，基于明确定义的评估方式和解释，实施评估活动。

（2）经济性和可重用性原则：评估工作可重用已有评估结果，包括商用密码应用安全性评估结果。所有重用结果都应以结果适用于待评估系统为前提，并能够客观反映目前系统的安全状态。

（3）可重复性和可再现性原则：依照同样的要求，使用同样的评估方法，不同的评估机构对每个评估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，前者关注不同评估者评估结果的一致性，后者则与同一评估者评估结果的一致性有关。

（4）结果完善性原则：在正确理解《GB/T39786-2021 信息安全技术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系统的运行状态。评估过程和结果应服从正确的评估方法，确保其满足要求。

**7.3.3测评服务过程及内容要求**

测评服务过程包括四项基本测评活动：测评准备活动、方案编制活动、现场测评活动、分析与报告编制活动。测评方与被测单位之间的沟通与洽谈应贯穿整个测评过程。

（1）测评准备活动

本活动是开展测评工作的前提和基础，主要任务是掌握被测信息系统的详细情况，准备测评工具，为编制密码应用测评方案做好准备。

（2）方案编制活动

本活动是开展测评工作的关键活动，主要任务是确定与被测信息系统相适应的测评对象、测评指标、测评检查点及测评内容等，形成密码应用测评方案，为实施现场测评提供依据。

（3）现场测评活动

本活动是开展测评工作的核心活动，主要任务是根据密码应用测评技术方案分步实施所有测评项目，以了解被测信息系统真实的密码应用现状，获取足够的证据，发现其存在的密码应用安全性问题。

（4）分析与报告编制活动

本活动是给出测评工作结果的活动，主要任务是根据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》的有关要求，通过单元测评、整体测评、量化评估和风险分析等方法，找出被测信息系统密码应用的安全保护现状与相应等级的保护要求之间的差距，并分析这些差距可能导致的被测信息系统所面临的风险，从而给出各个测评对象的测评结果和被测信息系统的评估结论，形成密码应用测评报告。

测评各阶段详细的服务内容如下表：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **测评阶段** | **测评类** | **服务说明** |
| 1 | 评估准备 | 准备阶段 | 编制项目计划书、收集被测系统基本资料并完成调查表格，分析调查结果，准备工具和评估表单 |
| 2 | 方案编制 | 评估方案编制 | 识别并描述被测系统基本情况、确定测评对象、资产和威胁评估、系统定级结果和测评指标、确定检查点和检查方法、确定单元测评内容 |
| 3 | 总体测评 | 总体要求 | 通过访谈、配置检查和工具测试的方式评估信息系统的密码算法、密码技术、密码产品和密码服务的合规性 |
| 4 | 安全技术测评 | 物理和环境安全 | 通过访谈、配置检查和工具测试的方式测评信息系统机房环境的安全情况。主要涉及对象为机房环境的电子门禁系统。本次评测包括电子门禁的身份鉴别和电子门禁记录的完整性保护。 |
| 网络和通信安全 | 通过访谈、配置检查和工具测试的方式测评信息系统的网络和通信安全保障情况。本次重点测评包括通信对象的身份鉴别、访问控制信息完整性、通信数据完整性和通信数据机密性等 |
| 设备和计算安全 | 通过访谈、配置检查和工具测试的方式测评信息系统的主机安全保障情况，本次重点测评包括本地主机和数据库服务器身份鉴别、远程管理身份鉴别身份信息机密性、访问控制信息完整性、敏感标记完整性、日志记录完整性等 |
| 应用和数据安全 | 将通过访谈、配置检查的方式测评信息系统的数据安全保障情况，主要涉及对象为信息系统的管理数据及业务数据等,本次重点测评包括信息系统身份鉴别、访问控制信息完整性、数据传输机密性、数据存储机密性、数据传输完整性、数据存储完整性、日志记录完整性等 |
| 5 | 安全管理测评 | 安全管理 | 安全管理部分为全局性问题，涉及密码安全管理制度、密码安全管理人员、系统实施和系统应急管理等四个方面。 |
| 6 | 分析报告阶段 | 报告编制 | 根据测评编制《信息系统密码应用测评报告》，包括：概述、被测系统描述、测评对象说明、测评指标说明、测评内容和方法说明、单元测评的结果记录及结果汇总、整体测评、测评结果汇总、风险分析、评估结论等内容。 |

**7.3.4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/T 39786-2021）标准，参照《商用密码应用安全性评估管理办法》、《信息安全技术 信息系统密码应用测评要求》（GB/T 43206-2023）、《信息系统密码应用测评过程指南》（GM/T 0116-2021）、《信息系统密码应用高风险判定指引》、《商用密码应用安全性评估量化评估规则》等技术要求，逐一对信息系统进行密码应用的合规性、正确性、有效性进行安全性评估，通过商用密码应用安全性评估深入查找密码应用的薄弱环节和安全隐患，分析面临的风险，为提升信息系统安全奠定基础。

测评的内容包括但不限于以下内容：

1、安全技术测评：包括物理和环境安全、 网络和通信安全、 设备和计算安全、 应用和数据安全等四个方面的安全测评。

（1）物理和环境安全

|  |  |
| --- | --- |
| **测评类别** | **测评单元** |
| 安全技术测评-物理和环境安全 | 身份鉴别 |
| 电子门禁记录数据完整性 |
| 视频记录数据完整性 |

（2）网络和通信安全

|  |  |
| --- | --- |
| **测评类别** | **测评单元** |
| 安全技术测评-网络和通信安全 | 身份鉴别 |
| 通信数据完整性 |
| 通信过程中重要数据的机密性 |
| 网络边界访问控制信息完整性 |
| 安全接入认证 |

（3）设备和计算安全

|  |  |
| --- | --- |
| **测评类别** | **测评单元** |
| 安全技术测评-设备和计算安全 | 身份鉴别 |
| 远程管理通道安全 |
| 系统资源访问控制信息完整性 |
| 重要信息资源安全标记完整性 |
| 日志记录完整性 |
| 重要可执行程序完整性、重要可执行程序来源真实性 |

（4）应用和数据安全

|  |  |
| --- | --- |
| **测评类别** | **测评单元** |
| 安全技术测评-应用和数据安全 | 身份鉴别 |
| 访问控制信息完整性 |
| 重要信息资源安全标记完整性 |
| 重要数据存储机密性 |
| 重要数据传输机密性 |
| 重要数据传输完整性 |
| 重要数据存储完整性 |
| 不可否认性 |

2、安全管理测评：包括安全管理（分为制度、人员、建设和应急四个子模块）的安全测评。

（1）管理制度

|  |  |
| --- | --- |
| **测评类别** | **测评单元** |
| 安全管理测评-管理制度 | 具备密码应用安全管理制度 |
| 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 |

（2）人员管理

|  |  |
| --- | --- |
| **测评类别** | **测评单元** |
| 安全管理测评-人员管理度 | 了解并遵守密码相关法律法规和密码管理制度 |
| 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 |

（3）建设运行

|  |  |
| --- | --- |
| **测评类别** | **测评单元** |
| 安全管理测评-建设运行 | 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 |

（4）应急处置

|  |  |
| --- | --- |
| **测评类别** | **测评单元** |
| 安全管理测评-应急处置 | 应急策略 |
| 事件处置 |
| 向有关主管部门上报处置情况 |

7.4人员及设备要求

7.4.1本项目中人员岗位要求（但不仅限于）详见下表。

**人员配备一览表**

包件：

|  |  |  |  |
| --- | --- | --- | --- |
| **岗位** | **建议配置岗位人数** | **基本要求** | **备注** |
| 项目经理 | 1 | 1.具备《商用密码应用测评人员测评能力考核》证书；  2.具备5年及以上密码应用安全性评估经验，需提供证明材料；  3.具有注册密码安全专业人员证书NSATP-CSP、信息安全高级工程师，需提供有效证书扫描件。 |  |
| 测评人员 | 3 | 1.提供不少于3人商用密码应用安全性评估服务团队（不包含项目经理），需提供加盖供应商公章的人员名单表；  2.具备《商用密码应用测评人员测评能力考核》和密码技术应用员证书；  3.具备3年及以上密码应用安全性评估经验的，需提供证明材料。 |  |
| 档案管理员 | 1 | 具备《商用密码应用测评人员测评能力考核》证书 |  |

注：以上人员应为本单位正式员工，提供在职证明材料，表中相关专业及任职资格请提供相关资格证书。项目服务人员经采购人确认后未经采购人书面批准不得随意更换，遇有应急事项发生，人员可2小时内到场。

7.4.2测评工具要求

本次项目实施过程中所使用到的测评工具，应包括具有自主知识产权或计算机软件著作权的密码检测工具（详细描述所使用工具的型号、功能、使用的方式和对环境和平台的要求以及使用可能对系统造成的风险等），对系统数据进行分析，并以分析结果辅证评估报告。

检测工具包括但不限于以下几类：

1、密码算法验证工具，包括国密算法SM2、SM3、SM4，常见的国际通用算法AES、DES、RSA等的验证；

2、随机数随机性检测工具；

3、数字证书检测工具，包括数字证书的格式的合规性验证、数字证书的证书链的检验等；

4、网络协议分析工具；包括但不限于SSL协议、IPSec 协议；包括主动协议分析工具和被动分析工具。

7.4.3 模拟测评环境要求

服务提供方具有密码测评模拟验证环境的能力及相关设备，包括但不限于以下的密码设备：

1、SSL VPN：支持国密算法；具有商用密码产品认证证书，用于搭建SSL VPN网络，模拟SSL VPN通信信道的测评。

2、IPSec VPN：支持国密算法；具有商用密码产品认证证书，用于搭建IPSec VPN网络，模拟IPSec VPN通信信道的测评。

3、服务器密码机：支持国密算法；具有商用密码产品认证证书，用于实现重要数据的加解密和完整性保护，模拟重要数据加解密和完整性保护的测评。

7.5工作成果

《浦东新区“一网统管”项目密码应用测评报告》

7.6工作进度

合同签订，收到采购人正式通知后30日内完全全部测评工作并出具相关成果报告。

**8安全文明作业要求**

8.1 安全文明作业要求

8.1.1 供应商及其劳务分包商应具备上海市或有关行业管理部门规定的在本市进行相关服务所需的资质（包括国家和本市各类专业工种持证上岗要求）、资格和一切手续（如有的话），由此引起的所有有关事宜及费用由供应商自行负责。

8.1.2 在提供服务期间为确保服务区域及周围环境的整洁和不影响其他活动正常进行，供应商应严格执行国家与上海市有关安全文明施工管理的法律、法规和政策，积极主动加强和落实安全文明施工及环境保护等有关管理工作，并按规定承担相应的费用。若违反规定而造成的一切损失和责任由成交供应商承担。

8.1.3 成交供应商在项目实施期间，必须遵守国家与上海市各项有关安全作业规章、规范与制度，建立动用明火申请批准制度，安全用电等制度，确保杜绝各类事故的发生。

**9管理、考核要求**

9.1 项目管理要求

9.1.1 供应商在磋商阶段应根据本项目具体情况、采购人需求和国家、本市有关规定与标准制定管理方案，在成交后据此进行细化，经采购人确认后按照确认的管理方案和管理计划组织管理，接受采购人代表对管理质量的检查、监督和考核。未经采购人事前书面许可，成交供应商不得自行调整管理方案或更改管理措施。

9.1.2 根据实际需要或其他原因，采购人认为确有必要调整管理方案并以书面形式要求成交供应商管理人员调整管理时间或更改管理措施时，成交供应商应遵从采购人要求，但如该项调整导致的费用增加，成交供应商需提出增加费用预算和依据，经由采购人确认后由采购人承担。

9.1.3 成交供应商在响应文件中承诺并经采购人认定的项目负责人及专业技术、管理人员应是本单位职工，且为该项目现场的实际操作者，并应常驻项目现场。未经采购人同意，成交供应商不得调换或撤离上述人员，如采购人认为有必要，可要求成交供应商对上述人员中的部分人员作出更好的调整。

9.1.4 成交供应商需建立职工（含劳务工等各种类型用工）花名册等档案资料，与职工签订劳动合同，为其办理国家规定的相关保险，并按规定标准安排专业健康体检和配备劳动防护用品。

9.1.5 本项目所用材料、制品、设备等均需符合相关技术规程、规范要求。

9.1.6 本项目所用的材料、制品、设备等，供货单位送达施工现场后，由成交供应商负责办理验收交割手续，并负责日常保管工作。

**10保密要求**

10.1 成交供应商应遵守合同文件约定内容的保密要求。如果采购人提供的内容属于保密的，应签订保密协议，且双方均有保密义务。成交供应商不得利用工作之便外泄资料或做其他用途，否则成交供应商需承担由此引起的法律责任和赔偿采购人的经济损失。本款规定的效力及于成交供应商及成交供应商的所有雇用人员。

四、报价须知

**11磋商报价依据**

11.1 磋商报价计算依据包括本项目的磋商文件（包括提供的附件）、磋商文件答疑或修改的补充文书、磋商过程中实质性变动的内容、服务内容一览表、项目现场条件等。

11.2磋商文件明确的项目范围、实施内容、实施期限、质量要求、售后服务（如果有）、管理要求与标准及考核要求等。

11.3服务内容一览表说明

11.3.1服务内容一览表应与供应商须知、合同条件、项目质量标准和要求等文件结合起来理解或解释。

11.3.2采购人提供的服务内容一览表是依照采购需求测算出的主要工作内容，允许供应商对服务内容一览表内非核心工作内容进行优化设计，并依照优化后的方案进行报价。各供应商应认真了解采购需求，如发现核心工作内容和实际采购需求不一致时，应立即以书面形式通知采购人核查，除非采购人以答疑文件、补充文件或磋商过程中实质性内容对磋商文件予以更正，否则，应以服务内容一览表为准。

**1****2磋商报价内容**

12.1 本项目报价为全费用报价，是履行合同的最终价格，除采购需求中另有说明外，磋商报价（即磋商总价）应包括项目启动阶段、实施阶段、试运行阶段、验收阶段等这一系列过程中所包含的所有费用。

12.2 磋商报价中供应商应考虑本项目可能存在的风险因素。磋商报价应将所有工作内容考虑在内，如有漏项或缺项，均属于供应商的风险，其费用视作已分配在磋商报价明细表内单价或总价之中。供应商应逐项计算并填写单价、合计价和总价。

12.3在项目实施期内，对于除不可抗力因素之外，人工价格上涨以及可能存在的其它任何风险因素，供应商应自行考虑，在合同履约期内中标价不作调整。

12.4 供应商按照响应文件格式中所附的表式完整地填写《磋商报价一览表》及各类磋商报价明细表，说明其拟提供服务的内容、数量、价格、时间、价格构成等。

**13磋商报价控制性条款**

13.1 磋商最后报价不得超过公布的预算金额或最高限价，其中各年度或各分项报价（如有要求）均不得超过对应的预算金额或最高限价。

13.2 本项目只允许有一个报价，任何有选择的报价将不予接受。

13.3 供应商提供的服务应当符合国家和上海市有关法律、法规和标准规范，满足合同约定的服务内容和质量等要求。不得违反法规标准规定或合同约定，不得通过降低服务质量、减少服务内容等手段进行恶性低价竞争，扰乱正常市场秩序。

**★**13.4 经磋商小组审定，磋商报价存在下列情形之一的，该响应文件作无效处理：

13.4.1 磋商最后报价和技术方案明显不相符的；

13.4.2 磋商最后报价中缩减磋商小组最终确定的服务内容的。

五、政府采购政策

**14促进中小企业发展**

14.1中小企业（含中型、小型、微型企业，下同）的划定按照《中小企业划型标准规定》（工信部联企业【2011】300号）执行，参加磋商的中小企业应当提供《中小企业声明函》（具体格式见“响应文件格式”），反之，视作非中、小微企业，不具备参与磋商资格。如项目允许联合体参与竞争的，则联合体中各方均应为中小企业，并按本款要求提供《中小企业声明函》。

14.2 事业单位、团体组织等非企业性质的政府采购供应商，不属于中小企业划型标准确定的中小企业，不得按《关于印发中小企业划型标准规定的通知》规定声明为中小微企业，也不适用《政府采购促进中小企业发展管理办法》。

14.3 如项目允许联合体参与竞争的，组成联合体的中型企业和其他自然人、法人或者其他组织，与小型、微型企业之间不得存在投资关系。

14.4供应商如提供虚假材料以谋取成交的，按照《政府采购法》有关条款处理，并记入供应商诚信档案。

**15促进残疾人就业**

15.1 符合财库【2017】141号文中所示条件的残疾人福利性单位视同小型、微型企业，享受促进中小企业发展的政府采购政策。残疾人福利性单位属于小型、微型企业的，不重复享受政策。

15.2 残疾人福利性单位在参加政府采购活动时，应当按财库【2017】141号规定的《残疾人福利性单位声明函》（具体格式详见“响应文件格式”），并对声明的真实性负责。