

# 竞争性磋商文件

项目名称：国家移民管理局互联网门户网站和政务服务  
平台等保及商用密码应用评估项目

项目编号：BJYM25FW021

采 购 人：国家移民管理局

采购代理机构：永明项目管理有限公司

2025 年 7 月

# 目 录

|     |                 |    |
|-----|-----------------|----|
| 第一章 | 采购邀请 .....      | 1  |
| 第二章 | 供应商须知 .....     | 4  |
| 第三章 | 评审方法和评审标准 ..... | 22 |
| 第四章 | 采购需求 .....      | 34 |
| 第五章 | 合同草案条款 .....    | 72 |
| 第六章 | 响应文件格式 .....    | 84 |

# 第一章 采购邀请

## 一、项目基本情况

1. 项目编号：BJYM25FW021
2. 项目名称：国家移民管理局互联网门户网站和政务服务平台等保及商用密码应用评估项目
3. 采购方式：竞争性磋商
4. 项目预算金额：40 万元；最高限价金额：32 万元。
5. 采购需求：依据国家网络安全等级保护相关标准规范的要求，完成国家移民管理局互联网门户网站和政务服务平台等 2 个三级系统网络安全等级保护测评和商用密码应用安全评估。（详见第四章采购需求）
6. 合同履行期限：合同签订后 180 日内。
7. 本项目是否接受联合体：☐是 ☒否。

## 二、申请人的资格要求（须同时满足）

1. 满足《中华人民共和国政府采购法》第二十二条规定；
2. 落实政府采购政策需满足的资格要求：
  - 2.1 中小企业政策  
☒ 本项目不专门面向中小企业预留采购份额  
☐ 本项目专门面向 ☐ 中小企业 ☐ 小微企业 采购。即：提供的货物全部由符合政策要求的中小/小微企业制造、服务全部由符合政策要求的中小/小微企业承接。  
☐ 本项目预留部分采购项目预算专门面向中小企业采购。对于预留份额，提供的货物由符合政策要求的中小企业制造、服务由符合政策要求的中小企业承接。预留份额通过以下措施进行：\_\_\_\_\_ / \_\_\_\_\_。
  - 2.2 其它落实政府采购政策的资格要求（如有）：\_\_\_\_\_ / \_\_\_\_\_。
3. 本项目的特定资格要求：
  - 3.1 本项目是否属于政府购买服务：  
☒ 否

□是，公益一类事业单位、使用事业编制且由财政拨款保障的群团组织，不得作为承接主体；

3.2 其他特定资格要求：（1）供应商须为国家密码管理局发布的《商用密码检测机构（商用密码应用安全性评估业务）目录》中的机构，且具有商用密码检测机构资质证书；（2）供应商应具有公安部第三研究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。

### 三、获取磋商文件

1. 时间：2025 年 07 月 28 日至 2025 年 08 月 04 日，每天上午 9:30 至 12:00，下午 13:30 至 16:30（北京时间，法定节假日除外）。

2. 地点：北京市丰台区广安路 9 号院国投财富广场 5 号楼 12A15 室。

3. 方式：现场或线上购买磋商文件，现场购买须使用现金，售后不退。

3.1 现场领取竞争性磋商文件时供应商代表须携带以下资料（**所有复印件均需加盖供应商公章**）：

A. 授权代表办理的：

- 1) 法定代表人授权委托书原件；
- 2) 法定代表人有效身份证复印件；
- 3) 授权代表本人有效身份证原件及复印件。

B. 法定代表人办理的：

- 1) 法定代表人身份证明原件；
- 2) 法定代表人有效身份证复印件及原件。

3.2 须将填写完整的磋商文件领取登记表、标书款汇款底单、法定代表人委托授权书及法定代表人、被委托人的身份证复印件加盖公章扫描发送至 [bjymxmgl@163.com](mailto:bjymxmgl@163.com) 并电话确认。

3.3 标书款账号信息（**请务必备注项目编号和用途**）

开户名（全称）：永明项目管理有限公司北京第一分公司

开户银行：招商银行北京丽泽商务区支行

账 号：110948262310701

4. 售价：200 元（售后不退）

#### **四、响应文件提交**

截止时间：2025 年 08 月 08 日 9 点 30 分（北京时间）。

地点：北京市丰台区广安路 9 号院国投财富广场 5 号楼 12A12 室。

#### **五、开启**

时间：2025 年 08 月 08 日 9 点 30 分（北京时间）。

地点：北京市丰台区广安路 9 号院国投财富广场 5 号楼 12A12 室。

#### **六、公告期限**

自本公告发布之日起 3 个工作日。

#### **七、其他补充事宜**

1. 本项目需要落实的政府采购政策：

- 1) 支持政府采购促进中小企业发展；
- 2) 支持政府采购支持监狱企业发展；
- 3) 支持政府采购促进残疾人就业；
- 4) 支持政府采购信用担保。

#### **八、对本项目提出询问，请按以下方式联系。**

##### **1. 采购人信息**

名 称：国家移民管理局

地 址：北京市东城区长安街 6 号

联系方式：蔺警官，010-66265830

##### **2. 采购代理机构信息**

名 称：永明项目管理有限公司

地 址：北京市丰台区广安路 9 号院国投财富广场 5 号楼 12A15 室

联系方式：于淼、王文革、秦铁仓、010-63268382-8004

##### **3. 项目联系方式**

项目联系人：于淼、王文革、秦铁仓

电 话：010-63268382-8004

## 第二章 供应商须知

### 供应商须知资料表

本表是对供应商须知的具体补充和修改，如有矛盾，均以本资料表为准。标记“■”的选项意为适用于本项目，标记“□”的选项意为不适用于本项目。

| 条款号                                | 条目           | 内容                                                                                                                                                                                                                                     |      |              |                                    |            |
|------------------------------------|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|--------------|------------------------------------|------------|
| 2.2                                | 项目属性         | 项目属性：<br><input checked="" type="checkbox"/> 服务<br><input type="checkbox"/> 货物<br><input type="checkbox"/> 工程                                                                                                                          |      |              |                                    |            |
| 2.3                                | 科研仪器设备       | 是否属于科研仪器设备采购项目：<br><input type="checkbox"/> 是<br><input checked="" type="checkbox"/> 否                                                                                                                                                 |      |              |                                    |            |
| 3.1                                | 现场考察         | <input checked="" type="checkbox"/> 不组织<br><input type="checkbox"/> 组织，考察时间：____年____月____日____点____分<br>考察地点：_____。                                                                                                                   |      |              |                                    |            |
|                                    | 磋商前答疑会       | <input checked="" type="checkbox"/> 不召开<br><input type="checkbox"/> 召开，召开时间：____年____月____日____点____分<br>召开地点：_____。                                                                                                                   |      |              |                                    |            |
| 4.2.5                              | 标的所属行业       | 本项目采购标的对应的中小企业划分标准所属行业： <table border="1" style="width: 100%;"> <tr> <td style="width: 60%;">标的名称</td><td style="width: 40%;">中小企业划分标准所属行业</td></tr> <tr> <td>国家移民管理局互联网门户网站和政务服务平台等保及商用密码应用评估项目</td><td>软件和信息技术服务业</td></tr> </table> | 标的名称 | 中小企业划分标准所属行业 | 国家移民管理局互联网门户网站和政务服务平台等保及商用密码应用评估项目 | 软件和信息技术服务业 |
| 标的名称                               | 中小企业划分标准所属行业 |                                                                                                                                                                                                                                        |      |              |                                    |            |
| 国家移民管理局互联网门户网站和政务服务平台等保及商用密码应用评估项目 | 软件和信息技术服务业   |                                                                                                                                                                                                                                        |      |              |                                    |            |
| 10.2                               | 报价           | 报价的特殊规定：<br><input checked="" type="checkbox"/> 无                                                                                                                                                                                      |      |              |                                    |            |

| 条款号    | 条目       | 内容                                                                                                                                                                                |
|--------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        |          | <input type="checkbox"/> 有，具体情形：_____。                                                                                                                                            |
| 11.1   | 磋商保证金    | <b>磋商保证金金额：___/___万元</b><br>磋商保证金收受人信息：<br>开户名（全称）：永明项目管理有限公司北京第一分公司<br>开户银行：招商银行北京丽泽商务区支行<br>账    号：110948262310701<br>请注明“项目编号+项目名称简称”                                          |
| 11.7.5 |          | 磋商保证金不予退还的其他情形：<br><input checked="" type="checkbox"/> 无<br><input type="checkbox"/> 有，具体情形：___/___。                                                                              |
| 12.1   | 响应有效期    | 自提交响应文件的截止之日起算 90 日历天。                                                                                                                                                            |
| 20.1   | 成交供应商的确认 | 采购人是否授权磋商小组直接确定成交供应商：<br><input checked="" type="checkbox"/> 否<br><input type="checkbox"/> 是<br>成交候选人并列的，按照以下方式确定成交供应商： <u>评审得分相同的，按照最后报价由低到高的顺序推荐。评审得分且最后报价相同的，按照技术指标优劣顺序推荐。</u> |
| 23.5   | 分包       | 本项目是否允许分包：<br><input checked="" type="checkbox"/> 不允许<br><input type="checkbox"/> 允许，具体要求：_____。<br>（1）可以分包履行的具体内容：_____；<br>（2）允许分包的金额或者比例：_____；<br>（3）其他要求：_____。              |
| 24.1.1 | 询问       | 询问送达形式：现场，书面形式送达。                                                                                                                                                                 |
| 24.3   | 联系方式     | 接收询问和质疑的联系方式                                                                                                                                                                      |

| 条款号 | 条 目           | 内 容                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |        |               |    |  |     |     |   |       |        |        |   |           |        |        |
|-----|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|---------------|----|--|-----|-----|---|-------|--------|--------|---|-----------|--------|--------|
|     |               | 联系部门：永明项目管理有限公司招标部；<br>联系电话：010-63268382 转 8004；<br>通讯地址：北京市丰台区广安路 9 号院国投财富广场 5 号楼 12A15 室。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |        |               |    |  |     |     |   |       |        |        |   |           |        |        |
| 25  | 代理费           | 收费对象：<br><input type="checkbox"/> 采购人<br><input checked="" type="checkbox"/> 成交供应商<br><br>收费标准：采购代理机构采用差额累进方式计算服务费，<br>按下表计算出的收费金额下浮 30%计取。<br><table border="1"><thead><tr><th rowspan="2">序号</th><th rowspan="2">金 额 M<br/>(万元)</th><th colspan="2">费率</th></tr><tr><th>货 物</th><th>服 务</th></tr></thead><tbody><tr><td>1</td><td>M≤100</td><td>1. 50%</td><td>1. 50%</td></tr><tr><td>2</td><td>100&lt;M≤500</td><td>1. 10%</td><td>0. 80%</td></tr></tbody></table><br>成交服务费缴纳信息：<br><br>开户名（全称）：永明项目管理有限公司北京第一分公司<br>开户银行：招商银行北京丽泽商务区支行<br>账        号：110948262310701 | 序号     | 金 额 M<br>(万元) | 费率 |  | 货 物 | 服 务 | 1 | M≤100 | 1. 50% | 1. 50% | 2 | 100<M≤500 | 1. 10% | 0. 80% |
| 序号  | 金 额 M<br>(万元) | 费率                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |        |               |    |  |     |     |   |       |        |        |   |           |        |        |
|     |               | 货 物                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 服 务    |               |    |  |     |     |   |       |        |        |   |           |        |        |
| 1   | M≤100         | 1. 50%                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 1. 50% |               |    |  |     |     |   |       |        |        |   |           |        |        |
| 2   | 100<M≤500     | 1. 10%                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 0. 80% |               |    |  |     |     |   |       |        |        |   |           |        |        |
| 26  | 履约保证金         | 本项目不涉及。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |        |               |    |  |     |     |   |       |        |        |   |           |        |        |

## 供应商须知

### 一 说 明

#### 1 采购人、采购代理机构、供应商、联合体

1.1 采购人、采购代理机构：指依法进行政府采购的国家机关、事业单位、团体组织，及其委托的采购代理机构。本项目采购人、采购代理机构见第一章《采购邀请》。

1.2 供应商（也称“申请人”）：指向采购人提供货物、工程或者服务的法人、其他组织或者自然人。

1.3 联合体：指两个以上的自然人、法人或者其他组织组成一个联合体，以一个供应商的身份共同参加政府采购。

#### 2 资金来源、项目属性、科研仪器设备采购

2.1 资金来源为财政性资金和/或本项目采购中无法与财政性资金分割的非财政性资金。

2.2 项目属性见《供应商须知资料表》。

2.3 是否属于科研仪器设备采购见《供应商须知资料表》。

#### 3 现场考察、磋商前答疑会

3.1 若《供应商须知资料表》中规定了组织现场考察、召开磋商前答疑会，则供应商应按要求在规定的的时间和地点参加。

3.2 由于未参加现场考察或磋商前答疑会而导致对项目实际情况不了解，影响响应文件编制、报价准确性、综合因素响应不全面等问题的，由供应商自行承担不利评审后果。

#### 4 政府采购政策（包括但不限于下列具体政策要求）

##### 4.1 采购本国货物、工程和服务

4.1.1 政府采购应当采购本国货物、工程和服务。但有《**中华人民共和国政府采购法**》第十条规定情形的除外。

4.1.2 本项目如接受非本国货物、工程、服务参与投标，则具体要求见第

#### 四章《采购需求》。

- 4.1.3 进口产品指通过中国海关报关验放进入中国境内且产自关境外的产品，包括已经进入中国境内的进口产品。关于进口产品的相关规定依据《政府采购进口产品管理办法》（财库〔2007〕119号文）、《关于政府采购进口产品管理有关问题的通知》（财办库〔2008〕248号文）。

#### 4.2 中小企业、监狱企业及残疾人福利性单位

##### 4.2.1 中小企业定义：

- 4.2.1.1 中小企业是指在中华人民共和国境内依法设立，依据国务院批准的中小企业划分标准确定的中型企业、小型企业和微型企业，但与大企业的负责人为同一人，或者与大企业存在直接控股、管理关系的除外。符合中小企业划分标准的个体工商户，在政府采购活动中视同中小企业。关于中小企业的相关规定依据《中华人民共和国中小企业促进法》、《关于进一步加大政府采购支持中小企业力度的通知》（财库〔2022〕19号）、《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）、《关于印发中小企业划型标准规定的通知》（工信部联企业〔2011〕300号）。

- 4.2.1.2 供应商提供的货物、工程或者服务符合下列情形的，享受中小企业扶持政策：

（1）在货物采购项目中，货物由中小企业制造，即货物由中小企业生产且使用该中小企业商号或者注册商标；

（2）在工程采购项目中，工程由中小企业承建，即工程施工单位为中小企业；

（3）在服务采购项目中，服务由中小企业承接，即提供服务的人员为中小企业依照《中华人民共和国劳动合同法》订立劳动合同的从业人员。

- 4.2.1.3 在货物采购项目中，供应商提供的货物既有中小企业制造货物，也有大型企业制造货物的，不享受中小企业扶持政策。
- 4.2.1.4 以联合体形式参加政府采购活动，联合体各方均为中小企业的，联合体视同中小企业。其中，联合体各方均为小微企业的，联合体视同小微企业。
- 4.2.2 在政府采购活动中，监狱企业视同小型、微型企业，享受预留份额、评审中价格扣除等政府采购促进中小企业发展的政府采购政策。监狱企业定义：是指由司法部认定的为罪犯、戒毒人员提供生产项目和劳动对象，且全部产权属于司法部监狱管理局、戒毒管理局、直属煤矿管理局，各省、自治区、直辖市监狱管理局、戒毒管理局，各地（设区的市）监狱、强制隔离戒毒所、戒毒康复所，以及新疆生产建设兵团监狱管理局、戒毒管理局的企业。
- 4.2.3 在政府采购活动中，残疾人福利性单位视同小型、微型企业，享受预留份额、评审中价格扣除等促进中小企业发展的政府采购政策。残疾人福利性单位定义：享受政府采购支持政策的残疾人福利性单位应当同时满足以下条件：
- 4.2.3.1 安置的残疾人占本单位在职职工人数的比例不低于 25%（含 25%），并且安置的残疾人人数不少于 10 人（含 10 人）；
- 4.2.3.2 依法与安置的每位残疾人签订了一年以上（含一年）的劳动合同或服务协议；
- 4.2.3.3 为安置的每位残疾人按月足额缴纳了基本养老保险、基本医疗保险、失业保险、工伤保险和生育保险等社会保险费；
- 4.2.3.4 通过银行等金融机构向安置的每位残疾人，按月支付了不低于单位所在区县适用的经省级人民政府批准的月最低工资标准的工资；
- 4.2.3.5 提供本单位制造的货物、承担的工程或者服务（以下简

称产品），或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）；

4.2.3.6 前款所称残疾人是指法定劳动年龄内，持有《中华人民共和国残疾人证》或者《中华人民共和国残疾军人证（1至8级）》的自然人，包括具有劳动条件和劳动意愿的精神残疾人。在职职工人数是指与残疾人福利性单位建立劳动关系并依法签订劳动合同或服务协议的雇员人数。

4.2.4 本项目是否专门面向中小企业预留采购份额见第一章《采购邀请》。

4.2.5 采购标的对应的中小企业划分标准所属行业见《供应商须知资料表》。

4.2.6 小微企业价格评审优惠的政策调整：见第三章《评审方法和评审标准》。

#### 4.3 政府采购节能产品、环境标志产品

4.3.1 政府采购节能产品、环境标志产品实施品目清单管理。财政部、发展改革委、生态环境部等部门根据产品节能环保性能、技术水平和市场成熟程度等因素，确定实施政府优先采购和强制采购的产品类别及所依据的相关标准规范，以品目清单的形式发布并适时调整。依据品目清单和认证证书实施政府优先采购和强制采购。

4.3.2 采购人拟采购的产品属于品目清单范围的，采购人及其委托的采购代理机构依据国家确定的认证机构出具的、处于有效期之内的节能产品、环境标志产品认证证书，对获得证书的产品实施政府优先采购或强制采购。关于政府采购节能产品、环境标志产品的相关规定依据《关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9号）。

4.3.3 如本项目采购产品属于实施政府强制采购品目清单范围的节能产品，则供应商所报产品必须获得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，否则**响应无效**；

- 4.3.4 非政府强制采购的节能产品或环境标志产品，依据品目清单和认证证书实施政府优先采购。优先采购的具体规定见第三章《评审方法和评审标准》（如涉及）。

#### 4.4 正版软件

- 4.4.1 依据《财政部国家发展改革委信息产业部关于印发无线局域网产品政府采购实施意见的通知》（财库〔2005〕366号），采购无线局域网产品和含有无线局域网功能的计算机、通信设备、打印机、复印机、投影仪等产品的，优先采购符合国家无线局域网安全标准（GB 15629.11/1102）并通过国家产品认证的产品。其中，国家有特殊信息安全要求的项目必须采购认证产品，否则**响应无效**。财政部、国家发展改革委、信息产业部根据政府采购改革进展和无线局域网产品技术及市场成熟等情况，从国家指定的认证机构认证的生产厂商和产品型号中确定优先采购的产品，并以“无线局域网认证产品政府采购清单”（以下简称清单）的形式公布。清单中新增认证产品厂商和型号，由财政部、国家发展改革委、信息产业部以文件形式确定、公布并适时调整。
- 4.4.2 各级政府部门在购置计算机办公设备时，必须采购预装正版操作系统软件的计算机产品，相关规定依据《国家版权局、信息产业部、财政部、国务院机关事务管理局关于政府部门购置计算机办公设备必须采购已预装正版操作系统软件产品的通知》（国权联〔2006〕1号）、《国务院办公厅关于进一步做好政府机关使用正版软件工作的通知》（国办发〔2010〕47号）、《财政部关于进一步做好政府机关使用正版软件工作的通知》（财预〔2010〕536号）。

#### 4.5 网络安全专用产品

- 4.5.1 所投产品属于列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品，应当在国家互联网信息办公室会同工业和信息化部、公安部、国家认证认可监督管理委员会统一公布和更新的符合

要求的网络关键设备和网络安全专用产品清单中。

#### 4.6 采购需求标准

##### 4.6.1 商品包装、快递包装政府采购需求标准（试行）

为助力打好污染防治攻坚战，推广使用绿色包装，根据财政部关于印发《商品包装政府采购需求标准（试行）》、《快递包装政府采购需求标准（试行）》的通知（财办库〔2020〕123号），本项目如涉及商品包装和快递包装的，则其具体要求见第四章《采购需求》。

##### 4.6.2 绿色数据中心政府采购需求标准（试行）

为加快数据中心绿色转型，根据财政部生态环境部工业和信息化部关于印发《绿色数据中心政府采购需求标准（试行）》的通知（财库〔2023〕7号），本项目如涉及绿色数据中心，则具体要求见第四章《采购需求》。

#### 5 响应费用

- 5.1 供应商应自行承担所有与准备和参加磋商有关费用，无论磋商的结果如何，采购人或采购代理机构在任何情况下均无承担这些费用的义务和责任。

## 二 竞争性磋商文件

#### 6 竞争性磋商文件构成

##### 6.1 竞争性磋商文件包括以下部分：

- 第一章 采购邀请
- 第二章 供应商须知
- 第三章 评审方法和评审标准
- 第四章 采购需求
- 第五章 合同草案条款
- 第六章 响应文件格式

- 6.2 供应商应认真阅读竞争性磋商文件的全部内容。供应商应按照竞争性磋商文件要求提交响应文件并保证所提供的全部资料的真实性，并对竞争性磋商

商文件做出实质性响应，否则**响应无效**。

7 对竞争性磋商文件的澄清或修改

7.1 采购人、采购代理机构或者磋商小组对已发出的竞争性磋商文件进行必要澄清或者修改的，将以书面形式通知所有获取竞争性磋商文件的潜在供应商。采用公告方式邀请供应商参与的，还将在原公告发布媒体上发布更正公告。

7.2 上述书面通知，按照获取竞争性磋商文件的潜在供应商提供的联系方式发出，因提供的信息有误导致通知延迟或无法通知的，采购人或采购代理机构不承担责任。

7.3 澄清或者修改的内容为竞争性磋商文件的组成部分，并对所有获取竞争性磋商文件的潜在供应商具有约束力。澄清或者修改的内容可能影响响应文件编制的，将在提交首次响应文件截止之日 3 个工作日前，以书面形式通知所有获取磋商文件的供应商；不足上述时间的，将顺延提交响应文件截止时间。

### 三 响应文件的编制

8 响应范围、竞争性磋商文件中计量单位的使用及磋商语言

8.1 本项目如划分采购包，供应商可以对本项目的其中一个采购包进行响应，也可同时对多个采购包进行响应。供应商应当对所参与采购包对应第四章《采购需求》所列的全部内容进行响应，不得将一个采购包中的内容拆分响应，否则其对该采购包的响应将被认定为**无效响应**。

8.2 除竞争性磋商文件有特殊要求外，本项目磋商所使用的计量单位，应采用中华人民共和国法定计量单位。

8.3 除专用术语外，响应文件及来往函电均应使用中文书写。必要时专用术语应附有中文解释。供应商提交的支持资料和已印制的文献可以用外文，但相应内容应附有中文翻译本，在解释响应文件时以中文翻译本为准。未附中文翻译本或翻译本中文内容明显与外文内容不一致的，其不利后果由供应商自行承担。

## 9 响应文件构成

- 9.1 供应商应当按照竞争性磋商文件的要求编制响应文件，并对其提交的响应文件的真实性、合法性承担法律责任。响应文件的部分格式要求，见第六章《响应文件格式》。
- 9.2 对于竞争性磋商文件中标记了“实质性格式”文件的，供应商不得改变格式中给定的文字所表达的含义，不得删减格式中的实质性内容，不得自行添加与格式中给定的文字内容相矛盾的内容，不得对应当填写的空格不填写或不实质性响应，**否则响应无效**。未标记“实质性格式”的文件和竞争性磋商文件未提供格式的内容，可由供应商自行编写。
- 9.3 第三章《评审方法和评审标准》中涉及的证明文件。
- 9.4 对照第四章《采购需求》，说明所提供货物和服务已对第四章《采购需求》做出了响应，或申明与第四章《采购需求》的偏差和例外。如第四章《采购需求》中要求提供证明文件的，供应商应当按具体要求提供证明文件。
- 9.5 供应商认为应附的其他材料。

## 10 报价

- 10.1 所有响应均以人民币报价。
- 10.2 供应商的报价应包括为完成本项目所发生的一切费用和税费，采购人将不再支付报价以外的任何费用。供应商的报价应包括但不限于下列内容，  
《供应商须知资料表》中有特殊规定的，从其规定。
  - 10.2.1 响应货物及标准附件、备品备件、专用工具等的出厂价（包括已在中国国内的进口货物完税后的仓库交货价、展室交货价或货架交货价）和运至最终目的地的运输费和保险费，安装调试、检验、技术服务、培训、质量保证、售后服务、税费等；
  - 10.2.2 按照竞争性磋商文件要求完成本项目的全部相关费用。
- 10.3 采购人不得向供应商索要或者接受其给予的赠品、回扣或者与采购无关的其他商品、服务。
- 10.4 供应商不能提供任何有选择性或可调整的最后报价（竞争性磋商文件另有

规定的除外），否则其**响应无效**。

## 11 磋商保证金

- 11.1 供应商应按《供应商须知资料表》中规定的金额及要求交纳磋商保证金。
- 11.2 交纳磋商保证金可采用的形式：政府采购法律法规接受的支票、汇票、本票、网上银行支付或者金融机构、担保机构出具的保函等非现金形式。
- 11.3 磋商保证金到账（保函提交）截止时间同首次响应文件提交截止时间。以支票、汇票、本票、网上银行支付等形式提交磋商保证金的，应在首次响应文件提交截止时间前到账；以金融机构、担保机构出具的保函等形式提交磋商保证金的，应在首次响应文件提交截止时间前将原件提交至采购代理机构；由于到账时间晚于首次响应文件提交截止时间的，或者票据错误、印鉴不清等原因导致不能到账的，其**响应无效**。
- 11.4 磋商保证金有效期同响应有效期。
- 11.5 供应商为联合体的，可以由联合体中的一方或者多方共同交纳磋商保证金，其交纳的保证金对联合体各方均具有约束力。
- 11.6 采购人、采购代理机构将及时退还供应商的保证金，采用银行保函、担保机构担保函等形式递交的保证金，经供应商同意后采购人、采购代理机构可以不再退还，但因供应商自身原因导致无法及时退还的除外：
  - 11.6.1 已提交响应文件的供应商，在提交最后报价之前，可以根据磋商情况退出磋商。采购人、采购代理机构将退还退出磋商的供应商的磋商保证金；
  - 11.6.2 成交供应商的磋商保证金，在采购合同签订后 5 个工作日内退还成交供应商；
  - 11.6.3 未成交供应商的磋商保证金，在成交通知书发出后 5 个工作日内退还。
- 11.7 有下列情形之一的，采购人或采购代理机构不予退还磋商保证金：
  - 11.7.1 供应商在提交响应文件截止时间后撤回响应文件的；
  - 11.7.2 供应商在响应文件中提供虚假材料的；

11.7.3 除因不可抗力或磋商文件认可的情形以外，成交供应商不与采购人签订合同的；

11.7.4 供应商与采购人、其他供应商或者采购代理机构恶意串通的；

11.7.5 《供应商须知资料表》规定的其他情形。

## 12 响应有效期

12.1 响应文件应在本竞争性磋商文件《供应商须知资料表》中规定的响应有效期内保持有效，响应有效期少于竞争性磋商文件规定期限的，其**响应无效**。

## 13 响应文件的签署、盖章

13.1 供应商的响应文件**正本（1份）、副本（3份）、电子版份数（1份，格式为 Word 版及与正本一致的 PDF 盖章版，应保证能正常打开并使用，U 盘形式，不予退还）**，响应文件的纸质正本及副本须在封面清楚地标明“正本”或“副本”；响应文件的纸质正本及副本须在封面除了清楚地标明“正本”或“副本”外，还应尽量注明该纸质文件的内容（例如“上册”、“下册”、“图纸”或“附件”等）。

13.2 若响应文件副本与正本不符，以正本为准。电子版与纸制文件不符，以纸制文件为准。所有纸制文件须牢固装订成册，凡用活页夹、文件夹、塑料方便式书脊(插入式或穿孔式)均不认为是牢固装订。

13.3 任何行间插字、涂改和增删，必须由法定代表人（单位负责人）或委托代理人在旁边签字才有效。

13.4 竞争性磋商文件要求盖章的内容，均为供应商公章，其他印章如投标专用章、业务专用章、合同专用章等均无效。

## 四 响应文件的提交

### 14 响应文件的提交

14.1 供应商应将响应文件“正本”、“副本”、“电子版”密封为一包，在包装封面上标明项目名称、项目编号/包号、供应商单位名称、“于\_\_\_\_\_之前不得开启的字样”和正本与副本数量。

14.2 供应商应将“报价一览表”单独密封，并在包装上标明“报价一览表”字

样。

- 14.3 供应商应将电子文档 U 盘（格式为 Word 版及与正本一致的 PDF 盖章版，应保证能正常打开并使用）单独置于一小包装内，并在该包装上标明“电子文档”字样。
- 14.4 响应文件有其它组成部分或分册装订等情况，应尽量注明包装内的内容（例如“上册”、“下册”、“图纸”、“附件”或“视频”等）。
- 14.5 供应商在响应文件递交截止时间前提交对其响应文件中价格等相关内容进行修改的磋商声明的，应与报价一览表一并或者单独包装，单独包装时需按密封要求加施明显标记。
- 14.6 如果未按本条上述要求加写标记，采购人和采购代理机构对误投或提前启封概不负责。

#### 15 响应文件提交截止时间

- 15.1 供应商应在竞争性磋商文件要求提交响应文件截止时间前，将响应文件纸质版提交至竞争性磋商文件预先确定的地点。

#### 16 响应文件的修改与撤回

- 16.1 提交响应文件截止时间前，供应商可以对所提交的响应文件进行补充、修改或者撤回，但应就其补充、修改或者撤回通知采购人或采购代理机构。
- 16.2 供应商对响应文件的补充、修改的内容应当按照竞争性磋商文件要求签署、盖章，作为响应文件的组成部分。补充、修改的内容与响应文件不一致的，以补充、修改的内容为准。

## 五 评审

#### 17 响应文件的开启

- 17.1 采购人或采购代理机构将按竞争性磋商文件的规定，在响应文件提交截止时间的同一时间和竞争性磋商文件预先确定的地点开启响应文件。
- 17.2 供应商应在竞争性磋商文件要求提交响应文件截止时间前，将响应文件提交至指定地点，逾期送达或者未按照竞争性磋商文件要求密封的响应文件，采购人、采购代理机构将拒收。

17.3 供应商认为采购人员及相关人员与其他供应商有利害关系的，可以向采购人或采购代理机构书面提出回避申请，并说明理由。采购人或采购代理机构将及时询问被申请回避人员，有利害关系的被申请回避人员将回避。

17.4 供应商不足 3 家的，不予开启。

17.5 本项目不公开报价。

## 18 磋商小组

18.1 磋商小组根据政府采购有关规定和本次采购项目的特点进行组建，并负责具体评审与磋商事务，独立履行职责。

18.2 评审专家须符合《财政部关于在政府采购活动中查询及使用信用记录有关问题的通知》（财库〔2016〕125 号）的规定。依法自行选定评审专家的，采购人和采购代理机构将查询有关信用记录，对具有行贿、受贿、欺诈等不良信用记录的人员，拒绝其参与政府采购活动。

## 19 评审方法和评审标准

19.1 见第三章《评审方法和评审标准》。

# 六 确定成交

## 20 确定成交供应商

20.1 采购人将在收到评审报告后，从评审报告提出的成交候选供应商中，按照排序由高到低的原则确定成交供应商。采购人是否授权磋商小组直接确定成交供应商，见《供应商须知资料表》。成交候选人并列的，按照《供应商须知资料表》要求确定成交供应商。

## 21 成交公告与成交通知书

21.1 采购人或采购代理机构将在成交供应商确定后 2 个工作日内，将成交结果通知所有供应商，同时向成交供应商发出成交通知书。

21.2 成交通知书对采购人和成交供应商均具有法律效力。成交通知书发出后，采购人改变成交结果的，或者成交供应商放弃成交项目的，应当依法承担法律责任。

## 22 终止

22.1 出现下列情形之一的，采购人或采购代理机构将终止竞争性磋商采购活动，发布项目终止公告并说明原因，重新开展采购活动：

22.1.1 因情况变化，不再符合规定的竞争性磋商采购方式适用情形的；

22.1.2 出现影响采购公正的违法、违规行为的；

22.1.3 除了“市场竞争不充分的科研项目，以及需要扶持的科技成果转化项目，提交最后报价的供应商可以为 2 家；政府购买服务项目（含政府和社会资本合作项目），在采购过程中符合要求的供应商（社会资本）只有 2 家的，竞争性磋商采购活动可以继续进行的”的情形外，在采购过程中符合要求的供应商或者报价未超过采购预算的供应商不足 3 家的。

## 23 签订合同

23.1 采购人与成交供应商应当在成交通知书发出之日起 30 日内，按照磋商文件确定的合同文本以及采购标的、规格型号、采购金额、采购数量、技术和服务要求等事项签订政府采购合同。

23.2 成交供应商拒绝签订政府采购合同的，采购人可以按照评审报告推荐的成交候选人名单排序，确定下一候选人为成交供应商，也可以重新开展采购活动。拒绝签订政府采购合同的成交供应商不得参加对该项目重新开展的采购活动。

23.3 联合体成交的，联合体各方应当共同与采购人签订合同，就采购合同约定的事项向采购人承担连带责任。

23.4 政府采购合同不能转包。

23.5 采购人允许采用分包方式履行合同的，成交供应商可以依法采取分包方式履行合同。本项目是否允许分包，见《供应商须知资料表》。政府采购合同分包履行的，应当在响应文件中载明分包承担主体，分包承担主体应当具备相应资质条件且不得再次分包，**否则响应无效**。成交供应商就采购项目和分包项目向采购人负责，分包供应商就分包项目承担责任。

## 24 询问与质疑

## 24.1 询问

24.1.1 供应商对政府采购活动事项有疑问的，可依法提出询问，并按《供应商须知资料表》载明的形式送达采购人或采购代理机构。

24.1.2 采购人或采购代理机构对供应商依法提出的询问，在 3 个工作日内作出答复，但答复的内容不得涉及商业秘密。

## 24.2 质疑

24.2.1 供应商认为竞争性磋商文件、采购过程、成交结果使自己的权益受到损害的，可以在知道或者应知其权益受到损害之日起 7 个工作日内，以书面形式向采购人、采购代理机构提出质疑。采购人、采购代理机构在收到质疑函后 7 个工作日内作出答复。

24.2.2 质疑函须使用财政部制定的范本文件。供应商为自然人的，质疑函应当由本人签字；供应商为法人或者其他组织的，质疑函应当由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。

24.2.3 供应商委托代理人进行质疑的，应当随质疑函同时提交供应商签署的授权委托书。授权委托书应当载明代理人的姓名或者名称、代理事项、具体权限、期限和相关事项。供应商为自然人的，应当由本人签字；供应商为法人或者其他组织的，应当由法定代表人、主要负责人签字或者盖章，并加盖公章。

24.2.4 供应商应在法定质疑期内一次性提出针对同一采购程序环节的质疑，法定质疑期内针对同一采购程序环节再次提出的质疑，采购人、采购代理机构有权不予答复。

24.3 接收询问和质疑的联系部门、联系电话和通讯地址见《供应商须知资料表》。

## 25 代理费

25.1 收费对象、收费标准及缴纳时间见《供应商须知资料表》。由成交供应商支付的，成交供应商须一次性向采购代理机构缴纳代理费，报价应包含代理费用。

## 26 履约保证金

- 26.1 在签订合同前，成交供应商应按供应商须知资料表规定的金额、担保形式和磋商文件第五章“合同草案条款”规定的履约保证金格式向采购人提交履约保证金。
- 26.2 成交供应商不能按本章第 26.1 项要求提交履约保证金的，视为放弃成交资格，其磋商保证金不予退还，给采购人造成的损失超过磋商保证金数额的，成交供应商还应当对超过部分予以赔偿。

### 第三章 评审方法和评审标准

#### 一、资格审查程序

##### 1 响应文件的资格审查和符合性审查

1.1 磋商小组将根据《资格审查要求》和《符合性审查要求》中规定的内容，对供应商进行检查，并形成检查结果。供应商《响应文件》有任何一项不符合《资格审查要求》和《符合性审查要求》要求的，视为未实质性响应磋商文件。未实质性响应磋商文件的响应文件按**无效响应**处理，磋商小组应当告知提交响应文件的供应商。

1.2 《资格审查要求》中对格式有要求的，除竞争性磋商文件另有规定外，均为“实质性格式”文件。

1.3 《资格审查要求》见下表：

资格审查要求

| 序号  | 检查因素                    | 检查内容                                                                                                                                                                                                                                                                                                   | 格式要求            |
|-----|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| 1   | 满足《中华人民共和国政府采购法》第二十二条规定 | 具体规定见第一章《采购邀请》                                                                                                                                                                                                                                                                                         |                 |
| 1-1 | 营业执照等证明文件               | 供应商为企业（包括合伙企业）的，应提供有效的“营业执照”；<br>供应商为事业单位的，应提供有效的“事业单位法人证书”；<br>供应商是非企业机构的，应提供有效的“执业许可证”、“登记证书”等证明文件；<br>供应商是个体工商户的，应提供有效的“个体工商户营业执照”；<br>供应商是自然人的，应提供有效的自然人身份证明。<br>分支机构参加响应的，应提供该分支机构或其所属法人/其他组织的相应证明文件；同时还应提供其所属法人/其他组织出具的授权其参与本项目的授权书（格式自拟，须加盖其所属法人/其他组织的公章）；对于银行、保险、石油石化、电力、电信等行业的分支机构，可以提供上述授权，也 | 提供证明文件复印件加盖单位公章 |

| 序号  | 检查因素           | 检查内容                                                                                                                                                                                                                                                                                                                                                                                         | 格式要求                   |
|-----|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
|     |                | 可以提供其所属法人/其他组织的有关文件或制度等能够证明授权其独立开展业务的证明材料。                                                                                                                                                                                                                                                                                                                                                   |                        |
| 1-2 | 供应商资格声明书       | 提供了符合竞争性磋商文件要求的《供应商资格声明书》。                                                                                                                                                                                                                                                                                                                                                                   | 格式见《响应文件格式》            |
| 1-3 | 供应商信用记录        | <p>查询渠道：信用中国网站和中国政府采购网（<a href="http://www.creditchina.gov.cn">www.creditchina.gov.cn</a>、<a href="http://www.ccgp.gov.cn">www.ccgp.gov.cn</a>）；</p> <p>截止时点：首次响应文件提交截止时间以后、资格性检查阶段采购人或采购代理机构的实际查询时间为准；</p> <p>信用信息查询记录和证据留存具体方式：查询结果网页打印页作为查询记录和证据，与其他竞争性磋商文件一并保存；</p> <p>信用信息的使用原则：经认定的被列入失信被执行人、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的供应商，其<b>响应无效</b>。联合体形式磋商的，联合体成员存在不良信用记录，视同联合体存在不良信用记录。</p> | 无须供应商提供，由采购人或采购代理机构查询。 |
| 1-4 | 法律、行政法规规定的其他条件 | 法律、行政法规规定的其他条件                                                                                                                                                                                                                                                                                                                                                                               | /                      |
| 2   | 本项目的特定资格要求     | 具体要求见第一章《采购邀请》                                                                                                                                                                                                                                                                                                                                                                               |                        |
| 2-1 | 其他特定资格要求       | （1）供应商须为国家密码管理局发布的《商用密码检测机构（商用密码应用安全性评估业务）目录》中的机构，且具有商用密码检测机构资质证书；（2）供应商应具有公安部第三研究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。                                                                                                                                                                                                                                                                                 | 提供证明文件复印件加盖公章          |

1.4 《符合性审查要求》见下表：

符合性审查要求

| 序号 | 检查因素       | 检查内容                                                                                                                                                                             | 是否允许澄清、说明或者更正 |
|----|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| 1  | 授权委托书      | 按磋商文件要求提供授权委托书；                                                                                                                                                                  | 不允许           |
| 2  | 响应完整性      | 未将一个采购包中的内容拆开分包；                                                                                                                                                                 | 不允许           |
| 3  | 响应有效期      | 响应文件中承诺的响应有效期满足竞争性磋商文件中载明的响应有效期的；                                                                                                                                                | 不允许           |
| 4  | 实质性格式      | 标记为“实质性格式”的文件均按磋商文件要求提供且签署、盖章的；                                                                                                                                                  | 不允许           |
| 5  | 报价合理性      | 报价合理，或供应商的报价明显低于其他通过符合性审查供应商的报价，有可能影响服务质量或者不能诚信履约的，能够应磋商小组要求在规定时间内证明其报价合理性的；                                                                                                     | 允许            |
| 6  | ★号条款响应（如有） | 响应文件满足竞争性磋商文件第四章《采购需求》中★号条款要求的；                                                                                                                                                  | 不允许           |
| 7  | 串通响应       | 不存在以下视为供应商串通响应的情形：（一）不同供应商的响应文件由同一单位或者个人编制；（二）不同供应商委托同一单位或者个人办理磋商事宜；（三）不同供应商的响应文件载明的项目管理成员或者联系人员为同一人；（四）不同供应商的响应文件异常一致或者报价呈规律性差异；（五）不同供应商的响应文件相互混装；（六）不同供应商的磋商保证金从同一单位或者个人的账户转出； | 不允许           |
| 8  | 附加条件       | 响应文件未含有采购人不能接受的附加条件的；                                                                                                                                                            | 不允许           |
| 9  | 其他无效情形     | 供应商、响应文件不存在不符合法律、法规和竞争性磋商文件规定的其他无效情形。                                                                                                                                            | 不允许           |

2 磋商、响应文件有关事项的澄清、说明或者更正和最后报价

2.1 磋商小组所有成员应当集中与单一供应商分别进行磋商，并给予所有参加磋商的供应商平等的磋商机会。

- 2.2 在磋商过程中，磋商小组可以根据竞争性磋商文件和磋商情况实质性变动采购需求中的技术、服务要求以及合同草案条款，但不得变动竞争性磋商文件中的其他内容。实质性变动的内容，须经采购人代表确认。
- 2.3 对竞争性磋商文件作出的实质性变动是竞争性磋商文件的有效组成部分，磋商小组应当及时以书面形式同时通知所有参加磋商的供应商。
- 2.4 供应商应当按照竞争性磋商文件的变动情况和磋商小组的要求重新提交响应文件，并由其法定代表人或授权代表签字或者加盖公章。由授权代表签字的，应当附授权委托书。供应商为自然人的，应当由本人签字并附身份证明。
- 2.5 响应文件的澄清、说明或者更正：
- 2.5.1 磋商小组在对响应文件的有效性、完整性和响应程度进行审查时，可以要求供应商对响应文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容等作出必要的澄清、说明或者更正。
- 2.5.2 磋商小组对响应文件进行审查，如发现供应商提交的响应文件存在不满足《符合性审查要求》的内容，如属于表中“不允许”澄清、说明或者更正的内容，则供应商响应文件按**无效处理**；如属于表中的“允许”澄清、说明或更正的内容，磋商小组将要求供应商在规定的时间内对响应文件进行澄清、说明或者更正。如供应商在磋商小组规定的时间内未作出必要的澄清、说明或者更正，或澄清、说明或者更正后仍不能满足磋商文件要求的，则供应商的响应文件按**无效处理**。
- 2.5.3 供应商的澄清、说明或者更正不得超出响应文件的范围或者改变响应文件的实质性内容。磋商小组要求供应商澄清、说明或者更正响应文件应当以书面形式作出。供应商的澄清、说明或者更正应当由法定代表人或其授权代表签字或者加盖公章。由授权代表签字的，应当附授权委托书。供应商为自然人的，应当由本人签字并附身份

证明。澄清文件将作为响应文件内容的一部分。

- 2.6 磋商结束后，磋商小组将要求所有实质性响应的供应商在规定时间内提交最后报价。最后报价时间为磋商小组指定的时间，具体时间根据磋商进度另行通知。
- 2.7 竞争性磋商文件能够详细列明采购标的的技术、服务要求的，磋商结束后，磋商小组应当要求所有实质性响应的供应商在规定时间内提交最后报价，提交最后报价的供应商不得少于 3 家。竞争性磋商文件不能详细列明采购标的的技术、服务要求，需经磋商由供应商提供最终设计方案或解决方案的，磋商结束后，磋商小组应当按照少数服从多数的原则投票推荐 3 家以上供应商的设计方案或者解决方案，并要求其在规定时间内提交最后报价。市场竞争不充分的科研项目，以及需要扶持的科技成果转化项目，提交最后报价的供应商可以为 2 家；政府购买服务项目（含政府和社会资本合作项目），在采购过程中符合要求的供应商（社会资本）只有 2 家的，竞争性磋商采购活动可以继续进行。
- 2.8 最后报价是供应商响应文件的有效组成部分。
- 2.9 已提交响应文件的供应商，在提交最后报价之前，可以根据磋商情况退出磋商。
- 3 最后报价的算术修正及政策调整
- 3.1 最后报价须包含竞争性磋商文件全部内容，如最后分项报价表有缺漏视为已含在其他各项报价中，将不对最后报价总价进行调整。磋商小组有权要求供应商在评审现场合理的时间内对此进行书面确认，供应商不确认的，视为将一个采购包中的内容拆开响应，其**响应无效**。
- 3.2 最后报价出现前后不一致的，按照下列规定修正：
- 3.2.1 竞争性磋商文件对于报价修正是否另有规定：
- ☐有，具体规定为：\_\_\_\_\_
- ☒无，按下述 3.2.2-3.2.6 项规定修正。
- 3.2.2 大写金额和小写金额不一致的，以大写金额为准；

- 3.2.3 单价金额小数点或者百分比有明显错位的，以最后报价一览表的总价为准，并修改单价；
- 3.2.4 总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。
- 3.2.5 同时出现两种以上不一致的，按照前款规定的顺序修正。
- 3.2.6 修正后的报价经供应商书面确认后产生约束力，供应商不确认的，**其响应无效。**
- 3.3 落实政府采购政策的价格调整：只有符合第二章《供应商须知》4.2 条规定情形的，可以享受中小企业扶持政策，用扣除后的价格参加评审；否则，评审时价格不予扣除。
- 3.3.1 对于未预留份额专门面向中小企业采购的采购项目，以及预留份额项目中的非预留部分采购包，对小微企业报价给予 10% 的扣除，用扣除后的价格参加评审。
- 3.3.2 对于未预留份额专门面向中小企业采购的采购项目，以及预留份额项目中的非预留部分采购包，且接受大中型企业与小微企业组成联合体或者允许大中型企业向一家或者多家小微企业分包的采购项目，对于联合协议或者分包意向协议约定小微企业的合同份额占到合同总金额 30% 以上的联合体或者大中型企业的报价给予    % 的扣除，用扣除后的价格参加评审。
- 3.3.3 组成联合体或者接受分包的小微企业与联合体内其他企业、分包企业之间存在直接控股、管理关系的，不享受价格扣除优惠政策。
- 3.3.4 价格扣除比例对小型企业和微型企业同等对待，不作区分。
- 3.3.5 中小企业参加政府采购活动，应当按照竞争性磋商文件给定的格式出具《中小企业声明函》，否则不得享受相关中小企业扶持政策。
- 3.3.6 监狱企业提供了由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件的，视同小微企业。
- 3.3.7 残疾人福利性单位按竞争性磋商文件要求提供了《残疾人福利性单位声明函》（见附件）的，视同小微企业。

3.3.8 若供应商同时属于小型或微型企业、监狱企业、残疾人福利性单位中的两种及以上，将不重复享受小微企业价格扣减的优惠政策。

3.3.9 其他为落实政府采购政策实施的优先采购：\_\_\_\_/\_\_\_\_。

4 磋商环节及提交最后报价后如出现以下情况的，供应商的**响应文件无效**：

4.1 供应商对实质性变动不予确认的；

4.2 不满足竞争性磋商文件★号条款或竞争性磋商文件技术指标超出竞争性磋商文件《采购需求》中主要技术参数允许偏差的最大范围的（如有）；

4.3 未按照磋商小组规定的时间、逾期提交最后报价的；

4.4 如供应商的最后报价超过竞争性磋商文件中规定的项目/采购包预算金额或者项目/采购包最高限价的；

4.5 响应文件中出现可选择性或可调整的报价的（竞争性磋商文件另有规定的除外）；

4.6 最后报价出现前后不一致，供应商对修正后的报价不予确认的；

4.7 其他：\_\_\_\_/\_\_\_\_。

5 评审方法和评审标准

5.1 本项目采用的评审方法为：本项目的评审采用综合评分法。综合评分法，是指响应文件满足竞争性磋商文件全部实质性要求且按评审因素的量化指标评审得分最高的供应商为成交候选供应商的评审方法。

5.2 竞争性磋商文件中没有规定的评审标准不得作为评审依据。

5.3 非政府强制采购的节能产品或环境标志产品，依据品目清单和认证证书实施政府优先采购。优先采购的具体规定（如涉及）\_\_\_\_/\_\_\_\_。

5.4 关于无线局域网认证产品政府采购清单中的产品，优先采购的具体规定（如涉及）\_\_\_\_/\_\_\_\_。

6 确定成交候选人名单

6.1 磋商小组将根据各供应商的评审排序以及竞争性磋商文件中关于成交候选人的相关规定，确定本项目成交候选人名单，按照评审得分由高到低顺序推荐成交候选人的排名顺序。评审得分相同的，按照最后报价由低到高的

顺序推荐。评审得分且最后报价相同的，按照技术指标优劣顺序推荐。响应文件满足竞争性磋商文件全部实质性要求，且按照评审因素的量化指标评审得分最高的供应商为排名第一的成交候选人。评分分值计算保留小数点后两位，第三位四舍五入。

6.2 磋商小组根据上述供应商排序，依次推荐排序前 3 名的供应商为成交候选供应商（若在竞争性磋商文件允许的情形下提交最后报价的供应商为二家，则依次推荐二名供应商为成交候选供应商），并编写评审报告。

6.3 磋商小组要对评分汇总情况进行复核，特别是对排名第一的、报价最低的、响应文件被认定为无效的情形进行重点复核。

## 7 报告违法行为

7.1 磋商小组在评审过程中发现供应商有行贿、提供虚假材料或者串通等违法行为时，有向采购人、采购代理机构或者有关部门报告的职责。

## 二、评审标准

| 序号 | 评分因素       | 分值 | 评分标准                                                                                                                                                                                                                                                                                                                                                               |
|----|------------|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 一  | 商务部分（31 分） |    |                                                                                                                                                                                                                                                                                                                                                                    |
| 1  | 类似业绩       | 16 | <p>1. 供应商提供自 2022 年 6 月 1 日至递交响应文件当日（以签订合同日期为准）与本项目类似的信息化系统测评（含网络安全等级保护测评和商用密码应用安全评估）成功案例，每个得 2 分，最高得 10 分。<br/>注：提供有效合同关键页（包括但不限于：合同首页、采购内容页、签字盖章页等部分）复印件并加盖供应商公章，否则不得分。</p> <p>2. 供应商提供自 2022 年 6 月 1 日至递交响应文件当日（以签订合同日期为准）与本项目类似的网络安全等级保护测评或商用密码应用安全评估成功案例，每个得 2 分，最高得 6 分。<br/>注：提供有效合同关键页（包括但不限于：合同首页、采购内容页、签字盖章页等部分）复印件并加盖供应商公章，否则不得分。<br/>备注：上述两项业绩不累计。</p> |
| 2  | 资质证书       | 15 | <p>1. 具有国家认监委颁发的检验检测机构资质认定（CMA）证书（非实验室证书），且检验检测的能力范围至少涵盖信息系统安全等级保护测评的得 6 分，须提供认定证书检验检测的能力范围页复印件并加盖供应商公章，否则不得分。</p> <p>2. 具有中国合格评定国家认可委员会 CNAS 检验机构认可证书（不含实验室认可证书），且检验能力范围包括网络安全等级保护评测、信息安全风险评估、信息系统商用密码应用安全性评估的，检验能力范围每具备一项的得 3 分，最高得 9 分，须提供认定证书检验检测的能力范围页复印件并加盖供应商公章，否则不得分。</p>                                                                                  |
| 二  | 技术部分（59 分） |    |                                                                                                                                                                                                                                                                                                                                                                    |

|   |      |    |                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---|------|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | 技术方案 | 16 | <p>根据供应商针对本项目的技术服务方案进行综合评分:①项目服务方案、②项目质量保证措施、③项目周期安排、④重难点分析及解决方案、⑤增值服务、⑥测评实施方案、⑦测评人员安排、⑧应急预案等。</p> <p>注:评审专家从思路清晰性、合理性、可行性等方面对以上①-⑧项进行打分,每项满分2分,共16分。任意一项思路清晰、切实可行、阐述合理,得2分;任意一项对思路及可行性进行了简单阐述,但不够清晰详细,得1分;未提供相关内容的,不得分。</p>                                                                                                                                                                                                     |
| 2 | 项目团队 | 10 | <p>项目负责人:</p> <ol style="list-style-type: none"> <li>1. 具有高级“网络安全等级测评师”证书,得3分,须提供证书复印件并加盖供应商公章,否则不得分;</li> <li>2. 具有高级专业技术职称资格,得2分,须提供职称证复印件并加盖供应商公章,否则不得分;</li> <li>3. 工作经验5年及以上,得2分,须提供工作简历并加盖供应商公章,否则不得分;</li> <li>4. 提供作为项目负责人近三年(2022年6月1日起至今)所承担的类似商用密码应用安全性评估或网络安全等级保护测评项目,每提供一个业绩得1分,最高得3分,须提供有效合同关键页(包括但不限于:合同首页、采购内容页、签字盖章页等部分)复印件并加盖供应商公章,否则不得分。</li> </ol> <p>注:需提交响应文件前6个月内任意一个月缴纳社保证明或劳动合同复印件并加盖供应商公章,否则本项不得分。</p> |

|   |        |    |                                                                                                                                                                                                                                                                                                                                                             |
|---|--------|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   |        | 10 | <p>团队成员：</p> <p>1. 项目团队配备的测评人员不少于 6 人，得 2 分，出具拟派人员名单加盖供应商公章，否则不得分。</p> <p>2. 具有中级(含)以上网络安全等级测评师资格的人员占比不小于 60%，得 2 分，出具拟派人员资格证书复印件并加盖供应商公章，否则不得分。</p> <p>3. 团队成员从业经验均为 2 年（含）以上，得 2 分，出具拟派人员工作简历并加盖供应商公章，否则不得分。</p> <p>4. 每提供具备注册信息安全专业人员（CISP）证书的人员 1 名得 2 分，最高的 4 分，出具证书复印件并加盖供应商公章，否则不得分。</p> <p>注：需提交响应文件前 6 个月内任意一个月缴纳社保证明或劳动合同复印件并加盖供应商公章，否则本项不得分。</p> |
| 3 | 项目管理措施 | 10 | <p>根据供应商针对本项目的项目管理措施进行综合评分：①资金管理措施、②风险管理措施、③质量管理措施、④沟通协调管理措施、⑤人员管理措施等。</p> <p>注：评审专家从思路清晰性、合理性、可行性等方面对以上①-⑤项进行打分，每项满分 2 分，共 10 分。任意一项思路清晰、切实可行、阐述合理，得 2 分；任意一项对思路及可行性进行了简单阐述，但不够清晰详细，得 1 分；未提供相关内容的，不得分。</p>                                                                                                                                                |
| 4 | 售后服务方案 | 7  | <p>售后服务方案全面细致可行、针对性强、提供驻场服务，具备完善的服务体系，具有完备的售后服务体系，得 7 分；</p> <p>售后服务方案较全面、针对性有欠缺，提供驻场服务，售后服务体系较完整，得 5 分；</p> <p>售后服务方案有欠缺、针对性较差，提供驻场服务，有简单的售后服务体系，得 2 分；</p> <p>不提供驻场服务或售后服务方案较差，得 0 分。</p>                                                                                                                                                                 |

|    |            |     |                                                                                           |
|----|------------|-----|-------------------------------------------------------------------------------------------|
| 5  | 保密措施       | 6   | 保密措施细致可行、针对性强，得 6 分；<br>保密措施较细致、针对性较强，得 4 分；<br>保密措施有欠缺、针对性一般，得 2 分；<br>保密措施较差或未提供，得 0 分。 |
| 三  | 价格部分（10 分） |     |                                                                                           |
| 1  | 报价         | 10  | 满足竞争性磋商文件要求的最后报价最低的供应商的价格为磋商基准价，其价格分为满分。其他供应商的价格分统一按照下列公式计算：<br>磋商报价得分=（磋商基准价/最后报价）×分值    |
| 合计 |            | 100 |                                                                                           |

## 第四章 采购需求

### 一、需求清单

#### （一）项目概况

为贯彻落实《中华人民共和国网络安全法》、《中华人民共和国密码法》、《关键信息基础设施安全保护条例》、《关于印发〈信息安全等级保护管理办法〉的通知》（公通字〔2007〕43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）、《商用密码管理条例》等法律和文件规定，依据国家网络安全等级保护相关标准规范的要求，完成国家移民管理局互联网门户网站和政务服务平台等2个三级系统网络安全等级保护测评和商用密码应用安全评估。

#### （二）采购项目预（概）算

（1）预算金额 40 万元。

（2）付款方式

1. 合同签订后 15 日内，成交供应商提交等额普通发票，采购人收到发票后 10 日内向成交供应商支付合同总额的 40%款项；

2. 正式提交网络安全等级保护测评报告及密码应用安全性评估报告后 15 个工作日内，成交供应商提交等额普通发票，采购人收到发票后 10 日内向中标单位支付合同总额的 60%款项。

#### （三）采购标的需实现的功能或者目标

1. 采购标的需实现的功能

第三方测评机构根据《中华人民共和国网络安全法》规定以及《信息安全等级保护管理办法》和密码应用安全性评估有关要求，为有效应对日益严峻复杂的网络安全威胁和挑战，切实加强和改进网络安全工作，提高网络安全保障能力和水平。

2. 采购标的需实现的目标

通过开展网络安全等级保护测评和密码应用安全性评估工作，提高网络和信息系统自身安全水平，加强整体网络安全保障能力，提高安全管理水平。

（四）采购标的需执行的国家相关标准、行业标准、地方标准或者其他标准、规范

1. 国家有无强制标准要求

- 《中华人民共和国网络安全法》
- 《中华人民共和国数据安全法》
- 《关键信息基础设施安全保护条例》
- 《信息安全等级保护管理办法》（公通字〔2007〕43号）
- 《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》（公网安〔2020〕1960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）》
- GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》
- GB/T 25058-2019《信息安全技术 网络安全等级保护实施指南》
- GB/T 25070-2019《信息安全技术 网络安全等级保护安全设计技术要求》
- GB/T 22240-2020《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 20984-2022《信息安全技术 信息安全风险评估方法》
- T/ISEAA 001-2020《网络安全等级保护测评高风险判定指引》
- GB/T 36627-2018《信息安全技术 网络安全等级保护测试评估技术指南》
- GB/T 20984-2022《信息安全技术 信息安全风险评估方法》
- GM/Z 0001-2013《密码术语》
- 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》
- GM/T 0116-2021《信息系统密码应用测评过程指南》
- GB/T 33560-2017《信息安全技术-密码应用标识规范》
- 《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》

备注：以上标准如有最新标准发布，以最新标准执行。

#### （五）采购标的的数量、采购项目交付或者实施的时间和地点

##### 1. 采购标的的名称及数量

| 序号 | 名称                                                 | 数量 | 进口/国产 | 备注 |
|----|----------------------------------------------------|----|-------|----|
| 1  | 国家移民管理局互联网门户网站、政务服务平台 2 个三级系统网络安全等级保护测评和商用密码应用安全评估 | 1  | 国产    |    |

##### 2. 项目实施的地点：国家移民管理局指定地点

##### 3. 采购项目交付时间：合同签订后 180 日内。

#### （六）采购标的需满足的技术指标或者服务标准内容

##### 1 总体要求

国家移民管理局互联网门户网站和政务服务平台 2 个三级系统网络安全等级保护测评及商用密码应用安全评估项目（服务类）

服务内容包含：国家移民管理局互联网门户网站和政务服务平台网络安全等级保护测评及密码应用安全性评估。旨在为国家移民管理局互联网门户网站和政务服务平台提高网络和信息自身安全水平，详细服务要求如下：

##### 1.1 网络安全等级保护测评和安全测试

###### 1. 定级备案

依据 GB/T 22240-2020《信息安全技术 网络安全等级保护定级指南》，审核建设系统初步确定的安全等级，提出审核意见；组织召开定级专家评审会，提供定级意见；其他定级备案材料准备。

###### 2. 信息安全等级保护测评

依据 GB/T22239-2019《信息安全技术 网络安全等级保护基本要求》和 GB/T25070-2019《信息安全技术 网络安全等级保护安全设计技术要求》对已经建设的信息系统进行全面的安全检查与等级测评，通过对信息系统生命周期各环节进行安全把关，提升系统整体安全性。测评工作应依据 GB/T 28448-2019《信息安全技术 网

络安全等级保护测评要求》以及其他文件和标准完成测评，主要工作应包括：调研和测评方案编制、现场测评、安全整改、报告编制。

3. 安全测试

利用专业的工具，针对国家移民管理局互联网门户网站和政务服务平台的网络、系统、应用、安全域开展安全测试，包括系统脆弱性扫描、渗透测试。

1.2 密码应用安全性评估

按照《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）及有关密码评估标准，对国家移民管理局互联网门户网站和政务服务平台开展商用密码应用安全性评估工作。主要包括：调研与测评方案编制、现场评估、国家移民管理局互联网门户网站密码应用方案评审、安全整改，形成密码应用安全性评估报告及密码应用方案评估报告等。

2 详细设计要求

2.1 网络安全等级保护测评

2.1.1 定级备案

根据等级保护中对信息资产的分类分级的管理要求国家移民管理局互联网门户网站和政务服务平台进行分析、梳理和分类，主要内容包括系统、网络、物理环境、软硬件、数据等。

基本思路如下：

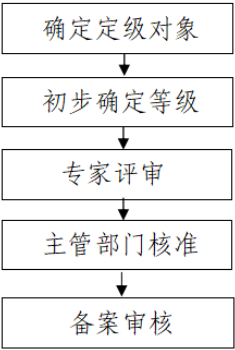


图 1：等级保护对象定级工作一般流程

安全保护等级初步确定为第二级及以上的等级保护对象，其网络运营者依据《定

级指南》要求组织进行专家评审、主管部门核准和备案审核，最终确定其安全保护等级。

2.1.2 信息安全等级测评

依据国家标准《实施指南》和《测评要求》完成已上线运行系统的网络安全等级测评工作，基本思路如下：

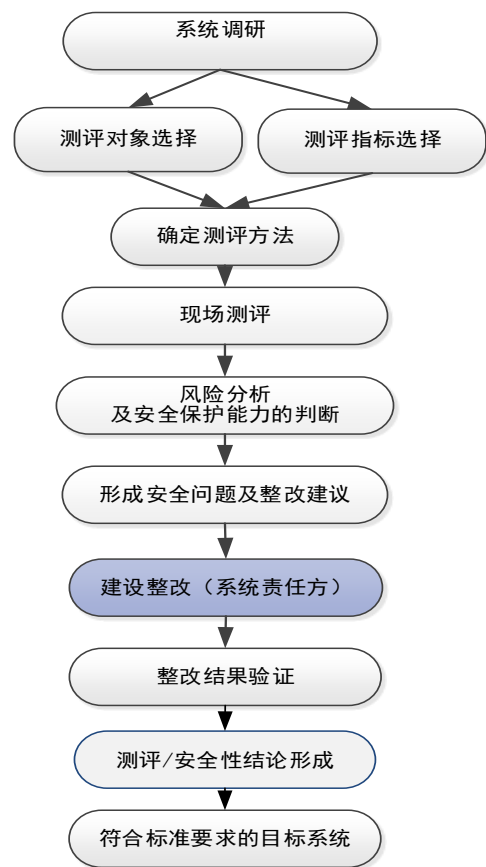


图 2：网络安全等级测评工作流程图

1. 系统调研

系统地识别国家移民管理局互联网门户网站、政务服务平台相关的信息资产，从技术和管理角度全面了解国家移民管理局互联网门户网站、政务服务平台信息化和信息安全现状，为编制等级测评方案打好基础。通过下发表单形式对测评系统的业务应用、业务数据、信息安全管理、信息系统运行做全面了解和统计，为现场工作计划采集数据。

## 2. 测评对象选择

等级测评中，不同级别的信息系统的测评强度和安全性要求是不同的，按初步定级和《信息安全技术网络安全等级保护测评要求》中规定执行。

## 3. 测评指标形成

由于国家对不同级别的信息系统有不同的安全保护能力要求，国家标准《信息安全技术信息系统安全等级保护基本要求》描述了不同级别信息系统应该实现的各类安全控制措施，信息系统的安全保护等级确定之后，对被测系统进行测评的测评指标的提取和形成，是等级测评工作的基础。

## 4. 现场测评内容确定和实施

在确定测评对象和测评指标后，就需要结合被测系统的实际情况，将测评指标落实到具体的测评对象上，形成需要进行现场测评的具体实施内容。

具体的做法上，就是把各层面上的测评指标结合到具体测评对象上，并说明具体的测试方法和测评对象，可构成一个个具体可实施的工作单元，现场实施的主要工作内容如下：

依据《信息安全技术网络安全等级保护测评要求》，从管理和技术两个方面十个层面开展现场数据的采集工作。

## 5. 风险分析及安全保护能力的判断

根据等级测评和后续安全性测试情况，对现场测评的单个测评对象的单个测评项的测评结果是否符合要求进行判断，即单项判定，形成单项判定结果（复核、部分符合、不符合）。根据单项判定结果和数据汇总统计情况进行系统整体测评分析，分析存在问题的测评项是否影响系统的整体安全保护能力，分析系统的整体结构是否合理。

## 6. 形成安全问题及整改建议

对影响系统的整体安全保护能力、系统整体结构安全的测评项综合分析，形成安全问题，最后提出有针对性的系统整改建议或意见。汇总分析等级测评中的不符合项，针对测评对象给出相关的改进建议，改进建议根据不符合项的重要程度、安全控制措施实施的难易程度、实施的时间周期等因素，可以分为立即整改建议和持续整改建议。

## 7. 整改结果验证

建设单位完成信息系统安全整改后，进行整改结果验证工作。主要是对原等级测评中发现的“部分符合”及“不符合”项进行再次测评。

## 8. 测评结论形成

在测评结果分析的基础上，通过层面汇总分析和综合分析等过程找出系统保护现状与等级保护基本要求之间的差距，并形成等级测评结论。

### 2.1.3 网络安全等级测评指标

根据公安部《信息安全等级保护管理办法》（公通字〔2007〕43号）、依据《信息安全技术 网络安全等级保护测评要求》等级保护测评应包括以下内容：

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 and 安全管理中心等五个方面的安全测评；

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、安全建设管理和安全运维管理等五个方面的安全测评。

#### （1）安全物理环境

安全物理环境层面涉及 10 个指标，具体如下表：

| 序号 | 指标名称    | 指标要求                                                                                    |
|----|---------|-----------------------------------------------------------------------------------------|
| 1  | 物理位置的选择 | a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内；<br>b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。                   |
| 2  | 物理访问控制  | 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。                                                           |
| 3  | 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；<br>b) 应将通信线缆铺设在隐蔽安全处；<br>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。 |
| 4  | 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；                                                             |

| 序号 | 指标名称  | 指标要求                                                                                                          |
|----|-------|---------------------------------------------------------------------------------------------------------------|
|    |       | 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。                                                                              |
| 5  | 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；<br>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；<br>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。 |
| 6  | 防水和防潮 | a) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；<br>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；<br>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。             |
| 7  | 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；<br>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。                                           |
| 8  | 温湿度控制 | 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。                                                                          |
| 9  | 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；<br>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；<br>c) 应设置冗余或并行的电力电缆线路为计算机系统供电。             |
| 10 | 电磁防护  | a) 电源线和通信线缆应隔离铺设，避免互相干扰；<br>b) 应对关键设备实施电磁屏蔽。                                                                  |

## (2) 安全通信网络

安全通信网络层面涉及网络架构、通信传输、可信验证 3 个指标，具体如下表：

| 序号 | 指标名称 | 指标要求                                                                                                                                                                                              |
|----|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | 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；<br>b) 应保证网络各个部分的带宽满足业务高峰期需要；<br>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；<br>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；<br>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。 |
| 2  | 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；<br>b) 应采用密码技术保证通信过程中数据的保密性。                                                                                                                                         |
| 3  | 可信验证 | 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。                                                                                        |

### (3) 安全区域边界

安全区域边界层面涉及边界防护、访问控制、入侵防范、可信验证、恶意代码防范和安全审计等 6 个指标，具体如下表：

| 序号 | 指标名称 | 指标要求                                                                                                                                       |
|----|------|--------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | 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；<br>b) 应能够对非授权设备私自联到内部网络的行为进行检查或限制；<br>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；<br>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 |

| 序号 | 指标名称   | 指标要求                                                                                                                                                                                                                                                  |
|----|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |        | 接入内部网络。                                                                                                                                                                                                                                               |
| 2  | 访问控制   | <p>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；</p> <p>b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；</p> <p>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；</p> <p>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；</p> <p>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。</p> |
| 3  | 入侵防范   | <p>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；</p> <p>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；</p> <p>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；</p> <p>d) 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。</p>                                                      |
| 4  | 可信验证   | 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。                                                                                                                                          |
| 5  | 恶意代码防范 | <p>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；</p> <p>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</p>                                                                                                                                                               |

| 序号 | 指标名称 | 指标要求                                                                                                                                                                                         |
|----|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |      | 圾邮件防护机制的升级和更新。                                                                                                                                                                               |
| 6  | 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；<br>b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；<br>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；<br>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。 |

#### (4) 安全计算环境

安全计算环境层面涉及身份鉴别、访问控制、安全审计、可信验证、入侵防范、恶意代码防范、数据完整性、数据保密性、数据备份恢复、剩余信息保护和个人信息保护等指标，具体如下表：

| 序号 | 指标名称 | 指标要求                                                                                                                                                                                                                    |
|----|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | 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；<br>b) 应具有登录失败处理功能，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自动退出等相关措施；<br>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；<br>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来实现。 |
| 2  | 访问控制 | a) 应对登录的用户分配账户和权限；<br>b) 应重命名或删除默认账户，修改默认账户的默认口令；                                                                                                                                                                       |

|   |      |                                                                                                                                                                                                                                                                       |
|---|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   |      | <p>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；</p> <p>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；</p> <p>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；</p> <p>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；</p> <p>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。</p>                                                   |
| 3 | 安全审计 | <p>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；</p> <p>b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；</p> <p>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；</p> <p>d) 应对审计进程进行保护，防止未经授权的中断。</p>                                                                                  |
| 4 | 入侵防范 | <p>a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；</p> <p>b) 应关闭不需要的系统服务、默认共享和高危端口；</p> <p>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；</p> <p>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；</p> <p>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；</p> <p>f) 应能够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。</p> |
| 5 | 恶意代码 | 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                                                                                                                                                                                                                                           |

|    |         |                                                                                                                                                                    |
|----|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | 防范      | 及时识别入侵和病毒行为，并将其有效阻断。                                                                                                                                               |
| 6  | 可信验证    | 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。                                                           |
| 7  | 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个人信息等；<br>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个人信息等。 |
| 8  | 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，包括但不限于鉴别数据、重要业务数据和重要个人信息等；<br>b) 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。                                                     |
| 9  | 安全备份和恢复 | a) 应提供重要数据的本地数据备份与恢复功能；<br>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份场地；<br>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。                                                                   |
| 10 | 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；<br>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。                                                                                             |
| 11 | 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；<br>b) 应禁止未授权访问和非法使用用户个人信息。                                                                                                                  |

#### (5) 安全管理中心

安全管理中心涉及 4 个指标，具体如下表：

| 序号 | 指标名称 | 指标要求                                                                                                                                                                                                                                                                            |
|----|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | 系统管理 | <p>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；</p> <p>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。</p>                                                                                                                                |
| 2  | 审计管理 | <p>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；</p> <p>b) 应通过审计管理员对审计记录应进行分析，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、管理和查询等。</p>                                                                                                                                               |
| 3  | 安全管理 | <p>a) 应对安全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管理操作，并对这些操作进行审计；</p> <p>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记，对主体进行授权，配置可信验证策略等。</p>                                                                                                                                         |
| 4  | 集中管控 | <p>a) 应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；</p> <p>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；</p> <p>c) 应对网络链路、安全设备、网络设备和服务器等运行状况进行集中监测；</p> <p>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；</p> <p>e) 应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；</p> <p>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。</p> |

## （6） 安全管理制度

安全管理制度涉及 4 个指标，具体如下表：

| 序号 | 指标名称  | 指标要求                                                                                                         |
|----|-------|--------------------------------------------------------------------------------------------------------------|
| 1  | 安全策略  | 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。                                                               |
| 2  | 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；<br>b) 应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；<br>c) 应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。 |
| 3  | 制定与发布 | 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；<br>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。                                             |
| 4  | 评审和修订 | 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。                                                             |

## （7） 安全管理机构

安全管理机构涉及 5 个指标，具体如下表：

| 序号 | 指标名称 | 指标要求                                                                                                                                                  |
|----|------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | 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；<br>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；<br>c) 应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。 |
| 2  | 人员配备 | a) 应配备一定数量的系统管理员、审计管理员和安全管理员等；<br>b) 应配备专职安全管理员，不可兼任。                                                                                                 |

| 序号 | 指标名称  | 指标要求                                                                                                                                                                            |
|----|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3  | 授权和审批 | <p>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；</p> <p>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；</p> <p>c) 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。</p>                 |
| 4  | 沟通和合作 | <p>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；</p> <p>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；</p> <p>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。</p>               |
| 5  | 审核和核查 | <p>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；</p> <p>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、安全配置与安全策略的一致性、安全管理制度的执行情况等；</p> <p>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。</p> |

#### (8) 安全人员管理

人员安全管理涉及 4 个指标，具体如下表：

| 序号 | 指标名称 | 指标要求                     |
|----|------|--------------------------|
| 1  | 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； |

| 序号 | 指标名称     | 指标要求                                                                                                                                                                                |
|----|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |          | b) 应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核；<br>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。                                                                                                |
| 2  | 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；<br>b) 应办理严格的调离手续，并承诺调离后的保密义务后方可离开。                                                                                                 |
| 3  | 安全意识和培训  | 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；<br>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；<br>c) 应定期对不同岗位的人员进行技能考核。                                                                      |
| 4  | 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，批准后可由专人全程陪同，并登记备案；<br>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，批准后可由专人开设账户、分配权限，并登记备案；<br>c) 外部人员离场后应及时清除其所有的访问权限；<br>d) 获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。 |

#### (9) 安全建设管理

安全建设管理涉及 10 个指标，具体如下表：

| 序号 | 指标名称  | 指标要求                                |
|----|-------|-------------------------------------|
| 1  | 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等级的方法和理由； |

| 序号 | 指标名称    | 指标要求                                                                                                                                                                                              |
|----|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |         | 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；<br>c) 应保证定级结果经过相关部门的批准；<br>d) 应将备案材料报主管部门和相应公安机关备案。                                                                                                      |
| 2  | 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；<br>b) 应根据保护对象的安全保护等级及与其他级别保护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；<br>c) 应组织相关部门和有关安全专家对安全整体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。                  |
| 3  | 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；<br>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；<br>c) 应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。                                                                                   |
| 4  | 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；<br>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；<br>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；<br>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；<br>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； |

| 序号 | 指标名称    | 指标要求                                                                                          |
|----|---------|-----------------------------------------------------------------------------------------------|
|    |         | 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；<br>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。                 |
| 5  | 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；<br>b) 应保证开发单位提供软件设计文档和使用指南；<br>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门和隐蔽信道。 |
| 6  | 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；<br>b) 应制定安全工程实施方案控制工程实施过程；<br>c) 应通过第三方工程监理控制项目的实施过程。           |
| 7  | 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；<br>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测试相关内容。   |
| 8  | 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；<br>b) 应对负责运行维护的技术人员进行相应的技能培训；<br>c) 应提供建设过程文档和运行维护文档。   |
| 9  | 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；<br>b) 应在发生重大变更或级别发生变化时进行等级测评；<br>c) 应确保测评机构的选择符合国家有关规定。    |
| 10 | 服务供应商选择 | a) 应确保服务供应商的选择符合国家的有关规定；<br>b) 应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务；                      |

| 序号 | 指标名称 | 指标要求                                    |
|----|------|-----------------------------------------|
|    |      | c) 应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。 |

#### (10) 安全运维管理

安全运维管理涉及 14 个指标，具体如下表：

| 序号 | 指标名称   | 指标要求                                                                                                                                                      |
|----|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | 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；<br>b) 应建立机房安全管理制度，对有关物理访问、物品带进出和环境安全等方面的管理作出规定；<br>c) 应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。 |
| 2  | 资产管理   | a) 应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；<br>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；<br>c) 应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。                     |
| 3  | 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；<br>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，并对介质的归档和查询等进行登记记录。                                        |
| 4  | 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；<br>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                                                                              |

| 序号 | 指标名称      | 指标要求                                                                                                                                                                                                                                                                                                                                                                                            |
|----|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |           | <p>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；</p> <p>c) 信息处理设备必须经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据必须加密；</p> <p>d) 含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。</p>                                                                                                                                                                                                                  |
| 5  | 漏洞和风险管理   | <p>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；</p> <p>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。</p>                                                                                                                                                                                                                                                                                         |
| 6  | 网络和系统安全管理 | <p>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；</p> <p>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；</p> <p>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；</p> <p>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；</p> <p>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、参数的设置和修改等内容；</p> <p>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；</p> <p>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</p> |

| 序号 | 指标名称     | 指标要求                                                                                                                                                                                                                                      |
|----|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |          | <p>志，操作结束后应同步更新配置信息库；</p> <p>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；</p> <p>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；</p> <p>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的行为。</p> |
| 7  | 恶意代码防范管理 | <p>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；</p> <p>b) 应定期验证防范恶意代码攻击的技术措施的有效性。</p>                                                                                                                                                    |
| 8  | 配置管理     | <p>a) 应记录和保存基本配置信息，包括网络拓扑结构、各个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；</p> <p>b) 应将基本配置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。</p>                                                                                                           |
| 9  | 密码管理     | <p>a) 应遵循密码相关国家标准和行业标准；</p> <p>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。</p>                                                                                                                                                                          |
| 10 | 变更管理     | <p>a) 应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施；</p> <p>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；</p> <p>c) 应建立中止变更并从失败变更中恢复的程序，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。</p>                                                                             |
| 11 | 备份和恢     | <p>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</p>                                                                                                                                                                                                      |

| 序号 | 指标名称       | 指标要求                                                                                                                                                                                                      |
|----|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | 复管理        | 等；<br>b) 应规定备份信息的备份方式、备份频度、存储介质、保存期等；<br>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。                                                                                                               |
| 12 | 安全事件<br>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；<br>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；<br>c) 应在安全事件报告和响应处理过程中，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；<br>d) 对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。 |
| 13 | 应急预案<br>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；<br>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；<br>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；<br>d) 应定期对原有的应急预案重新评估，修订完善。                                              |
| 14 | 外包运维<br>管理 | a) 应确保外包运维服务商的选择符合国家的有关规定；<br>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；<br>c) 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，并将能力要求在签订的协议中明确；                                                                |

| 序号 | 指标名称 | 指标要求                                                                        |
|----|------|-----------------------------------------------------------------------------|
|    |      | 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、存储要求，对 IT 基础设施中断服务的应急保障要求等。 |

#### (11) 云计算扩展

云计算扩展涉及 16 个指标，具体如下表：

| 序号 | 指标名称   |        | 指标要求                                                                                                                                                                                                                     |
|----|--------|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | 安全物理环境 | 基础设施位置 | 应保证云计算基础设施位于中国境内。                                                                                                                                                                                                        |
| 2  | 安全通信网络 | 网络架构   | a) 应保证云计算平台不承载高于其安全保护等级的业务应用系统；<br>b) 应实现不同云服务客户虚拟网络之间的隔离；<br>c) 应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力；<br>d) 应具有根据云服务客户业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略；<br>e) 应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务。 |
| 3  | 安全区域边界 | 访问控制   | a) 应在虚拟化网络边界部署访问控制机制，并设置访问控制规则；<br>b) 应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。                                                                                                                                                    |
| 4  |        | 入侵防范   | a) 应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；                                                                                                                                                                              |

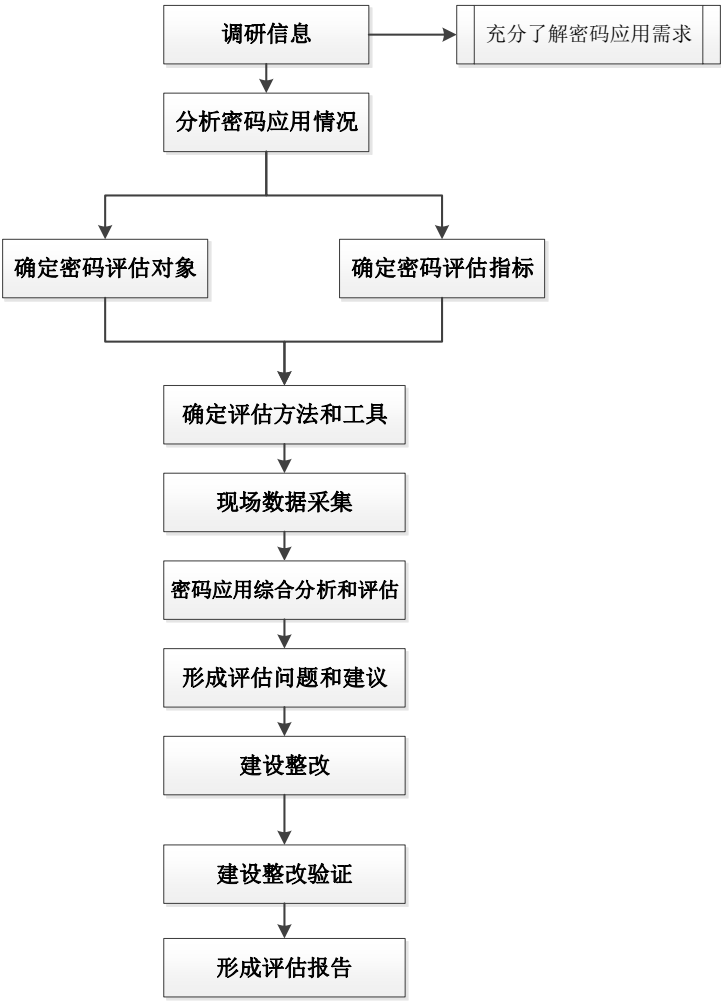
| 序号 | 指标名称   |         | 指标要求                                                                                                                      |
|----|--------|---------|---------------------------------------------------------------------------------------------------------------------------|
|    |        |         | b) 应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；<br>c) 应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量；<br>d) 应在检测到网络攻击行为、异常流量情况时进行告警。             |
| 5  |        | 安全审计    | a) 应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启；<br>b) 应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。                                   |
| 6  | 安全计算环境 | 身份鉴别    | 当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制。                                                                                   |
| 7  |        | 访问控制    | a) 应保证当虚拟机迁移时，访问控制策略随其迁移；<br>b) 应允许云服务客户设置不同虚拟机之间的访问控制策略。                                                                 |
| 8  |        | 入侵防范    | a) 应能检测虚拟机之间的资源隔离失效，并进行告警；<br>b) 应能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警；<br>c) 应能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警。                         |
| 9  |        | 镜像和快照保护 | a) 应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务；<br>b) 应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；<br>c) 应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 |

| 序号 | 指标名称   |           | 指标要求                                                                                                                                                                                                |
|----|--------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10 |        | 数据完整性和保密性 | a) 应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定；<br>b) 应确保只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限；<br>c) 应使用校验码或密码技术确保虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施；<br>d) 应支持云服务客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程。 |
| 11 |        | 数据备份恢复    | a) 云服务客户应在本地保存其业务数据的备份；<br>b) 应提供查询云服务客户数据及备份存储位置的能力；<br>c) 云服务商的云存储服务应保证云服务客户数据存在若干个可用的副本，各副本之间的内容应保持一致；<br>d) 应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。                                     |
| 12 |        | 剩余信息保护    | a) 应保证虚拟机所使用的内存和存储空间回收时得到完全清除；<br>b) 云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除。                                                                                                                              |
| 13 | 安全管理中心 | 集中管控      | a) 应能对物理资源和虚拟资源按照策略做统一管理调度与分配；<br>b) 应保证云计算平台管理流量与云服务客户业务流量分离；<br>c) 应根据云服务商和云服务客户的职责划分，收集各                                                                                                         |

| 序号 | 指标名称   |         | 指标要求                                                                                                                                                                                                                                                 |
|----|--------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |        |         | 自控制部分的审计数据并实现各自的集中审计；<br>d) 应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测。                                                                                                                                                              |
| 14 | 安全建设管理 | 云服务商选择  | a) 应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力；<br>b) 应在服务水平协议中规定云服务的各项服务内容和具体技术指标；<br>c) 应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等；<br>d) 应在服务水平协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关数据在云计算平台上清除；<br>e) 应与选定的云服务商签署保密协议，要求其不得泄露云服务客户数据。 |
| 15 |        | 供应链管理   | a) 应确保供应商的选择符合国家有关规定；<br>b) 应将供应链安全事件信息或安全威胁信息及时传达到云服务客户；<br>c) 应将供应商的重要变更及时传达到云服务客户，并评估变更带来的安全风险，采取措施对风险进行控制。                                                                                                                                       |
| 16 | 安全运维管理 | 云计算环境管理 | 云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。                                                                                                                                                                                                         |

### 2.2 密码应用安全性评估

根据《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）为标准，对国家移民管理局互联网门户网站、政务服务平台基本情况调研，并通过合理选择对象、指标、方法完成现场密码应用测评。基本思路和测试指标如下：



图：密码应用性安全评估流程示意图

#### 1、测评准备

根据测评双方签订的委托测评协议书和系统规模，测评机构组建测评项目组，从人员方面做好准备，并编制项目计划书。测评机构通过查阅被测系统已有资料并使用调查表格的方式，了解整个系统的构成和商用密码保护情况，为编写测评方案和开展

现场测评工作奠定基础。测评项目组成员在进行现场测评之前，熟悉与被测系统相关的各种组件、调试测评工具、准备各种表单等。

## 2、方案编制

根据已经了解到的被测系统信息，分析整个被测系统及其涉及的业务应用系统，以及与此相关的商用密码应用情况，确定出本次测评的测评对象；根据已经了解到的被测系统定级结果，确定出本次测评的测评指标；测评过程中，确认现场检查的关键安全点，并且充分考虑到检查的可行性和风险，最低限度的避免对被测系统，尤其是在线运行业务系统的影响；确定现场测评的具体实施内容，即单元测评内容；最终完成测评方案的编制。

## 3、现场测评

现场测评准备：召开测评现场首次会，测评机构介绍测评工作，交流测评信息，进一步明确测评计划和方案中的内容，说明测评过程中具体的实施工作内容，测评时间安排，测评过程中可能存在的安全风险等，以便于后面的测评工作开展。测评双方确认现场测评需要的各种资源，包括测评委托单位的配合人员和需要提供的测评条件等，确认被测系统已备份过系统及数据。测评委托单位签署现场测评授权书。测评人员根据会议沟通结果，对测评结果记录表单和测评程序进行必要的更新。

测评小组根据测评方案以及现场测评准备的结果，安排测评人员在现场完成测评工作，汇总现场测评的测评记录；召开测评现场结束会，测评双方对测评过程中发现的问题进行现场确认；测评机构归还测评过程中借阅的所有文档资料，并由测评委托单位文档资料提供者签字确认。

## 4、报告编制

在现场测评工作结束后，测评机构对现场测评获得的测评结果进行汇总分析，形成测评结论，并编制评估报告。

测评人员在初步判定单元测评结果后，进而进行整体测评，经过整体测评后，进行风险分析和评价，形成测评结论。

测评机构完成测评结果记录的整理、密码应用安全问题分析，并与评估系统建设、开发单位进行问题反馈，开发人员针对存在的密码应用安全问题进行相应的整改，经最终整改确认，编制完成评估报告。

依据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》通过对采购人指定的信息系统从物理和环境安全、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、应急处置等安全层面测评，给出信息系统在密码应用状况其相应要求之间的差距，并给出整改建议，合同期内完成项目商用密码应用安全性评估工作。

### 2.2.1 密码应用安全性评估指标

依据《信息安全技术信息系统密码应用基本要求》，密码应用安全性评估应包括以下内容：

密码技术测评：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；

密码管理测评：包括管理制度、人员管理、建设运行、应急处置等四个方面的安全测评。

#### （1）物理和环境安全

| 序号 | 指标名称              | 指标要求                                  |
|----|-------------------|---------------------------------------|
| 1  | 身份鉴别              | 宜采用密码技术进行物理访问身份鉴别，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<br>存储完整性 | 宜采用密码技术保证电子门禁系统进出记录数据的存储完整性。          |
| 3  | 视频监控记录数据<br>存储完整性 | 宜采用密码技术保证视频监控音像记录数据的存储完整性。            |
| 4  | 密码服务              | 以上如采用密码服务，应符合法律法规的相关要求并经商用密码认证机构认证合格。 |

| 序号 | 指标名称 | 指标要求                                |
|----|------|-------------------------------------|
| 5  | 密码产品 | 以上采用的密码产品，应达到 GB/T 37092 二级及以上安全要求。 |

## (2) 网络和通信安全

| 序号 | 指标名称           | 指标要求                                      |
|----|----------------|-------------------------------------------|
| 1  | 身份鉴别           | 应采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性。          |
| 2  | 通信数据完整性        | 宜采用密码技术保证通信过程中数据的完整性。                     |
| 3  | 敏感信息或通信报文的机密性  | 应采用密码技术保证通信过程中重要数据的机密性。                   |
| 4  | 网络边界访问控制信息的完整性 | 宜采用密码技术保证网络边界访问控制信息的完整性。                  |
| 5  | 安全接入认证         | 可采用密码技术对从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。 |
| 6  | 密码服务           | 以上如采用密码服务，应符合法律法规的相关要求并经商用密码认证机构认证合格。     |
| 7  | 密码产品           | 以上采用的密码产品，应达到 GB/T 37092 二级及以上安全要求。       |

## (3) 设备和计算安全

| 序号 | 指标名称          | 指标要求                              |
|----|---------------|-----------------------------------|
| 1  | 身份鉴别          | 应采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性。 |
| 2  | 安全的信息传输通道     | 远程管理设备时，应采用密码技术建立安全的信息传输通道。       |
| 3  | 系统资源访问控制信息完整性 | 宜采用密码技术保证系统资源访问控制信息的完整性。          |

| 序号 | 指标名称                    | 指标要求                                  |
|----|-------------------------|---------------------------------------|
| 4  | 重要信息资源安全标记完整性           | 宜采用密码技术保证设备中的重要信息资源安全标记的完整性。          |
| 5  | 日志记录完整性                 | 宜采用密码技术保证日志记录的完整性。                    |
| 6  | 重要可执行程序完整性、重要可执行程序来源真实性 | 宜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。  |
| 7  | 密码服务                    | 以上如采用密码服务，应符合法律法规的相关要求并经商用密码认证机构认证合格。 |
| 8  | 密码产品                    | 以上采用的密码产品，应达到 GB/T 37092 二级及以上安全要求。   |

#### (4) 应用和数据安全

| 序号 | 指标名称          | 指标要求                               |
|----|---------------|------------------------------------|
| 1  | 身份鉴别          | 应采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性。 |
| 2  | 访问控制信息完整性     | 宜采用密码技术保证信息系统应用的访问控制信息的完整性。        |
| 3  | 重要信息资源安全标记完整性 | 宜采用密码技术保证信息系统应用的重要信息资源安全标记的完整性。    |
| 4  | 重要数据传输机密性     | 应采用密码技术保证信息系统应用的重要数据在传输过程中的机密性。    |
| 5  | 重要数据存储机密性     | 应采用密码技术保证信息系统应用的重要数据在存储过程中的机密性。    |
| 6  | 重要数据传输完整性     | 宜采用密码技术保证信息系统应用的重要数据在传输过程中的完整性。    |

| 序号 | 指标名称      | 指标要求                                                                |
|----|-----------|---------------------------------------------------------------------|
| 7  | 重要数据存储完整性 | 宜采用密码技术保证信息系统应用的重要数据在存储过程中的完整性。                                     |
| 8  | 不可否认性     | 在可能涉及法律责任认定的应用中，宜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。 |
| 9  | 密码服务      | 以上如采用密码服务，应符合法律法规的相关要求并经商用密码认证机构认证合格。                               |
| 10 | 密码产品      | 以上采用的密码产品，应达到 GB/T 37092 二级及以上安全要求。                                 |

#### (5) 管理制度

| 序号 | 指标名称         | 指标要求                                                 |
|----|--------------|------------------------------------------------------|
| 1  | 具备密码应用安全管理制度 | 应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。 |
| 2  | 密钥管理规则       | 应根据密码应用方案建立相应密钥管理规则。                                 |
| 3  | 建立操作规程       | 应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。                          |
| 4  | 定期修订安全管理制度   | 应定期对密码应用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之处进行修订。      |
| 5  | 明确管理制度发布流程   | 应明确相关密码应用安全管理制度的发布流程并进行版本控制。                         |
| 6  | 制度执行过程记录留存   | 应具有密码应用操作规程的相关执行记录并妥善保存。                             |

#### (6) 人员管理

| 序号 | 指标名称                 | 指标要求                                                                                                                                                                                                                    |
|----|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | 了解并遵守密码相关法律法规和密码管理制度 | 相关人员应了解并遵守密码相关法律法规、密码应用安全管理制度。                                                                                                                                                                                          |
| 2  | 建立密码应用岗位责任制度         | <p>应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：</p> <p>1) 根据密码应用的实际情况，设置密钥管理员、密码审计员、密码操作员等关键安全岗位；</p> <p>2) 对关键岗位建立多人共管机制；</p> <p>3) 密钥管理、密码安全审计、密码操作人员职责互相制约互相监督，其中密码安全审计员岗位不可与密钥管理员、密码操作员兼任；</p> <p>4) 相关设备与系统的管理和使用账号不得多人共用。</p> |
| 3  | 建立上岗人员培训制度           | 应建立上岗人员培训制度，对于涉及密码的操作和管理的人员进行专门培训，确保其具备岗位所需专业技能。                                                                                                                                                                        |
| 4  | 定期进行安全岗位人员考核         | 应定期对密码应用安全岗位人员进行考核。                                                                                                                                                                                                     |
| 5  | 建立关键岗位人员保密制度和调离制度    | 应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。                                                                                                                                                                                         |

#### (7) 建设运行

| 序号 | 指标名称       | 指标要求                                              |
|----|------------|---------------------------------------------------|
| 1  | 制定密码应用方案   | 应依据密码相关标准和密码应用需求，制定密码应用方案。                        |
| 2  | 制定密钥安全管理策略 | 应根据密码应用方案，确定系统涉及的密钥种类、体系及其生命周期环节，各环节安全管理要求参照附录 B。 |

| 序号 | 指标名称                 | 指标要求                                                         |
|----|----------------------|--------------------------------------------------------------|
| 3  | 制定实施方案               | 应按照应用方案，制定实施方案。                                              |
| 4  | 投入运行前进行密码应用安全性评估     | 投入运行前应进行密码应用安全性评估，评估通过后系统方可正式运行。                             |
| 5  | 定期开展密码应用安全性评估及攻防对抗演习 | 在运行过程中，应严格执行既定的密码应用安全管理制度，应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。 |

#### (8) 应急处置

| 序号 | 指标名称          | 指标要求                                                        |
|----|---------------|-------------------------------------------------------------|
| 1  | 应急预案          | 应制定密码应用应急处置方案，做好应急资源准备，当密码应用安全事件发生时，应立即启动应急处置方案，结合实际情况及时处置。 |
| 2  | 事件处置          | 事件发生后，应及时向信息系统主管部门进行报告。                                     |
| 3  | 向有关主管部门上报处置情况 | 事件处置完成后，应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。                |

#### (七) 采购标的验收方案和标准

##### 1. 履约验收主体

1.1 采购单位：国家移民管理局

1.2 是否选择代理机构：否

1.3 是否邀请本项目的其他供应商：否

1.4 是否邀请专家：否

1.5 是否邀请服务对象：否

1.6 其他

2. 履约验收方式：简易程序

3. 履约验收程序：一次性验收

#### 4. 履约验收内容

##### 4.1 技术履约内容

完成采购需求中涉及的相关内容无偏离

##### 4.2 商务履约内容

具备投标单位相关资质无偏离

#### 5. 履约验收标准

承建方应提供服务直至国家移民管理局互联网门户网站和政务服务平台网络安全等级保护和密码应用安全性评估通过验收（包括成交供应商提交经采购人审核确认的最终密码应用安全性评估及网络安全等级测评报告）。

#### 6. 履约验收其他事项

完成网络安全等级保护和密码应用安全性评估并提供报告。

#### **（八）采购标的的其他技术、服务等要求**

##### 1. 其他技术、服务等要求。

要具有保质保量、按时完成项目的履约能力；能提供响应产品或服务通过检测、认证等情况，产品服务销售渠道，评审现场需提供顺畅、有效的商务和技术沟通等。

第三方测评机构需遵循：保证项目建设成果符合国家有关法律规定的要求；识别系统中可能存在的系统威胁、脆弱性等，评估可能由此造成的潜在风险，并提出改进建议。

##### 1.1 测评原则

为保障项目的顺利实施，在项目实施过程须遵循以下原则：

###### （1）规范性原则

供应商须根据项目实施的需要及采购人的要求，在人员、质量和时间进度等方面进行严格管控。

###### （2）标准化原则

测评过程须严格遵守国家和采购方的相关法律、法规、规范、标准等相关要求。

###### （3）完整性原则

供应商在测评过程中，必须确保测评数据、过程记录的完整性和真实性。

#### （4）保密性原则

在测评过程中，供应商须切实加强对人员、技术等方面的组织管理；供应商必须与采购人签署具有法律意义的保密协议，确保在项目实施过程中涉及的所有信息，不会泄露给第三方单位或个人，不得擅自利用这些信息。

#### （5）影响最小原则

供应商在项目实施的过程中，须充分考虑到相关活动对系统正常运行的不利影响，采取必要的措施将相关风险降到最低。

### 1.2 组织机构设置要求

根据项目特点，为进一步加强对本项目相关工作的组织领导和协调，第三方测评机构需成立项目领导小组，并选派资深技术人员组成实施团队。

第三方测评机构依据任务分工不同分为等级保护测评组、商用密码应用安全性评估组、风险评估组，根据实际情况可分为多个小组并行开展现场测评工作。

### 1.3 测评人员要求

（1）测评项目负责人需具有高级“网络安全等级测评师”证书及高级专业技术职称资格，且要求工作经验 5 年及以上；并对等级保护相关标准有深刻理解和准确把握，直接主持或参与制定等级保护相关标准。需提交响应文件前 6 个月内任意一个月缴纳社保证明或劳动合同。

（2）项目团队配备的测评人员不少于 6 人。其中，具有中级（含）以上网络安全等级测评师资格的人员占比应不小于 60%，应配置具备中级（含）网络安全等级测评师，从业经验 2 年（含）以上的人员；至少配备一名具有注册信息安全专业人员（CISP）证书（需提供该材料复印件）的人员。需提交响应文件前 6 个月内任意一个月缴纳社保证明或劳动合同。

### 2. 其他要求

成交供应商未经采购人许可，不得私自更换项目负责人和其它测评工程师。

各方向测评工程师在测评期间，可按照项目的需要进行人员调配，以满足不同时期的需要。

#### 2.1 保密性要求

项目实施期间，成交供应商团队成员不得将开发过程中接触到的业务数据用于任何形式的本项目以外的用途，不得私自复制、传播采购人所有的文件、数据。成交供应商未经采购人允许，不得以任何形式向第三方泄露项目开发源代码、技术资料及采购人的业务信息、数据、文档。

#### 4.2 实施周期要求

自合同签订之日 6 个月内完成，以出具整改建议报告为准。

共分两个阶段完成：

初次测评：自合同签订之日起 3 个月内完成，以完成网络安全等级初测、密码应用方案初测工作，并出具测试方案、安全问题列表及整改建议为准；

复测：自安全整改工作完成后 3 个月内完成，以完成全部网络安全等级测评、密码应用方案测评工作，并出具网络安全等级测评报告、密码应用安全性评估报告为准。

#### 4.3 成果要求

| 名称                       | 内容及形式要求 | 数量 | 交付时间      |
|--------------------------|---------|----|-----------|
| 《测试方案》                   | 电子版和纸质版 | 3  | 正式入场后 1 周 |
| 《网络安全等级保护测评报告》           | 电子版和纸质版 | 3  | 整改完毕后 4 周 |
| 《密码应用安全性评估报告》            | 电子版和纸质版 | 3  | 整改完毕后 4 周 |
| 国家移民管理局互联网门户网站密码应用方案评估报告 | 电子版和纸质版 | 3  | 整改完毕后 4 周 |

各测试报告应包括测试结果、测试结论、测试问题以及整改建议，并附详细的测试记录。

## 第五章 合同草案条款

合同编号：\_\_\_\_\_

# 国家移民管理局 互联网门户网站和政务服务平台等保及 商用密码应用评估项目采购合同

甲方： 国家移民管理局

乙方：

二〇二五年\_\_月

根据《中华人民共和国民法典》及其他相关法律规定，甲、乙双方本着平等互利的原则，就“国家移民管理局互联网门户网站和政务服务平台等保及商用密码应用评估项目”（以下简称“本项目”）的采购事宜，同意按下述条款签署本合同。

## 一、声明

（一）本合同中使用的词语和术语含义与合同条款中的定义相同。

（二）甲方将按照本合同约定向乙方支付合同价款，乙方在此保证全部按照合同的约定向甲方提供服务。

## 二、服务内容和期限

（一）服务内容

完成国家移民管理局互联网门户网站和政务服务平台等2个三级系统网络安全等级保护测评和商用密码应用安全评估服务（具体服务内容详见附件二）。

（二）服务期限：自本合同生效之日起180日内。其中：初次测评工作自合同生效之日起3个月内完成；复测工作自安全整改工作完成后3个月内完成。

## 三、服务费用

本合同服务费用为（大写）人民币\_\_\_\_\_整（小写）¥\_\_\_\_\_元。前述费用包含乙方因履行本合同所发生的服务费、税费等全部费用。除前述费用外，甲方无需向乙方支付任何其他费用。

## 四、支付和结算方式

（一）双方因本合同发生的一切费用均以人民币结算及支付，乙方的账户名称、开户银行及账号以本合同提供的为准。

（二）本合同生效后15个工作日内，乙方向甲方开具并送达等额、合法、有效的增值税普通发票，甲方收到前述发票后10个工作日内向乙方支付服务费用的40%，即（大写）人民币\_\_\_\_\_整（小写）¥\_\_\_\_\_元。

（三）甲方对本项目验收合格后，乙方向甲方开具并送达等额、合法、有效的增值税普通发票，甲方收到前述发票后10个工作日内向乙方支付服务费用的60%，即（大写）人民币\_\_\_\_\_整（小写）¥\_\_\_\_\_元。

## 五、验收方式及标准

### （一）验收方式

乙方完成本合同项下全部服务内容后，应以书面形式申请甲方对本项目进行验收，甲方在收到乙方验收申请后15日内组织验收。验收时，乙方应提交\_\_\_\_\_。符合验收标准的，为验收合格，双方签订《履约验收报告》。验收不合格的，甲方有权要求乙方限期整改或采取其他补救措施，直至验收合格。

### （二）验收标准

1. 乙方在服务期限内，提供的\_\_\_\_\_等满足甲方要求。
2. 乙方\_\_\_\_\_等服务内容满足甲方要求。
3. 乙方提交的《测试方案》、《国家移民管理局互联网门户网站密码应用方案评估报告》《最终密码应用安全性评估报告》《网络安全等级保护测评报告》等报告要素齐全、格式规范、内容完整，符合甲方要求。

## 六、甲、乙双方权利和义务

### （一）甲方的权利和义务

1. 甲方应按本合同约定及时、足额向乙方支付服务费用；
2. 甲方有权根据需要以书面形式向乙方下达工作任务；
3. 甲方有权根据项目要求监督乙方的服务质量；
4. 甲方负责协调乙方在提供服务过程中与相关的政府部门和单位沟通等有关事宜。

### （二）乙方的权利和义务

1. 乙方有权要求甲方按合同约定及时、足额支付服务费用；
2. 乙方应依法独立完成本合同项下的全部服务内容，不得以任何形式向第三方全部或部分转让本合同项下权利义务；
3. 乙方应严格按照本合同约定及甲方要求完成本合同项下的全部服务工作；
4. 乙方同意并保证尊重任何第三方的知识产权及其他合法权益，承诺其提供的服务不会侵犯任何第三方知识产权及其他合法权益，否则所引起的全部责任均应当由乙方承担；

5. 乙方承诺严格保守秘密，遵守安全管理规定，具体内容见附件一《保密责任承诺书》。

## **七、不可抗力**

（一）不可抗力指下列事件：战争、动乱、瘟疫、严重火灾、洪水、地震、风暴或其他自然灾害，以及本合同双方不能预见、不能避免且不能克服的一切其他客观情况。

（二）任何一方因不可抗力不能履行本合同约定的全部或部分义务，该方应尽快通知另一方，并须在不可抗力结束后三日内以书面形式向另一方提供详细情况报告及不可抗力对履行本合同的影响程度的说明。就上述不可抗力的发生须由受到不可抗力影响的一方负责同时提供由公证机关作出的公证证明。

（三）发生不可抗力事件，任何一方均不对因不可抗力无法履行或迟延履行本合同义务而使另一方蒙受的任何损失承担责任。但遭受不可抗力影响的一方有责任尽可能及时采取适当或必要措施减少或消除不可抗力的影响。遭受不可抗力影响的一方对因未尽本项责任而造成的相关损失承担责任。

（四）合同双方应根据不可抗力对本合同履行的影响程度，协商确定是否终止本合同，或是继续履行本合同。

## **八、合同的解释和法律适用**

（一）任何一方对本合同及其附件的解释均应遵循诚实信用原则，依照本合同签订时有效的中华人民共和国法律、法规以及通常的理解进行。

（二）对本合同的任何解释均应以书面作出。

（三）本合同及附件的订立、效力、履行、争议的解决等均适用本合同签订时有效的中华人民共和国法律、法规的有关规定。

## **九、合同的终止或解除**

出现下列任一情形的，本合同终止或解除：

- （一）本合同正常履行完毕；
- （二）合同双方协商一致终止本合同的履行；
- （三）不可抗力事件导致本合同无法履行或履行不能；

（四）任何一方行使解除权，解除本合同。

本合同终止或解除，对本合同终止或解除有过错的一方应赔偿另一方因合同终止或解除而遭受的全部损失；双方对合同终止或解除均无过错的，则各自承担所遭受的全部损失。

## **十、违约责任**

（一）因甲方原因造成乙方不能按照本合同约定提供服务的（如甲方需求变更），甲方应提前 10 个工作日书面通知乙方，与乙方协商达成一致后，由乙方根据实际情况协助甲方制定新的工作计划，并按新的工作计划开展工作。如甲、乙双方无法达成一致，乙方无需向甲方承担违约责任，但应积极配合甲方完成合同终止或变更的相关事宜。

（二）非因甲方原因，乙方不能按照本合同约定提供服务的，应提前 10 个工作日向甲方提交书面说明，详细列明无法履行合同的具体原因和拟采取的补救措施，乙方提出的补救措施须经甲方书面同意后方可执行。如乙方未按时提交书面说明或未按照甲方书面同意的内容采取有效补救措施，甲方有权要求乙方支付服务费用 20% 的违约金（最高不超过甲方实际损失的 30%），并有权从应付款项中直接扣除。

（三）若乙方违反本合同约定，给甲方造成损失的，甲方有权要求乙方赔偿甲方全部损失。甲方的全部损失除包括直接损失和间接损失外，还包括因维护自身合法权益而产生的律师费、诉讼费、公证费、公告费、保全保险费、交通费、差旅费等合理费用。

## **十一、争议解决**

（一）合同双方应通过友好协商解决因解释、履行本合同所发生的和本合同有关的一切争议。协商不成的，任何一方均应向甲方住所地有管辖权的人民法院提起诉讼。

（二）甲、乙双方一致同意，本合同仅属于甲、乙双方之间的协议，任何争议均应当按照本合同的约定方式解决。

（三）在争议解决期间，除诉讼过程中正在解决的部分问题外，合同其余部分应继续履行。

## **十二、其他事项**

（一）甲、乙双方协商一致，可以对本合同进行补充、修改或变更并另行签署书面补充协议。补充协议与本合同具有同等法律效力，与本合同对同一事项有不同约定的，以补充协议为准。

（二）本项目竞争性磋商文件、乙方响应文件及其全部条款作为本合同的组成部分，与本合同具有同等法律效力。如前述文件内容存在不一致的，按照本合同、响应文件、竞争性磋商文件的顺序进行解释。

（三）本合同自甲、乙双方法定代表人或其委托代理人签字并加盖单位公章或合同专用章之日起生效。本合同一式陆份，甲方执肆份，乙方执贰份，具有同等法律效力。

（四）附件作为本合同的重要组成部分，与合同正文具有同等法律效力。附件与合同正文对同一事项有不同约定的，以\_\_\_\_\_为准。

（以下无正文）

| 甲方（采购人）          |                | 乙方（供应商）          |              |
|------------------|----------------|------------------|--------------|
| 单位名称（公章或合同专用章）   | 国家移民管理局        | 单位名称（公章或合同专用章）   |              |
| 法定代表人或其委托代理人（签字） | 王志忠            | 法定代表人或其委托代理人（签字） |              |
|                  |                | 拥有者性别            |              |
| 住 所              | 北京市东城区东长安街 6 号 | 住 所              |              |
| 联 系 人            |                | 联 系 人            |              |
| 联系电话             |                | 联系电话             |              |
| 通信地址             | 北京市东城区东长安街 6 号 | 通信地址             |              |
| 邮政编码             | 100006         | 邮政编码             |              |
|                  |                | 统一社会信用代码         |              |
|                  |                | 账户名称             |              |
|                  |                | 开户银行             |              |
|                  |                | 银行账号             |              |
| 签订时间             | 2025 年__月__日   | 签订时间             | 2025 年__月__日 |

附件一

## 保密责任承诺书

甲方：国家移民管理局

乙方：\_\_\_\_\_

为明确乙方单位和人员的保密责任，遵守安全管理规定，有效保守甲方秘密，乙方作出以下承诺。

### 一、保密的内容与范围

1、甲方因乙方工作需要传送或交付给乙方的项目文件及未来传送或交付给乙方的与项目相关的任何商业、行政或其它相关信息、文件、资料等，包括但不限于乙方在提供服务过程中获知的既存和/或潜在的商业交易、可行性研究、建议、设计方案、建设项目等特定信息、资料，均属于保密信息的范畴。

2、下列各项将不被认为是保密信息：

- a) 保密信息已经公开或者在此后公开，但违反本承诺书条款导致公开的除外。
- b) 有书面记录证明在乙方接受甲方保密信息之前，乙方已享有该信息的权利并有权披露。
- c) 乙方完全独立地从第三方获得有关信息，并不受禁止披露的限制。
- d) 根据有关法律、法规、规定、有合法管辖权的法院或任何具备法定资格的司法、行政或政府机关作出的判决、裁决、决定命令而必须披露的信息。

### 二、违反安全管理义务的行为

违反安全管理义务的行为包括但不限于：网络安全方面，擅自建立跨网跨域运维通道，违规连接公安网络，设置应用系统后门、木马等恶意程序，恶意探测扫描网络及系统，拆除破坏监管设施、程序等；数据安全方面，违规下载、留存、使用公安数据，篡改、毁损、出售公安数据等；安全保密方面，擅自扩大与项目相关信息的知悉范围，不及时清除、收回离职离岗或者不再参与国家移民管理局互联网门户网站和政务服务平台等保及商用密码应用评估项目人员持有的公安文档资料、数据等。

### 三、保密责任

1、乙方对为甲方提供服务的整个过程中知悉的保密信息负有保密责任。乙方在为甲方提供服务的整个过程中，应遵守中华人民共和国的法律、法规及甲方保密工作管理规定，做到不该问的秘密不问，不准看的秘密不看，不该记录的秘密不记录。

2、非经甲方授权，乙方不得以任何直接或间接的方式泄露、散布、发表、披露、传递或者其它方式利用保密信息。

3、未经甲方同意，乙方不得对甲方的产品、建筑、设备设施及工作环境和场所摄像、拍照。

4、未经甲方同意，乙方不得私自携带各种涉密载体(如：文件、图纸、资料、计算机磁盘、光盘、活动硬盘等)。

5、乙方同意维护甲方通过口头、书面、来往信函和/或其它方式提供给乙方的保密信息的保密性，同意不将本承诺书项下的保密信息披露给除为达到甲方授权目的而需要知道保密信息的“特定人员”。该“特定人员”指乙方提供的经甲方认可的相关服务人员。

6、乙方承诺在保密期限内以严格保密的态度、方式对待保密信息。乙方同意将采取必要和适当的预防措施来维护保密信息的保密性。甲方有明确要求的，乙方承诺将遵循甲方以书面形式提出的要求乙方采取的任何合理防范措施。

7、乙方同意对其参加服务的相关工作人员进行保密教育，履行保密义务，签订保密协议，确保甲方利益。

8、乙方违反本承诺书造成泄密，给甲方造成损失的，甲方有追究乙方责任的权利，对构成犯罪的人员，交有关部门依法追究其法律责任。

### 四、保密信息的权利归属及移交

1、甲方作为保密责任承诺书项下保密信息的合法权利人，享有对保密信息的一切权利。乙方不应对保密信息的任何利用获得对保密信息的任何权利或利益。

2、一旦本承诺书所涉的项目终止或者经甲方要求，乙方应当及时归还甲方提供的所有/任何含有或属于保密信息的任何载体的材料，并且消除或销毁所有无形的相关保密信息。

## 五、保密期限

本承诺书经乙方法定代表人或委托代理人签字并加盖公章或合同专用章后持续有效，至甲方书面通知乙方终止本承诺书项下的义务时失效。保密期限同本承诺书有效期限。保密期限内，乙方应严格遵守本承诺书约定的保守秘密和限制使用保密信息的义务。

## 六、违约责任

如果乙方违反本承诺书中的保密义务或安全管理义务，甲方有权要求乙方承担以下一项或多项责任：

1、采取补救措施。乙方应采取切实有效的针对性补救措施，对违约行为限期整改。

2、支付违约金。违约金的计算标准为《国家移民管理局互联网门户网站和政务服务平台等保及商用密码应用评估项目采购合同》服务费用的 20%，违约金应在收到甲方书面通知后 30 日内支付，并由违约方承担消除负面影响产生的诉讼费、取证费、律师费等费用。如果违约金不足以弥补采购方损失的，甲方有权要求乙方赔偿损失，补足违约金不足部分。

3、提前解除《国家移民管理局互联网门户网站和政务服务平台等保及商用密码应用评估项目采购合同》。对违约行为无法采取补救措施且造成公安网络、数据无法恢复损失等特别严重后果，乙方拒不采取补救措施或采取补救措施后仍不符合安全管理要求，或者违约行为造成《国家移民管理局互联网门户网站和政务服务平台等保及商用密码应用评估项目采购合同》目的无法实现的，甲方有权单方提前解除《国家移民管理局互联网门户网站和政务服务平台等保及商用密码应用评估项目采购合同》。

4、失信惩戒措施。对同时构成违法犯罪的违约行为，甲方有权将涉事参与单位人员提请列入政府采购严重违法失信行为记录名单、市场监督管理严重失信名单。

5、后续追偿权利。鉴于有的违约行为造成的后果较长时间才能显现，或者损失数额难以一次性确认，甲方保留进一步追偿的权利。

## 七、争议解决

凡因本承诺书引起的或与本承诺书有关的任何争议，包括对本承诺书的任何违约事宜，双方均应本着诚信原则，进行友好协商，解决争议，如不能通过协商解决，可按照《国家移民管理局互联网门户网站和政务服务平台等保及商用密码应用评估项目采购合同》争议解决条款约定的方式解决。

#### 八、其他

1、本承诺书作为《国家移民管理局互联网门户网站和政务服务平台等保及商用密码应用评估项目采购合同》附件，与合同正文具有同等法律效力。

2、本承诺书一式陆份，甲方持肆份，乙方持贰份，具有同等法律效力。  
本承诺书自乙方法定代表人/委托代理人签字并加盖单位公章或合同专用章之日起生效。

乙方（盖章）：

法定代表人/委托代理人（签字）：

年 月 日

附件二

## 服务内容

完成国家移民管理局\_\_\_\_\_服务，主要实现功能及服务如下：详细参见需求文件。

## 第六章 响应文件格式

### 供应商编制文件须知

- 1、供应商按照本部分的顺序编制响应文件，编制中涉及格式资料的，应按照本部分提供的内容和格式（所有表格的格式可扩展）填写提交。
- 2、对于竞争性磋商文件中标记了“实质性格式”文件的，供应商不得改变格式中给定的文字所表达的含义，不得删减格式中的实质性内容，不得自行添加与格式中给定的文字内容相矛盾的内容，不得对应当填写的空格不填写或不实质性响应，**否则响应无效**。未标记“实质性格式”的文件和竞争性磋商文件未提供格式的内容，可由供应商自行编写。
- 3、全部声明和问题的回答及所附材料必须是真实的、准确的和完整的。

响应文件封面（非实质性格式）

# 响 应 文 件

项目名称：

项目编号：

供应商名称：

1 满足《中华人民共和国政府采购法》第二十二条规定

1-1 营业执照等证明文件复印件并加盖单位公章

1-2 供应商资格声明书（实质性格式）

供应商资格声明书

致：采购人或采购代理机构

在参与本次项目磋商中，我单位承诺：

- （一）具有良好的商业信誉和健全的财务会计制度；
- （二）具有履行合同所必需的设备和专业技术能力；
- （三）有依法缴纳税收和社会保障资金的良好记录；
- （四）参加政府采购活动前三年内，在经营活动中没有重大违法记录（重大违法记录指因违法经营受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚，不包括因违法经营被禁止在一定期限内参加政府采购活动，但期限已经届满的情形）；
- （五）我单位不属于政府采购法律、行政法规规定的公益一类事业单位、或使用事业编制且由财政拨款保障的群团组织（仅适用于政府购买服务项目）；
- （六）我单位不存在为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务后，再参加该采购项目的其他采购活动的情形（单一来源采购项目除外）；
- （七）与我单位存在“单位负责人为同一人或者存在直接控股、管理关系”的其他法人单位信息如下（如有，不论其是否参加同一合同项下的政府采购活动均须填写）：

| 序号  | 单位名称 | 相互关系 |
|-----|------|------|
| 1   |      |      |
| 2   |      |      |
| ... |      |      |

上述声明真实有效，否则我方负全部责任。

供应商名称（加盖公章）：\_\_\_\_\_

日期：\_\_\_\_年\_\_\_\_月\_\_\_\_日

说明：供应商承诺不实的，依据《政府采购法》第七十七条“提供虚假材料谋取中标、成交的”有关规定予以处理。

## 2 落实政府采购政策需满足的资格要求（如有）

### 2-1 中小企业政策证明文件

说明：

（1）如本项目（包）不专门面向中小企业预留采购份额，供应商无须提供《中小企业声明函》或《残疾人福利性单位声明函》或由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件；当供应商拟享受中小企业扶持政策时，仍应提供上述证明文件，否则不享受相关中小企业扶持政策。

（2）如本项目（包）专门面向中小企业采购，响应文件中须提供《中小企业声明函》或《残疾人福利性单位声明函》，或提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件。

（3）如本项目（包）预留部分采购项目预算专门面向中小企业采购，且要求获得采购合同的供应商将采购项目中的一定比例分包给一家或者多家中小企业或要求供应商以联合体形式参加采购活动，响应文件中须提供《中小企业声明函》或《残疾人福利性单位声明函》或由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件。

（4）中小企业声明函填写注意事项 1）《中小企业声明函》由参加政府采购活动的供应商出具。联合体参与的，《中小企业声明函》可由牵头人出具。

2）对于联合体中由中小企业承担的部分，或者分包给中小企业的部分，必须全部由中小企业制造、承建或者承接。供应商应当在声明函“标的名称”部分标明联合体中中小企业承担的具体内容或者中小企业的具体分包内容。

3）对于多标的采购项目，供应商应充分、准确地了解所提供货物的制造企业、提供服务的承接企业信息。对相关情况了解不清楚的，不建议填报本声明函。

（5）温馨提示：为方便广大中小企业识别企业规模类型，工业和信息化部组织开发了中小企业规模类型自测小程序，在国务院客户端和工业和信息化部网站上均有链接，供应商填写所属的行业和指标数据可自动生成企业规模类型测试结果。本项目中小企业划分标准所属行业详见第二章《供应商须知资料表》，如在该程序中未找

到本项目文件规定的中小企业划分标准所属行业，则按照《关于印发中小企业划型标准规定的通知（工信部联企业〔2011〕300号）》及本项目文件规定的中小企业划分标准所属行业执行。

## 中小企业声明函（服务）格式

本公司（联合体）郑重声明，根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）的规定，本公司（联合体）参加（单位名称）的（项目名称）采购活动，工程的施工单位全部为符合政策要求的中小企业（或者：服务全部由符合政策要求的中小企业承接）。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

1. （标的名称），属于（采购文件中明确的所属行业）行业；承建（承接）企业为（企业名称），从业人员\_\_\_\_\_人，营业收入为\_\_\_\_\_万元，资产总额为\_\_\_\_\_万元<sup>1</sup>，属于（中型企业、小型企业、微型企业）；

2. （标的名称），属于（采购文件中明确的所属行业）行业；承建（承接）企业为（企业名称），从业人员\_\_\_\_\_人，营业收入为\_\_\_\_\_万元，资产总额为\_\_\_\_\_万元，属于（中型企业、小型企业、微型企业）；

.....

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：\_\_\_\_\_

日期：\_\_\_\_\_

---

<sup>1</sup>从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报。

## 残疾人福利性单位声明函格式

本单位郑重声明，根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141 号）的规定，本单位（请进行选择）：

☐不属于符合条件的残疾人福利性单位。

☐属于符合条件的残疾人福利性单位，且本单位参加\_\_\_\_\_单位的\_\_\_\_\_项目采购活动提供本单位制造的货物（由本单位承担工程/提供服务），或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

单位名称（盖章）：\_\_\_\_\_

日 期：\_\_\_\_\_

### 3 本项目的特定资格要求

#### 3-1 其他特定资格要求：

（1）供应商须为国家密码管理局发布的《商用密码检测机构（商用密码应用安全性评估业务）目录》中的机构，且具有商用密码检测机构资质证书，提供证明文件复印件加盖单位公章。

（2）供应商应具有公安部第三研究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，提供证明文件复印件加盖单位公章。

#### 4 响应书（实质性格式）

### 响应书

致： （采购人或采购代理机构）

我方参加你方就\_\_\_\_\_（项目名称，项目编号）组织的采购活动，并对此项目进行磋商。

1. 我方已详细审查全部竞争性磋商文件，自愿参与磋商并承诺如下：

（1）本响应有效期为自提交响应文件的截止之日起 90 个日历日。

（2）除合同条款及采购需求偏离表列出的偏离外，我方响应竞争性磋商文件的全部要求。

（3）我方已提供的全部文件资料是真实、准确的，并对此承担一切法律后果。

（4）如我方成交，我方将在法律规定的期限内与你方签订合同，并在合同约定的期限内完成合同规定的全部义务。

2. 其他补充条款（如有）：\_\_\_\_\_。

与本磋商有关的一切正式往来信函请寄：

地址\_\_\_\_\_

传 真\_\_\_\_\_

电话\_\_\_\_\_

电子函件\_\_\_\_\_

供应商名称（加盖公章）：\_\_\_\_\_

日期：\_\_\_\_年\_\_\_\_月\_\_\_\_日

## 5 授权委托书（实质性格式）

### 授权委托书

本人\_\_\_\_（姓名）系\_\_\_\_（供应商名称）的法定代表人（单位负责人），现委托\_\_\_\_（姓名）为我方代理人。代理人根据授权，以我方名义签署、澄清确认、递交、撤回、修改\_\_\_\_（项目名称）响应文件和处理有关事宜，其法律后果由我方承担。

委托期限：自本授权委托书签署之日起至响应有效期届满之日止。

代理人无转委托权。

供应商名称（加盖公章）：\_\_\_\_\_

法定代表人（单位负责人）（签字或盖章）：\_\_\_\_\_

委托代理人（签字或盖章）：\_\_\_\_\_

日期：\_\_\_\_年\_\_\_\_月\_\_\_\_日

附：法定代表人（单位负责人）及委托代理人身份证复印件：

说明：

1. 若供应商为事业单位或其他组织或分支机构，则法定代表人（单位负责人）处的签署人可为单位负责人。
2. 若响应文件中签字之处均为法定代表人（单位负责人）本人签署，则可不提供本《授权委托书》，但须提供《法定代表人（单位负责人）身份证明》；否则，不需要提供《法定代表人（单位负责人）身份证明》。
3. 供应商为自然人的情形，可不提供本《授权委托书》。
4. 供应商应随本《授权委托书》同时提供法定代表人（单位负责人）及委托代理人的有效的身份证或护照等身份证明文件复印件。提供身份证的，应同时提供身份证**双面**复印件。

## 附：法定代表人（单位负责人）身份证明

致：\_\_\_\_（采购人或采购代理机构）

兹证明，

姓名：\_\_\_\_性别：\_\_\_\_年龄：\_\_\_\_职务：\_\_\_\_

系\_\_\_\_（供应商名称）的法定代表人（单位负责人）。

附：法定代表人（单位负责人）身份证或护照等身份证复印件。

供应商名称（加盖公章）：\_\_\_\_

法定代表人（单位负责人）（签字或盖章）：\_\_\_\_

日期：\_\_\_\_年\_\_\_\_月\_\_\_\_日

6 报价一览表

报价一览表

项目编号：\_\_\_\_\_ 项目名称：\_\_\_\_\_

| 序号 | 供应商名称 | 报价 |    |
|----|-------|----|----|
|    |       | 大写 | 小写 |
|    |       |    |    |

注：  
1. 此表中，每包的报价应和《分项报价表》中的总价相一致。

供应商名称（加盖公章）：\_\_\_\_\_

日期：\_\_\_\_年\_\_\_\_月\_\_\_\_日

7 分项报价表

### 分项报价表

项目编号：\_\_\_\_\_ 项目名称：\_\_\_\_\_ 报价单位：人民币元

| 序号    | 分项名称 | 单价（元） | 合价（元） | 备注/说明 |
|-------|------|-------|-------|-------|
| 1     |      |       |       |       |
| 2     |      |       |       |       |
| 3     |      |       |       |       |
| ...   |      |       |       |       |
|       |      |       |       |       |
|       |      |       |       |       |
| 总价（元） |      |       |       |       |

- 注：1. 如果不提供分项报价将视为没有实质性响应竞争性磋商文件；  
2. 上述各项的详细规格（如有），可另页描述。

供应商名称（加盖公章）：\_\_\_\_\_

日期：\_\_\_\_年\_\_\_\_月\_\_\_\_日

8 合同条款偏离表（实质性格式）

## 合同条款偏离表

项目编号：\_\_\_\_\_ 项目名称：\_\_\_\_\_

| 序号                                                                                                                                                                                                                                              | 竞争性磋商<br>文件条目号<br>(页码) | 竞争性磋商文<br>件要求 | 响应文件内容 | 偏离情况 | 说明 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|---------------|--------|------|----|
| <b>对本项目合同条款的偏离情况（应进行选择，未选择响应无效）：</b><br><input type="checkbox"/> <b>无偏离</b> （如无偏离，仅选择无偏离即可；无偏离即为对合同条款中的所有要求，均视作供应商已对之理解和响应。）<br><input type="checkbox"/> <b>有偏离</b> （如有偏离，则应在本表中对负偏离项逐列明，否则 <b>响应无效</b> ；对合同条款中的所有要求，除本表列明的偏离外，均视作供应商已对之理解和响应。） |                        |               |        |      |    |
|                                                                                                                                                                                                                                                 |                        |               |        |      |    |
|                                                                                                                                                                                                                                                 |                        |               |        |      |    |
|                                                                                                                                                                                                                                                 |                        |               |        |      |    |
|                                                                                                                                                                                                                                                 |                        |               |        |      |    |
|                                                                                                                                                                                                                                                 |                        |               |        |      |    |

注：“偏离情况”列应据实填写“正偏离”或“负偏离”。

供应商名称（加盖公章）：\_\_\_\_\_

日期：\_\_\_\_年\_\_\_\_月\_\_\_\_日

9 采购需求偏离表（实质性格式）

## 采购需求偏离表

项目编号：\_\_\_\_\_ 项目名称：\_\_\_\_\_

| 序号 | 竞争性磋商文件<br>条目号(页码) | 竞争性磋商文件要求 | 响应内容 | 偏离情况<br>(据实填写) | 说明 |
|----|--------------------|-----------|------|----------------|----|
|    |                    |           |      |                |    |
|    |                    |           |      |                |    |
|    |                    |           |      |                |    |
|    |                    |           |      |                |    |
|    |                    |           |      |                |    |
|    |                    |           |      |                |    |

注：

1. 对竞争性磋商文件中的所有商务、技术要求，除本表所列明的所有偏离外，均视作供应商已对之理解和响应。此表中若无任何文字说明，内容为空白的**响应无效**。
2. “偏离情况”列应据实填写“正偏离”、“无偏离”或“负偏离”。

供应商名称（加盖公章）：\_\_\_\_\_

日期：\_\_\_\_年\_\_\_\_月\_\_\_\_日

10 磋商文件要求提供或供应商认为应附的其他材料

## 11 最后报价一览表（实质性格式，磋商后提交）

## 最后报价一览表

项目编号: \_\_\_\_\_ 项目名称: \_\_\_\_\_

| 序号    | 供应商名称 | 最后报价 |    |
|-------|-------|------|----|
|       |       | 大写   | 小写 |
|       |       |      |    |
| 其他声明： |       |      |    |

注：1. 此表中，每包的最后报价应和《最后分项报价表》中的总价相一致；  
2. 此表无需在响应文件中提交，磋商后供应商按磋商小组要求提交。

供应商名称:

供应商授权代表签字（或加盖供应商公章）：\_\_\_\_\_

日期： 年 月 日

12 最后分项报价表（实质性格式，磋商后提交）

**最后分项报价表**

项目编号：\_\_\_\_\_ 项目名称：\_\_\_\_\_ 报价单位：人民币元

| 序号    | 分项名称 | 单价（元） | 合价（元） | 备注/说明 |
|-------|------|-------|-------|-------|
| 1     |      |       |       |       |
| 2     |      |       |       |       |
| 3     |      |       |       |       |
| ...   |      |       |       |       |
|       |      |       |       |       |
|       |      |       |       |       |
| 总价（元） |      |       |       |       |

注：1. 如果不提供分项报价将视为没有实质性响应磋商文件；  
2. 上述各项的详细规格（如有），可另页描述；  
3. 此表无需在响应文件中提交，磋商后供应商按磋商小组要求提交。

供应商名称：\_\_\_\_\_

供应商授权代表签字（或加盖供应商公章）：\_\_\_\_\_

日期：\_\_\_\_年\_\_\_\_月\_\_\_\_日