**湖北省卫生健康委员会信息化常规项目--商用密码应用安全性评估服务采购需求**

# 第一部分：供应商资格要求

1、投标人须符合《政府采购法》第二十二条的规定

2、未被列入“信用中国”或“中国政府采购网”中的失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单；

3、投标人须具备商用密码应用安全性评估的能力（投标人需在国家密码管理局公告（第42号）发布的《商用密码应用安全性评估试点机构目录》中，或在省级密码管理局发布的《商用密码应用安全性评估试点工作机构名单》中）。

4、本项目不接受联合体投标。

**第二部分：采购内容**

# 采购内容：

|  |  |  |
| --- | --- | --- |
| 序号 | 服务名称 | 服务内容 |
| 1 | 密码应用方案设计咨询 | 协助采购人分析密码应用中的技术难点，为采购人设计商用密码应用方案提供技术咨询服务 |
| 2 | 密码应用方案评审 | 协助采购人对密码应用方案进行审核，审核通过后，出具密码应用方案的评估报告，协助采购人组织相关专家进行方案评审 |
| 3 | 密码建设咨询 | 密码方案通过专家评审后，为采购人单位进行商用密码建设提供技术咨询，协助分析实施过程中遇到的问题并提供参考建议 |
| 4 | 商用密码应用安全性评估 | 在密码体系建设完成后，通过技术手段抓包并验证密码算法和密码产品的正确性、有效性、合规性分析，并出具评估报告 |
| 5 | 密码安全保障服务 | 提供1年密码安全保障服务，利用攻防演练实验室平台提供密码攻防演练、漏洞检测、应急响应及安全咨询等服务 |

二、**采购预算**：40万元。

三、**交付时间、地点、对象及标准**

3.1交付时间：合同签订生效、具备进场条件后160个工作日内完成

3.2交付地点：采购人指定地点。

3.3测评对象及标准：测评对象参见《密评服务清单》，按照第三级技术标准开展商用密码应用安全性评估。

四、采购内容及要求

# 4.1密评服务内容

为了保障湖北省卫生健康委员会所有信息系统和子系统的商用密码应用安全性，要以年度服务形式对湖北省卫生健康委员会已建成和在建的所有信息系统及子系统开展商用密码应用安全性评估工作，进行密码应用方案评估和系统的商用密码评估。具体工作包括以下方面：

（1）密码应用方案评估:对现有的密码应用方案进行评估，包括密码算法的选择、密钥管理、访问控制等方面。通过评估，确定现有方案的安全性是否符合要求，并提出改进建议。

（2）系统的商用密码评估:对已建成和在建的所有信息系统及子系统的商用密码进行评估，包括加密算法、认证机制、安全协议等方面。通过评估，确定系统的商用密码是否符合国家法规和标准的要求，并提出改进建议。

（3）提供报告和建议:根据评估结果，提供详细的报告和建议，包括密码应用方案的改进建议和商用密码的合规性评估结果。同时，为用户提供专业的技术支持和服务。提升信息系统和子系统的商用密码应用安全性，确保信息安全得到有效的保护。

# 4.2、项目概况

## 4.2.1 项目背景

密码乃国之重器，是保护国家利益的战略性资源，是网络安全的核心技术和基础支撑；国产密码应用是我省卫生健康领域网络与信息系统的重要内容，是关系到信息安全、数据安全、国家安全的重要任务。国家卫生健康委《十四五全民健康信息化规划》明确提出“全面推广商用密码应用，完善卫生健康行业商用密码应用体系”。

为贯彻落实《中华人民共和国密码法》、《医疗卫生机构网络安全管理办法》、《关于进一步加强全省政务信息化项目密码应用有关工作的通知》（鄂密局发[2021]2号）、《商用密码管理条例》等法律法规、政策文件要求，进一步提高网络安全工作的管理水平和技术防护能力，省卫生健康委员会依托健康医疗大数据中心暨公共卫生应急管理平台建设项目,强化国产密码应用建设改造，建立密码应用服务平台，部署了数据库加密机，对卫生健康领域网络与信息系统进行保护。现计划从总体要求、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，对卫生健康领域网络与信息系统进行密码应用安全性评估，以实现卫生健康领域商用密码的合规、正确、有效使用。

## 4.2.2项目目标

### **4.2.2.1总体目标**

该项目以湖北省卫生健康委员会信息系统的实际情况和现实问题为基础，遵照国家的法律法规和标准规范，依据相应等级信息系统的基本要求和安全目标，设计并建设符合行业特点、融管理和技术为一体的整体安全保障体系。

依据湖北省卫生健康委员会信息系统所包括的信息资产的安全性、信息系统主要处理的业务信息类别、信息系统服务范围以及业务对信息系统的依赖性等指标，进行全面的测试、分析。找出信息系统中的风险和问题并提出相应的应对措施。

### **4.2.2.2信息安全体系目标**

按照商用密码应用安全性评估相关技术标准，科学合理的检测和评估湖北省卫生健康委员会信息系统风险、协助发现风险和问题。通过建设整改，实现对信息资产的保密、完整、可用、不可抵赖和可审计性，基本做到“进不来、拿不走、改不了，看不懂、跑不了、可审计、打不垮”。

## 4.2.3 标准和依据

1、本次商用密码应用安全性评估依据如下法律法规、政策文件执行：

* 《中华人民共和国网络安全法》
* 《中华人民共和国密码法》
* 《商用密码管理条例》
* 《国家政务信息化项目建设管理办法》（国办发[2019]57号）
* 《国家密码管理局关于进一步加强国家政务信息系统密码应用与安全性评估工作的函》（国密局函 [2020]119号）
* 《关于进一步加强全省政务信息化项目密码应用有关工作的通知》（鄂密局发[2021]2号）

2、本次商用密码应用安全性评估参照以下技术标准（项目执行期间，如国家技术标准调整，按新生效的标准执行）：

* 《计算机信息系统安全保护等级划分准则》(GB17859-1999)
* 《信息安全技术信息系统通用安全技术要求》(GB/T20271-2006)
* 《信息安全技术 网络基础安全技术要求》(GB/T20270-2006)
* 《信息安全技术 操作系统安全技术要求》(GB/T20272-2006)
* 《信息安全技术 数据库管理系统安全技术要求》(GB/T20273-2006)
* 《信息安全技术信息系统安全管理要求》(GB/T20269-2006)
* 《信息安全技术信息安全风险评估规范》（GB/T 20984-2007）
* 《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）
* 《信息系统密码应用基本要求》（GM/T 0054-2018）
* 《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）
* 政务信息系统密码应用与安全性评估工作指南（2020版）

## 4.2.4 测评实施原则

在项目实施过程中必须满足以下原则：

**1）保密原则**：对测评的过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据进行任何侵害招标方的行为。

**2）标准性原则**：测评方案的设计与实施应依据国家信息系统安全的相关标准进行。

**3）规范性原则**：投标人的工作中的过程和文档，具有很好的规范性，可以便于项目的跟踪和控制。

**4）可控性原则**：项目安排工作进度要跟上进度表的安排，保证工作的可控性。

**5）最小影响原则**：测评工作应尽可能小的影响系统和网络，并在可控范围内；测评工作不能对现有信息系统的正常运行、业务的正常开展产生任何影响。

**6）整体性原则**：测评的范围和内容应当整体全面，包括国家相关要求涉及的各个层面。

# 4.3、商用密码应用安全性评估技术要求

依据《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）、政务信息系统密码应用与安全性评估工作指南（2020 版）等相关技术标准要求，参照ISO20000或CNAS检验等信息技术服务体系，对被测信息系统开展商用密码应用安全性评估（项目执行期间，如国家技术标准发生变化，按照新生效的技术标准执行），为采购方开展密码应用方案设计提供技术咨询，评估内容如下：

|  |  |
| --- | --- |
| 序号 | 商用密码应用安全性评估 |
| 1 | 密码应用方案评估 | 密码应用解决方案评估 | 应对密码应用解决方案的完整性和密码应用设计的合规性、正确性和有效性进行评估。 |
| 2 | 实施方案评估 | 应检查文档结构是否完整，并审查实施方案是否按照《密码应用解决方案》的设计要求进行编制。 |
| 3 | 应急方案评估 | 应检查文档结构是否完整，并审查应急方案提出的风险应急预案是否完备、合理、周密。 |
| 4 | 总体要求 | 密码算法 | 应验证被测信息系统中使用的密码算法是否符合法律、法规的规定和密码相关国家标准、行业标准的有关要求。 |
| 5 | 密码技术 | 应验证被测信息系统中使用的密码技术是否遵循密码相关国家标准和行业标准。 |
| 6 | 密码产品 | 应验证被测信息系统中使用的密码产品与密码模块是否通过国家密码管理部门核准。 |
| 7 | 密码服务 | 应验证被测信息系统中使用的密码服务是否通过国家密码管理部门许可。 |
| 8 | 物理和环境安全 | 身份鉴别 | 应验证被测信息系统在电子门禁系统中是否使用密码技术的真实性服务来保护身份鉴别信息，保证重要区域进入人员身份的真实性。 |
| 9 | 电子门禁记录数据完整性 | 应验证被测信息系统是否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。 |
| 10 | 视频记录数据完整性 | 应验证被测信息系统是否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。 |
| 11 | 网络和通信安全 | 身份鉴别 | 应验证被测信息系统是否在通信前基于密码技术对通信双方进行验证或认证，使用密码技术的机密性和真实性服务来实现防截获、防假冒和防重用，保证传输过程中鉴别信息的机密性和网络设备实体身份的真实性。 |
| 12 | 访问控制信息完整性 | 应验证被测信息系统是否使用密码技术的完整性服务来保证网络边界和系统资源访问控制信息的完整性。 |
| 13 | 通信数据完整性 | 应验证被测信息系统是否采用密码技术保证通信过程中数据的完整性。 |
| 14 | 通信数据机密性 | 应验证被测信息系统是否采用密码技术保证通信过程中敏感信息数据字段或整个报文的机密性。 |
| 15 | 集中管理通道安全 | 应验证被测信息系统是否采用密码技术建立一条安全的信息传输通道，对网络中的安全设备或安全组件进行集中管理。 |
| 16 | 安全接入认证 | 应验证被测信息系统是否采用密码技术对外部连接到内部网络的设备进行接入认证，确保接入的设备身份真实性。 |
| 17 | 设备和计算安全 | 身份鉴别 | 应验证被测信息系统是否使用密码技术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。 |
| 18 | 远程管理通道安全 | 应验证被测信息系统是否远程管理时，应使用密码技术建立安全的信息传输通道 |
| 19 | 系统资源访问控制信息完整性 | 应验证被测信息系统是否使用密码技术的完整性服务来保证系统资源访问控制信息的完整性。 |
| 20 | 重要信息资源安全标记完整性 | 应验证被测信息系统设备是否使用密码技术的完整性服务来保证设备中重要信息资源安全标记的完整性。 |
| 21 | 重要可执行程序完整性、重要可执行程序来源真实性 | 应验证被测信息系统是否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。 |
| 22 | 日志记录完整性 | 应验证被测信息系统是否使用密码技术的完整性功能来对日志记录进行完整性保护。 |
| 23 | 应用和数据安全 | 身份鉴别 | 应验证被测信息系统是否使用密码技术对登录的用户进行身份标识和鉴别，实现身份鉴别信息的防截获、防假冒和防重用，保证应用系统用户身份的真实性。 |
| 24 | 访问控制信息和敏感标记完整性 | 应验证被测信息系统是否使用密码技术的完整性服务来保证业务应用系统访问控制策略、数据库表访问控制信息和重要信息资源敏感标记等信息的完整性。 |
| 25 | 数据传输机密性 | 应验证被测信息系统是否采用密码技术保证重要数据在传输过程中的机密性，包括但不限于鉴别数据、重要业务数据和重要用户信息等。 |
| 26 | 数据存储机密性 | 应验证被测信息系统是否采用密码技术保证重要数据在存储过程中的机密性，包括但不限于鉴别数据、重要业务数据和重要用户信息等。 |
| 27 | 数据传输完整性 | 应验证被测信息系统是否采用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用户信息等。 |
| 28 | 数据存储完整性 | 应验证被测信息系统是否采用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用户信息、重要可执行程序等。 |
| 29 | 重要信息资源安全标记完整性 | 应验证被测信息系统是否使用密码技术的完整性服务来保证重要信息资源敏感标记的完整性。 |
| 30 | 不可否认性 | 在可能涉及法律责任认定的应用中，应验证被测信息系统是否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。 |
| 31 | 管理制度 | 具备密码应用安全管理制度 | 应验证责任单位是否具备密码应用安全管理制度,包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度; |
| 32 | 密钥管理规则 | 应验证责任单位是否根据密码应用方案建立相应密钥管理规则; |
| 33 | 建立操作流程 | 应验证责任单位是否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 |
| 34 | 定期修订安全管理制度 | 应验证责任单位系统负责人是否定期对密码应用安全管理制度和操作规程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之处进行修订; |
| 35 | 明确管理制度发布流程 | 应验证责任单位系统负责人是否明确相关密码应用安全管理制度和操作规程的发布流程并进行版本控制; |
| 36 | 制度执行过程记录留存 | 应验证责任单位是否具有密码应用操作规程的相关执行记录并妥善保存。 |
| 37 | 人员管理 | 了解并遵守密码相关法律法规和密码管理制度 | 应验证责任单位相关人员是否了解并遵守密码相关法律法规、密码应用安全管理制度; |
| 38 | 建立密码应用岗位责任制度 | 应验证责任单位是否建立密码应用岗位责任制度，明确各岗位在安全系统中的职责和权限: |
| 39 | 建立上岗人员培训制度 | 应验证责任单位是否建立关键岗位人员保密制度和调离制度，签订保密合同，承担保密义务。 |
| 40 | 定期进行安全岗位人员考核 | 应验证责任单位是否定期对密码应用安全岗位人员进行考核; |
| 41 | 建立关键岗位人员保密制度和调离制度 | 应验证责任单位是否建立关键人员保密制度和调离制度.签订保密合同,承担保密义务。 |
| 42 | 建设运行 | 制定密码应用方案 | 应验证责任单位是否依据密码相关标准和密码应用需求,制定密码应用方案; |
| 43 | 制定密钥安全管理策略 | 应验证责任单位是否根据密码应用方案.确定系统涉及的密钥种类、体系及其生存周期环节； |
| 44 | 制定实施方案 | 应验证建设单位是否按照应用方案实施建设; |
| 45 | 投入运行前进行密码应用安全性评估 | 应验证被测系统投人运行前是否进行密码应用安全性评估; |
| 46 | 定期开展密码应用安全性评估及攻防对抗演习 | 应验证被测系统运行过程中,是否严格执行既定的密码应用安全管理制度,是否定期开展密码应用安全性评估及攻防对抗演习,并根据评估结果进行整改。 |
| 47 | 应急处置 | 应急策略 | 应验证责任单位是否制定密码应用应急策略,做好应急资源准备,当密码应用安全事件发生时,是否立即启动应急处置揩施.结合实际情况及时处置; |
| 48 | 事件处置 | 应验证责任单位在密码应用安全事件发生后,是否及时向信息系统主管部门及归属的密码管理部门进行报告; |
| 50 | 向有关主管部门上报处置情况 | 应验证责任单位在密码应用安全事件处置完成后,是否及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况。 |

**4.3.1密码安全保障工作内容**

投标人应提供一年网络安全综合保障服务，对采购人相关应用信息系统实施密码攻防演练、漏洞检测、应急响应及安全咨询等技术服务，并出具相关技术服务报告。投标人应具有攻防演练实验室平台，可提供高效、精准的信息安全风险检测结果，协助采购人开展密码应用安全整改加固工作；快速响应采购人密码应用安全应对需求，及时、有效地应对各种黑客攻击；协助采购人处置各类网络安全事件。服务包括但不限于以下内容：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 服务内容 | 工作描述 | 服务方式 |
| 1 | 密码攻防演练 | 组织安全服务团队，利用攻防演练实验室平台对发现事件、分析研判、应急处置、事件上报和风险防范等多个阶段提供攻防演练，检验系统密码应用安全能力和服务人员应急处置能力，增强密码服务人员的应急处置意识，提升了密码安全防范能力。 | 每年一次 |
| 2 | 漏洞检测 | 对信息系统进行安全扫描服务，通过对信息系统及其部署的服务器、关联的网络设备进行漏洞扫描，辅助以人工分析的方式，最大程度的发现客户重要应用系统的安全漏洞。（具体测试信息系统以实际情况为准） | 每季度提供一份漏洞检测报告 |
| 3 | 应急响应服务 | 协助采购人根据安全事件等级制定应急预案及管理制度，明确了应急事件处理流程及其他管理措施。提供安全应急响应服务，用最快的速度响应非法攻击，启动应急响应预案，处理相关安全事件，将事件影响降低到最低。应急响应服务应至少包括现场取证备查、分析查明被攻击原因以及提供可行的修复建议从而以保证重要系统能及时恢复上线。提供现场应急支持，并将应急响应的全过程结果以文档形式输出交付我校。协助处理安全事件，如挂马、被黑、后门等，协助处理漏洞通报处理并反馈结果。 | 7×24小时 |
| 4 | 密码安全培训 | 提供密码安全培训，提高密码应用安全意识及技能。其中要求一次现场不少于80人的集中培训，时间：1-2天；地点：武汉；场地、师资、教材、学员食宿由中标人负责。 | 视采购人方要求 |

# 4.4、服务要求

## 4.4.1 实施要求

本次项目测评实施及安全服务必须满足以下要求：

1）最小影响要求：投标人在测评实施过程中必须保证系统的正常运行，不得导致系统运行中断或服务性能明显下降，尽可能降低对系统的负面影响。在进行有风险的操作前必须出具书面材料，明确风险提示，指导采购人做好应急措施，征得采购人书面许可后并选择业务低峰期进行下一步操作。

2）保密要求：对测评或技术服务过程中获取的信息严格保密，包括但不限于采购人网络拓扑结构、IP地址、业务流程、业务数据、安全隐患等，未经授权不得泄露给任何单位和个人，不得利用保密信息进行任何侵害采购人的合法权益。

3）客观公正性要求：项目实施过程中，必须接受采购人的监督，每个测评环节完成后均由采购人进行审核确认，确保测评工作客观公正性。

4）规范性要求：测评实施等必须严格按照国家商用密码应用安全性评估相关标准进行。投标人须有严格质量控制体系,具备ISO20000或CNAS检验机构认可资质，并参照ISO20000信息技术服务管理体系或CNAS检验检测体系流程规范实施过程。

5）可控性要求：项目实施必须制定严格的实施计划及进度安排，经采购人审核确认后执行，确保项目实施的可控性。

## 4.4.2 人员要求

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。参与项目的测评人员不少于5人，需具备专业的测评能力和经验，参与商用密码应用安全性评估的人员需具备商用密码应用安全性评估人员测评能力考核资质证书。其中技术负责人须具备CISP、高级信息系统项目管理师、网络规划设计师之一的高级资质证书，且具备充足的技术实施能力和项目管理能力。

## 4.4.3 保密要求

1) 投标人必须和采购人签订保密协议，投标人必须要与参加此次项目的所有项目组成员签订保密协议，在合同签订时一并提供给采购人。

2) 投标人具体实施项目中的重要资料和结果，在项目实施期间和实施结束后，投标人不得带离该地点。

3) 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。

4) 投标人应保守在测评活动中知悉的国家秘密、商业秘密和个人隐私，防范测评风险。

5) 投标人应对测评人员进行安全保密教育，与其签订安全保密责任书，规定应当履行的安全保密义务和承担的法律责任，并负责检查落实。

## 4.4.4 质量要求

项目管理是贯穿整个项目的一项任务。通过实施有效的项目管理，保证本项目能够按工作范围要求、按时间、按质量完成。投标人应提供质量控制及保证措施方案，包含项目质量控制及保证措施等。

## 4.4.5 风险规避要求

项目开展工作涉及到单位重要信息系统和数据，在测评过程中必须加强安全风险控制。

测评工作的开展可能会给被测系统带来一定风险,测评机构应在测评开始前及测评过程中及时进行风险识别及分析，对可能发生的风险采取有效措施，以规避风险或降低风险产生带来的影响。可能面临的风险如下:

a)验证测试影响系统正常运行

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，可能对系统的运行造成不可预期的影响.

b)工具测试影响系统正常运行

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，可能对信息系统中的服务器和网络通讯造成一定影响甚至伤害.

c)敏感信息泄漏

泄漏被测系统信息，如加密机制、业务流程、安全隐患和有关文档信息.

d)其他可能面临的风险

其他可能在测评过程中影响信息系统可用性、机密性和完整性的风险.

## 4.4.6 商务要求

### 4.4.6.1投标要求

1)投标人应仔细阅读采购需求文件的所有内容，按要求编制投标文件，并对采购需求文件做出实质性响应，并保证所提供全部资料的真实性。

2)投标人应承担本项目的相关保密义务。未经采购人书面同意，不得将本项目相关信息透露给任何第三方。

3)投标人不得以任何方式转包或分包本项目。

### 4.4.6.2报价要求

投标总报价须为人民币报价，且应是交钥匙工程（包含：相关手续费、软件使用及版权费用、人工费、通讯费、运输费、培训费、交通费、调研费、文献查阅、资料装订印刷费等完成本项目的所有相关费用）。因投标人自身原因造成漏报、少报的，或在合同实施过程中可能发生的其它费用（如：工期延迟、材料涨价、人工及交通成本增加等因素），应由其自行承担责任，采购人不再补偿。

### 4.4.6.3知识产权

1)投标人必须保证采购人在接受其所提供服务期的任何时候不受到知识产权或版权的纠纷，否则由此产生的任何责任完全由投标人承担。

2)采购人拥有针对本项目形成的所有文档全部知识产权。未经采购人许可，投标人不得擅自使用全部或部分内容。

### 4.4.6.4合同签订

投标人中标后，持相关证明与采购人签订合同。本项目招标文件、投标人投标文件均作为合同签订的基础。

### 4.4.6.5验收要求

1)投标人和采购人双方依据项目内容和进度共同实施验收工作，验收结果和验收报告经双方确认后生效。

2)投标人必须提交正式的《商用密码应用安全性评估报告》。该项目过程中产生的文档，归采购人所有。

### 4.4.6.6测评服务成果物

项目交付清单：中标方在项目验收前须分别提交被测应用系统的商用密码应用安全性评估成果文档：

（1）《密码应用方案评估报告》

（2）《系统商用密码应用安全性评估报告》

（3）《密评结果备案材料接收回执》

### 4.4.6.7付款方式

### 按合同约定执行。

### 4.4.6.8售后服务要求

1)投标人承诺提供1年服务，服务方式包括电话技术支持、远程技术支持、现场技术支持等。

2)投标人应提供本地化服务，具有专业化服务团队。（提供常驻售后服务机构或合作企业资料复印件、营业场所租赁或购买合同复印件、人员社保证明资料等其他证明材料）。