重庆江北国际机场有限公司

重庆机场外网网站、行李管理系统、生产调度系统、大数据平台、离港系统安全等级保护测评采购项目

比选文件

编号：服务2021-018

重庆江北国际机场有限公司

市场运营部（代章）

二〇二一年六月

重庆机场外网网站、行李管理系统、生产调度系统、大数据平台、离港系统安全等级保护测评采购项目比选文件

我司决定于近期将对重庆机场外网网站、行李管理系统、生产调度系统、大数据平台、离港系统安全等级保护测评项目实施采购邀请符合相应条件的供应商就本项目进行比选。

**一、项目实施内容及要求**

**1.1 资格要求**

1.1.1 在中华人民共和国依法注册、具有独立法人资格，具有有效营业执照。（注明须提供营业执照复印件加盖鲜章）

1.1.2 具有网络安全等级测评资质且响应人能够在公安部中国信息安全等级保护网www.djbh.net推荐目录中查询到。（提供证明材料复印件）

1.1.3非重庆本地测评机构须提交承诺函（附件4）。

1.1.4法定代表人为同一个人的两个及两个以上法人，母公司、全资子公司及其控股公司，以及其他形式有管理关系的响应人，都不得参与同一比选项目。

1.1.5 本项目不接受联合体投标，不得转包、分包。

**1.2 项目要求及报价要求**

1.2.1 测评要求：根据GB/T22239-2019国家标准对重庆机场外网网站、行李管理系统、生产调度系统、大数据平台、离港系统按照三级标准进行测评并出具测评结果报告。

1.2.2本项目的报价应包括：测评费用以及完成本项目所需的其他费用。本项目报价为包干价，不再另行增加费用。

本项目总价最高限价（不含税）为(¥617,250.00)元（大写金额：人民币陆拾壹万柒仟贰佰伍拾圆整）各系统限价详见下表，报价超过总价最高限价或分项限价，将取消比选响应方的比选资格。

|  |  |  |
| --- | --- | --- |
| **序号** | **系统名称** | **最高限价（不含税）(元）** |
| **1** | **重庆机场外网网站** | **111600** |
| **2** | **重庆机场行李管理系统** | **128000** |
| **3** | **重庆机场生产调度系统** | **124850** |
| **4** | **重庆机场大数据平台** | **125000** |
| **5** | **重庆机场离港系统** | **127800** |

在修正范围内的以下情形不作为比选响应文件作废的依据：

（1）比选响应文件中的大写金额与小写金额不一致的，以大写金额为准；

（2）数字表示的数额与用文字表示的数额不一致时，以文字数额为准；

（3）总价金额与依据单价计算出的结果不一致的，以单价金额为准修正总价，但单价金额小数点有明显错误的除外。

**二、合格报价供应商**

具有与本比选文件要求相适应的生产、安装和维修能力，包括供应能力、售后服务能力和安装能力的经营商。比选响应单位必须具备：

2.1 满足1.1资格要求;

2.2 法定代表人授权书；

2.3 法定代表人身份证复印件和被授权人身份证复印件；

**三、成交标准**

本次比选成交人确定办法采用**经评审满足条件的最低价**成交。

具体比选规则如下：

3.1 递交比选响应文件截止时，送达的比选响应文件少于3个的，应停止比选活动，将递交的比选响应文件退还比选响应人，并重新组织比选。重新比选仍然不足3个单位的，比选项目将可以继续进行比选。

3.2 如有项目因专业性及特殊性，导致有效比选响应人不足3个的，评审委员会应当否决所有比选响应人。但是有效比选响应人的经济、技术等指标仍然具有市场竞争力，能够满足比选文件要求的，评审委员会可以继续评审，根据符合采购需求、质量和服务，且报价最低的原则确定成交候选人。

3.3 项目重新比选时，经评审有有效比选响应人的，应当按规定程序，根据符合采购需求、质量和服务，且报价最低的原则确定成交候选人。

**四、比选文件信息发布**

比选文件及相关信息于2021年6月24日由重庆江北机场官网发布。

**五、项目比选响应保证金及履约保证金**

5.1 项目比选响应保证金：金额为人民币 10000 元整。

5.1.1 提交方式：比选响应人企业基本账户银行转账。比选响应人提交比选响应保证金后应到采购人计财部（重庆市渝北区机场西路26号重庆江北国际机场有限公司办公楼1楼）换取保证金收据，并将保证金收据复印件装入比选响应文件中。

开户名：重庆江北国际机场有限公司

开户银行：中国建设银行股份有限公司重庆渝北机场支行

账号：5005 0108 3800 0000 0060

注意：比选响应人递交比选响应文件时应出示采购人计财部开具的项目比选保证金收据，否则，采购人将拒收比选响应文件。

5.1.2 提交时间：比选开始前

5.1.3项目比选响应保证金的退还：成交候选人以外的项目比选响应保证金在成交结果公示期结束且无异议后，**比选响应单位开具收据（加盖比选响应单位财务专用章），附比选响应单位营业执照及账户信息（复印件加盖公章）**一并递交我司市场运营部，我司凭借该收据根据相关规定在20个工作日内将项目比选响应保证金以银行转账方式退还至比选响应人，该项目比选响应保证金递交期间不计利息。成交的比选人交纳的比选响应保证金将转为履约保证金。

5.2 履约保证金为合同不含税总价款的5%，在收到成交通知书10日内缴纳，于履约结束后，由使用部门一次性退还（不记利息）。非重庆本地测评机构，若未按承诺函要求（附件4），在收到成交通知书后10个工作日内提供重庆市公安局网络安全保卫总队的备案证明材料复印件（原件必查），我司将没收比选响应保证金或履约保证金并纳入重庆江北国际机场有限公司供应商黑名单。

**六、支付方式**

项目测评完成并提供测评报告经验收合格后15个工作日内支付合同款的100%。

若乙方开具增值税专用发票，则甲方支付不含税合同金额和税额的总金额；若乙方开具增值税普通发票，则甲方仅支付不含税合同金额。如遇税率发生国家法规调整，折算为不含税价后以新适税率结算。

**七、工期时间**

自合同签订之日起 30个日历天。

**八、比选响应有效期**

90天（自比选响应人提交比选响应文件截止之日起计算）。

**九、比选响应文件的编制和提交**

9.1比选响应方应当按照比选采购文件的要求编制比选响应文件，比选响应文件应当对比选采购文件提出的要求和条件作出实质性应答。

9.2比选响应文件应用A4规格纸编制并装订成册，主要由以下几个部分组成：

9.2.1 封面。

9.2.2 加盖公章的报价函及声明（格式按附件1）。

9.2.3报价部分。比选响应方应按照比选采购文件要求报出拟提供服务的单价、总价等详细内容，各项报价应包括拟提供货物的运输、相关税金和服务等全部费用，报价为不含税报价，增值税税率单列。

9.2.4 技术部分。主要包括等级测评的实施方案等。如果提供的方案和服务与比选采购文件要求有偏差，必须详细说明。须经比选小组评定和采购人许可，才能作为供应商实质性响应。(表格自制)

9.2.5 商务部分。营业执照（复印件），法定代表人授权书和法定代表人身份证复印，被授权人身份证复印件（原件备查），网络安全等级测评资质且测评机构能够在公安部中国信息安全等级保护网www.djbh.net推荐目录中查询（提供证明材料复印件），非重庆本地测评机构须提交承诺函（附件4）等。

9.2.6 比选响应文件可合并装订成册，**纸质文件一式3份，其中正本1份，副本2份；电子比选响应文件1份（U盘形式）。**

**十、比选响应文件作废条款**

10.1 未按照规定交纳比选响应保证金的；

10.2 无报价或两个以上报价的；

10.3 报价超过总价最高限价或分项限价；

10.4 比选响应文件未装袋密封的。比选响应文件封面及密封袋封面上须注明“项目名称”、“项目编号”、“比选响应单位名称”，并未加盖单位公章。

10.5 比选响应文件装订要求不符：

10.5.1 散装或者活页装订的；

10.5.2 比选响应文件份数不足或未按要求提供电子U盘的；

10.5.3 比选响应文件封面未标注正副本（密封袋封面无需标注正副本）。

10.6 比选响应文件中报价函部分、授权部分未盖章，或无法定代表人签字（签章），或签字人无有效授权书的。

10.7 报价函部分未按规定的格式完整填写（增项填写不作为作废条款）。

10.8 评审委员会审查发现比选响应文件未能对比选文件提出的所有实质性要求和条件作出响应的。

10.9有串通比选或弄虚作假或有其他违法行为的。

**十一、异议**

11.1 比选响应人或其他利害关系人认为采购活动不符合法律、行政等规定的，应当在采购结果公示期之内以书面形式向采购人提出异议（以采购人收到书面异议之日为准）。

11.2 异议提出人向采购人提起异议时，应当提交异议书。异议书应当包括下列内容：

（一）异议提出人的名称、地址及有效联系方式。

（二）异议事项的基本事实。

（三）异议请求及主张。

（四）有效线索和相关证据、证明材料。

异议提出人是法人的，异议函必须由其法定代表人和委托代理人签字并盖章；异议提出人是其他组织或者自然人的，异议函必须由其主要负责人或者异议提出人本人签字，并附有效身份证明复印件。若异议函有关材料是外文，异议提出人应当同时提供中文译本。

11.3 异议提出人对异议事项提出的请求和主张，有责任提供证据；只有自己陈述而不能提出其他相关证据的，对其请求和主张不予支持。

11.4 异议提出人不得虚假异议、恶意异议，不得以异议为名排挤竞争对手，阻碍采购活动的正常进行。若出现该情况，视为无效异议，不再受理。

11.5 异议提出人不得捏造事实，不得伪造材料或者以非法手段取得证明材料提起异议。异议提出人提供证据存在下列情形之一，不能提供合法证明，或者不能合理说明来源的，视为以非法手段取得证明材料，不予采信：

（一）招标投标法第二十二条规定的招标投标保密信息。

（二）应当保密的采购响应文件（但采购人提起异议时，采购响应文件不作为非法证据）。

（三）招标投标法第四十四条规定保密的投标文件评审和比较情况、中标候选人推荐情况和评标有关的其他情况。

（四）其他依法应当保密的信息和资料。

11.6 有下列情形之一的异议，不予受理：

（一）异议事项不具体，且未提供有效线索、相关证据和证明材料，难以查证。

（二）未署异议提出人真实姓名、签字和有效联系方式。

（三）未经法定代表人或授权的委托代理人签字并加盖公章，或未经主要负责人或异议提出人本人签字。

（四）不在结果公示期内的。

（五）已对异议事项做出答复的。

注：对比选文件内容的异议应在比选文件规定的质疑期内提出；对比选唱价环节的异议应在比选唱价环节提出。

11.7 异议处理决定做出前，异议提出人要求撤回异议的，应当以书面形式提出，撤回异议不损害国家利益、社会公共利益或者其他当事人合法权益的，应当准予撤回，异议处理过程终止。异议提出人不得以同一事实和理由再提出异议，若再次提出则不再受理。

**十二、监督部门**

重庆江北国际机场有限公司综合办公室

地址：重庆江北国际机场有限公司办公楼

电话：023-67157523

**十三、比选时间、地点及结果通知**

13.1 比选响应文件必须在2021年6月29日9:00至10:00时送到重庆江北国际机场有限公司办公楼1013室，过期不予受理。

13.2 2021 年 6月29日10:00时在重庆江北国际机场有限公司（重庆市渝北区机场西路26号重庆江北国际机场有限公司）办公楼对本项目进行比选，各比选响应人须参加。注：比选开始前，各比选响应人须在重庆江北国际机场有限公司102会议室等候通知具体比选地点。

13.3参加比选唱价会议的比选响应人的法定代表人或其授权的代理人应当随身携带本人身份证（原件），授权的代理人还应当随身携带法定代表人授权委托书（原件），以备核验其合法身份。

比选响应人若未派法定代表人或委托代理人出席比选唱价会议，视为该比选响应人默认比选唱价结果。

13.4 比选结果通知：待结果确定后会及时通知，原则上只通知被选中的比选响应人，对未被选中的比选响应人不通知、不解释。

**十四、联系方式**

业主：重庆江北国际机场有限公司

联系人：张女士

电话：67152765

邮编：401120

**附件1：**

**报价函**

重庆江北国际机场有限公司：

1. 我方已仔细研究了 （项目名称）项目比选文件的全部内容，愿意以人民币（大写） 元（¥ ）**不含增值税**专用发票的总报价，增值税税率 %，工期 日历天，按合同约定实施和完成承包项目的全部工作，分项报价如下表所示。

|  |  |  |
| --- | --- | --- |
| **序号** | **系统名称** | **不含税报价(元）** |
| **1** | **重庆机场外网网站** |  |
| **2** | **重庆机场行李管理系统** |  |
| **3** | **重庆机场生产调度系统** |  |
| **4** | **重庆机场大数据平台** |  |
| **5** | **重庆机场离港系统** |  |
| **6** | **合计** |  |

2．我方承诺在比选有效期内不修改、撤销比选响应文件。

3．如我方成交：

（1）我方承诺在收到成交通知后，在规定的期限内与你方签订合同。

（2）随同本报价函递交的报价函附录属于合同文件的组成部分。

（3）我方承诺在合同约定的期限内完成并移交全部合同项目和成果。

4．我方在此声明，所递交的比选响应文件及有关资料内容完整、真实和准确。

5．除非达到另外协议并生效，你方的成交通知书和本比选响应文件将成为约束双方的合同文件组成部分。

比选人：（盖单位公章）

法定代表人或其委托代理人： （签字）

地址：

网址：

电话：

传真：

邮政编码：

年 月 日

**附件2：**

**法定代表人身份证明**

比选响应人名称：

单位性质：

地址：

成立时间： 年 月 日

经营期限：

姓名： 性别： 年龄： 职务：

系 （比选人名称）的法定代表人。

特此证明。

比选人： （盖单位公章）

年 月 日

**附法定代表人身份证复印件**

**附件3：**

**授权委托书（适用于有委托代理人的情况）**

本人\_\_\_\_\_\_\_\_（姓名）系\_\_\_\_\_\_\_\_\_\_\_\_（响应人名称）的法定代表人，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、修改咨询\_\_\_\_\_\_\_\_\_\_\_\_项目响应文件、签订合同和处理有关事宜，其法律后果由我方承担。

委托期限：\_\_\_\_\_\_\_\_。

代理人无转委托权。

注：本授权委托书需由投标人加盖单位鲜公章并由其法定代表人和委托代理人签字。

响应人： （单位鲜公章）

法定代表人： （签字或盖章）

身份证号码：

委托代理人： （签字）

身份证号码：

\_\_\_\_\_\_\_\_年\_\_\_\_月\_\_\_\_日

**附被授权人代理人身份证复印件**

**附件4：**

**承诺函（非重庆本地测评机构提供）**

重庆江北国际机场有限公司：

\_\_\_\_\_\_\_\_\_\_\_\_（响应人名称），若我方成为中标候选人，我方承诺在收到成交通知书后10个工作日内提供重庆市公安局网络安全保卫总队的备案证明材料复印件（原件必查），若无法按时提供，采购人有权要求我方承担相应损失并追究有关法律责任。。

我方对上述承诺负全部法律责任。

响应人： （盖单位公章）

年 月 日

**附件5：**

**重庆机场外网网站、行李管理系统、生产调度系统、大数据平台、离港系统安全等级保护测评项目服务合同**

甲方： 重庆江北国际机场有限公司

乙方：

甲乙双方根据《中华人民共和国民法典》及相关的法律法规之规定，本着友好合作、协商一致的原则，双方就 事宜签订本协议：

**1、释义**

文中“双方”指甲方和乙方，“一方”指甲方和乙方中的任何一方。

文中所涉及费用均以人民币“元”为计量单位。

文中“年、月、日”均指公历年、月、日。

**2、合同内容、方式和要求**

2.1合同内容：重庆机场外网网站、行李管理系统、生产调度系统、大数据平台、离港系统安全等级保护测评服务，依据《信息系统安全等级保护测评要求》、《信息系统安全等级保护测评过程指南》等国际标准进行等级测评服务，具体内容见附件：《重庆机场外网网站安全等级保护测评内容》、《大数据平台安全等级保护测评内容》、《行李管理系统安全等级保护测评内容》、《生产调度系统安全等级保护测评内容》、《离港系统安全等级保护测评内容》。

2.2方式：乙方按照公安部通知制订的《信息系统安全等级测评报告模板》（公信安【2014】2866号）格式出具的测评报告。其形式为 正式测评报告4份（包括安全风险评估、整改建议等, 书面文件4份和测评报告内容电子文件），并有义务协助甲方达到三级信息系统安全标准，提供必要的咨询服务，工作成果全部知识产权永久归甲方所有。

2.3合同期限：合同签订后60日内。

3、合同总额和支付方式

3.1技术服务费总额（不含增值税）为： 元，大写：人民币 ；本合同总价款（含增值税）为： 元，大写：人民币 ，合同总价款包括但不限于税费、人工、保险、利润等，开据增值税专用发票，增值税税率 。

3.2乙方提交正式测评报告经验收合格后15日内，甲方一次性支付合同总价款 元，大写：人民币 ，乙方需开具符合国家规定，税率为 %的全额增值税专用发票给甲方。

若乙方开具增值税专用发票，则甲方支付不含税合同金额和税额的总金额；若乙方开具增值税普通发票，则甲方仅支付不含税合同金额。如遇税率发生国家法规调整，折算为不含税价后以新适税率结算。

3.3乙方账户信息如下：

|  |  |
| --- | --- |
| 开户行 |  |
| 账户名 |  |
| 账号 |  |

**4、甲方义务**

4.1甲方应及时履行本合同中规定的付款义务。

4.2甲方承认，乙方提供信息系统安全测评服务的能力依赖于与甲方之间全面、及时的合作，以及甲方向乙方提供的信息和数据的准确性、全面性。为此，甲方应：

4.2.1在本合同生效之日起10个工作日内，按照乙方的合理要求提供相关信息、数据、资料、设施、工作空间和办公室服务等。

4.2.2指派一名代表，该名代表必需为甲方熟悉被测系统的工作人员和具备相关专业技术知识，负责及时与乙方进行专业联络，并按双方商定的时间，定期与乙方代表进行联系。

**5、乙方义务**

5.1乙方应根据本合同的规定，乙方安排项目经理1名、测试人员2人在合同规定时间内完成本合同约定的信息安全测评服务。

5.2乙方可以根据工作的需要合理安排工作次序和时间，同时有权对各类服务的时间分配作合理调整。

5.3乙方应根据工作清单中约定的工作进度提供测评服务。

5.4乙方必须加强质量和安全管理，如出现因乙方原因的质量和安全问题，乙方应承担相应的经济损失。

5.5在本合同生效并正常履约的情况下，在合同生效后的 30 日，提交测评报告（包括安全风险评估、整改建议等）。

**6、任务变更**

6.1经双方同意，双方可对工作清单中的内容做适当变更或修改。所有变更和修改均须以书面形式进行。

6.2所有任务变更须经双方书面同意。如合同任何一方提出变更任务，在双方就此达成一致前，双方应继续按照未变更合同约定履行其义务。

**7、实施标准**

依据《信息系统安全等级保护测评要求》、《信息系统安全等级保护测评过程指南》等国家标准进行等级测评服务。

**8、验收**

对测评服务的验收总结应于乙方完成工作并通知甲方之日起5日内进行，甲方根据《信息系统安全等级测评报告》中的内容和要求对乙方的工作进行验收。

**9、整改与补救**

因乙方在履行职责时遇到障碍或在执行本合同过程中产生失误，乙方采取必要的补救措施，按本合同规定的标准进行整改与补救。

**10、知识产权和保密**

10.1乙方利用甲方提供的技术资料和工作条件完成的新的技术成果，或者甲方利用乙方交付的工作成果完成的新的技术成果，均属于甲方。

10.2除非另有约定，任何一方均不因本合同的签订取得另一方所拥有的版权、专利、商业秘密、商标或任何其他知识产权。已存在的版权及其他知识产权应属拥有该等权利的一方所有。

10.3如为乙方履行其于本合同项下的义务所必须，甲方可以免费许可乙方使用甲方已有的版权作品或其他知识产权，使乙方以履行本合同义务为目的使用、复制、制作衍生产品、分派、展示、演示和传送。

10.4乙方只能在本合同约定范围内使用甲方提供的信息、技术资料和数据，不能将其用于与本合同无关的目的，或者向与本合同履行无关的第三方披露。

10.5测评工作的成果和结论属甲方所有，乙方对其引用和公开应得到甲方的授权。

10.6甲方如果要引用乙方出具的测评报告，必须完整引用，不得作部分内容引用。若因违背此约束而造成的不良后果，由甲方负责。

10.7甲乙双方应按照《信息安全等级测评保密协议》对双方的保密责任和义务进行约定。

10.8保密期限：遵照法律法规有关知识产权保护的相关规定。

**11、违约责任**

11.1 如果由于甲方原因，包括不限于甲方未按照约定提供相关的信息、数据、资料或办公条件等，影响工作成果的质量，乙方不承担责任，甲方须按照本合同的约定支付报酬。

11.2 任何一方违反本合同约定的保密义务，对方有权要求其支付本合同总价款（不含增值税）的10%的违约金。违约金不足以弥补损失的，还应赔偿对方损失。

11.3如乙方未按合同规定时间完成等级测评工作，每延期一日，乙方应向甲方支付合同总价款（不含增值税）的千分之一的违约金。

**12、合同的变更和解除**

12.1除非遇到不可抗力因素，导致本合同不能履行，未经甲乙双方一致书面同意，任何单方无权变更合同的内容。

12.2对本合同的任何修改或补充，只有在双方授权的代表签字后生效，并成为本合同不可分割的组成部分，与本合同具有同等法律效力。

12.3如本合同任何一方严重违反合同，另一方应及时向违约方发出书面纠正通知，违约方应于收到书面纠正通知之日起30日内纠正违约行为，否则守约方有权解除合同并要求违约方赔偿因解除合同而造成的经济损失。

12.4本合同任何一方破产、解散，本合同自动终止。

**13、不可抗力**

13.1甲乙双方任何一方由于不可抗力事件的影响而不能执行协议时，履行协议的期限应予以延长，其延长的期限应相当于事件所影响的时间。不可抗力事件系指买卖双方在缔结协议时所不能预见的，并且它的发生及其后果是无法避免和无法克服的事件，诸如战争、严重火灾、洪水、台风、地震政府政策调整等。

13.2受阻一方应在不可抗力事件发生后尽快用电报、传真或电传通知对方，并于事件发生后14日内将有关当局出具的证明文件用特快专递或挂号信寄给对方确认。

**14、通知**

14.1本合同中任何通知必须为书面形式。注：以传真、电报通知的必须同时以挂号及特快专递再行通知。

**15、争议解决和适用法律**

15.1与本合同有关的或因执行本合同所产生之争议，应由双方友好协商解决，不能解决时，任何一方均可向甲方所在地人民法院提起诉讼。

15.2争议处理期间除正在审理的部分以外，双方应继续执行合同的其余部分。

15.3本合同的订立、效力、解释、履行及争议的解决适用中华人民共和国的法律、法规。

**16、其他**

16.1本合同未尽事宜，应由甲、乙双方协商后以书面形式补充，加盖甲、乙双方公司印章或合同专用章后并经双方授权代表签字后生效。

16.2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。

16.3本合同自甲、乙双方加盖公司印章或合同专用章，并经双方法人授权代表签字后生效。

**17、附件**

17.1附件：《信息安全等级测评保密协议》

17.2附件：《现场测评授权书》

17.3附件：《重庆机场外网网站安全等级保护测评内容》、《大数据平台安全等级保护测评内容》、《行李管理系统安全等级保护测评内容》、《生产调度系统安全等级保护测评内容》、《离港系统安全等级保护测评内容》

甲方： 重庆江北国际机场有限公司

乙方：

（盖章） （盖章）

授权代表人（签字）： 授权代表人（签字）：

日期： 年 月 日 日期： 年 月 日

**信息安全等级测评保密协议**

甲 方: 重庆江北国际机场有限公司

乙 方：

为了保护甲乙双方在商业和技术合作中涉及的专有信息（如本协议第一款所定义的内容），经友好协商，甲乙双方签订如下协议：

乙方将遵照《信息系统安全等级测评委托协议书》完成重庆机场集团有限公司等级测评工作，经双方协商一致，为确保相应工作涉及的技术信息和技术资源不被泄露，并防止上述保密信息被滥用，甲乙双方达成如下协议：

乙方作为等级测评机构，其工作任务仅限于信息系统安全等级测评，本协议仅涉及乙方承担该项工作过程中及以后的保密责任。

本协议涉及密保的技术信息和技术资料包括：

《信息系统安全等级测评委托协议书》中涉及的技术信息和技术资料，以及有关会议文件和决定；

甲、乙双方之间工作往来的传真、信函、电子邮件等；

等级测评工作实施过程中产生的技术信息和技术资料；

等级测评工作实施过程中各有关当事人拥有的知识产权，已经公开的知识产权信息除外；

经甲、乙双方在等级测评工作实施过程中确认的需要保密的其他信息；

甲方责任

1、甲方应根据《信息系统安全等级测评委托协议书》的规定，向乙方提供必要的技术信息和技术资料；

2、甲方在以书面形式（包括：邮件、传真、光盘等）向乙方提供技术信息时，可以进行登记或备案；

3、甲方对乙方提供的注明保密的技术信息和资料负有保密责任，未经乙方同意不得提供给无关的任何第三方；

乙方责任

1、乙方应仅将甲方批露的保密信息只用于对甲方的等级测评工作中；

2、乙方对从甲方获得的涉及等级测评工作的技术信息和技术资料负有保密责任，未经甲方同意不得提供给任何第三方，包括乙方的分支机构，子公司或委托顾问方，接受咨询方；

3、乙方为承担本协议约定的保密责任，应妥善保管有关的文件和资料，未经工作组事先的书面许可，不对其复制，仿造等；

乙方应对有关人员进行有效管理，以确保本协议的履行；

在本协议约定的保密期限内，乙方如发现有关保密信息被泄露，应及时通知甲方，并采取积极的措施避免损失的扩大；

本协议中涉及的有关保密信息，其中已经拥有知识产权的归原所有人所有。

甲方为了等级测评工作的需要，除乙方特别声明不能提供给他人的以外，可以将乙方提供的有关信息向等级测评工作的有关方面（包括：上级管理单位、等级保护相关的管理部门）提供，此行为不视为甲方、乙方违约。

乙方在实施等级测评工作过程中，需要向等级测评工作的其他有关方面（等级保护相关的管理部门除外）提供保密信息时，必须取得甲方的书面许可，或者由甲方负责提供。

甲方违反本协议的约定均视为甲方违约。

违反本协议的约定，由违约方承担相应责任，并赔偿由此产生的一切损失。

本协议要求双方承担保密义务的期限为，自本协议签字之日或者自双方中的一方取得有关文件，资料之日起，以时间在前为准，至等级测评工作完成之日止。如在等级测评工作实施过程中，乙方提前退出本项目，双方应在终止《信息系统安全等级测评委托协议书》后的五年内继续履行有关保密责任。

双方在履行协议中产生的纠纷，应通过友好协商解决。如协商不成，提请重庆市仲裁委员会仲裁。

**现场测评授权书**

兹有重庆江北国际机场有限公司与 友好协商,特授权对 实施等保测评服务。

重庆江北国际机场有限公司 年 月 日

**附件：**

**重庆机场外网网站安全等级保护测评内容**

“重庆机场重庆机场外网网站”是重庆江北国际机场限公司的重要信息系统，为了提升系统的安全保护能力，加强信息安全管理，根据《网络安全等级保护管理办法》、《网络安全技术信息系统安全等级保护基本要求》等法规和标准的要求，需要进行相应的等级测评工作。“重庆机场外网网站”按照最新的等级保护三级要求进行等级测评。通过测评，准确反映以上信息系统的安全防护能力现状，对发现的问题进行深入分析，提出安全整改建议，最终出具信息系统等级保护测评报告。

一、测评系统基本情况

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 被测信息系统 | 安全保护等级 | 网络及设备 | 主机设备情况 | 系统架构 |
| 重庆机场外网网站 | 3 | 内部网络1  网络设备：若干  安全设备：若干 | 服务器：无  终端：无 | B/S |

二、测评主要流程

测评分预测评和回归测试，预测评提供差距分析报告和整改建议方案，指导采购人完成三级等保安全整改。完成整改后进行不符合项回归性测试，出具最终测评报告。

三、测评内容

（一）测评范围主要包括：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等方面。

（二）测评质量保证：测评中应严格按照GB/T 28449-2018《信息系统安全等级保护测评过程指南》标准的要求实施，加强质量监督和复查，保证测评工作质量。

技术测评：

（1）安全物理环境测评（物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护）；

（2）安全通信网络测评（网络架构、通信传输、可信验证）；

（3）安全区域边界测评（边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证）；

（4）安全计算环境测评（身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护）；

（5）安全管理中心测评（系统管理、审计管理、安全管理、集中管控）。

管理测评：

（1）安全管理制度测评（安全策略、管理制度、制定和发布、评审和修订）；

（2）安全管理机构测评（岗位设置、人员配备、授权和审批、沟通和合作、审核和检查）；

（3）安全管理人员测评（人员录用、人员离岗、安全意识教育和培训、外部人员访问管理）；

（4）安全建设管理测评（定级和备案、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统支付、等级测评、服务供应商选择）；

（5）安全运维管理测评（环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理、外包运维管理）。

云计算扩展测评：

（1）安全物理环境测评（基础设施位置）；

（2）安全通信网络测评（网络架构）；

（3）安全区域边界测评（访问控制、入侵防范、安全审计）；

（4）安全计算环境测评（身份鉴别、访问控制、入侵防范、镜像和快照保护、数据完整性和保密性、数据备份恢复、剩余信息保护）；

（5）安全管理中心测评（集中管控）；

（6）安全建设管理测评（云服务商选择、供应链管理）；

（7）安全运维管理测评（云计算环境管理）。

移动互联扩展测评：

（1）安全物理环境测评（无线接入点的物理位置）；

（2）安全区域边界测评（边界防护、访问控制、入侵防范）；

（3）安全计算环境测评（移动终端管控、移动应用管控）；

（4）安全建设管理测评（移动应用软件采购、移动应用软件开发）；

（5）安全运维管理测评（配置管理）。

物联网扩展测评：

（1）安全物理环境测评（感知节点设备物理防护）；

（2）安全区域边界测评（接入控制、入侵防范）；

（3）安全计算环境测评（感知节点设备安全、网关节点设备安全、抗数据重放、数据融合处理）；

（4）安全运维管理测评（感知节点管理）。

工业控制系统扩展测评：

（1）安全物理环境测评（室外控制设备物理防护）；

（2）安全通信网络（网络架构、通信传输）

（3）安全区域边界测评（访问控制、拨号使用控制、无线使用控制）；

（4）安全计算环境测评（控制设备安全）；

（5）安全建设管理测评（产品采购和使用、外包软件开发）。

四、实施要求：

（一）供应商必须承诺对本项目技术文件以及由用户提供的所有内部资料、技术文档和信息予以保密。

（二）供应商应加强本项目资料的保密管控，必须针对本项目建立项目纸质、声音、影像、图像、电子等各种形态资料及其载体的保密管控措施，记录资料由生成到销毁整个生命周期内的使用日志，并根据实际工作情况及时对制度进行调整。供应商应加强本项目在用户工作场所使用设备，特别是笔记本电脑、移动存储介质等便携设备使用的保密管理。接入系统网络内使用的设备，必须遵守该系统关于终端安全管理、移动存储介质管理等要求。

（三）供应商为用户提供信息安全规划、方针、策略和管理制度体系咨询服务，配合用户，为被测信息系统安全整改和加固提供咨询和技术服务。

（四）测评过程中，应针对关键设备、重点网段和高危漏洞进行渗透测试，形成相应的实施和分析报告。

（五）依据《网络安全等级保护测评机构管理办法》相关规定：“属于异地测评项目的，测评机构应从项目管理系统中生成测评项目基本情况表，并于测评项目实施前报送或传至被测评网络备案公安机关”。属于异地测评项目的,成交供应商应在合同签订前提交审核通过的《测评项目基本情况表》。如出现不能按时提交或备案不通过的，视为成交供应商不具备签订合同的基本条件，采购人有权按评审排名依序顺延。

**大数据平台安全等级保护测评内容**

“重庆机场大数据信息平台”是重庆江北国际机场限公司的重要信息系统，为了提升系统的安全保护能力，加强信息安全管理，根据《网络安全等级保护管理办法》、《网络安全技术信息系统安全等级保护基本要求》等法规和标准的要求，需要进行相应的等级测评工作。“重庆机场大数据信息平台”按照最新的等级保护三级要求进行等级测评。通过测评，准确反映以上信息系统的安全防护能力现状，对发现的问题进行深入分析，提出安全整改建议，最终出具信息系统等级保护测评报告。

一、测评系统基本情况

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 被测信息系统 | 安全保护等级 | 网络及设备 | 主机设备情况 | 系统架构 |
| 大数据信息平台 | 3 | 内部网络1  网络设备：若干  安全设备：若干 | 服务器：6余台  终端：无 | B/S |

二、测评主要流程

测评分预测评和回归测试，预测评提供差距分析报告和整改建议方案，指导采购人完成三级等保安全整改。完成整改后进行不符合项回归性测试，出具最终测评报告。

三、测评内容

（一）测评范围主要包括：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等方面。

（二）测评质量保证：测评中应严格按照GB/T 28449-2018《信息系统安全等级保护测评过程指南》标准的要求实施，加强质量监督和复查，保证测评工作质量。

技术测评：

（1）安全物理环境测评（物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护）；

（2）安全通信网络测评（网络架构、通信传输、可信验证）；

（3）安全区域边界测评（边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证）；

（4）安全计算环境测评（身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护）；

（5）安全管理中心测评（系统管理、审计管理、安全管理、集中管控）。

管理测评：

（1）安全管理制度测评（安全策略、管理制度、制定和发布、评审和修订）；

（2）安全管理机构测评（岗位设置、人员配备、授权和审批、沟通和合作、审核和检查）；

（3）安全管理人员测评（人员录用、人员离岗、安全意识教育和培训、外部人员访问管理）；

（4）安全建设管理测评（定级和备案、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统支付、等级测评、服务供应商选择）；

（5）安全运维管理测评（环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理、外包运维管理）。

云计算扩展测评：

（1）安全物理环境测评（基础设施位置）；

（2）安全通信网络测评（网络架构）；

（3）安全区域边界测评（访问控制、入侵防范、安全审计）；

（4）安全计算环境测评（身份鉴别、访问控制、入侵防范、镜像和快照保护、数据完整性和保密性、数据备份恢复、剩余信息保护）；

（5）安全管理中心测评（集中管控）；

（6）安全建设管理测评（云服务商选择、供应链管理）；

（7）安全运维管理测评（云计算环境管理）。

移动互联扩展测评：

（1）安全物理环境测评（无线接入点的物理位置）；

（2）安全区域边界测评（边界防护、访问控制、入侵防范）；

（3）安全计算环境测评（移动终端管控、移动应用管控）；

（4）安全建设管理测评（移动应用软件采购、移动应用软件开发）；

（5）安全运维管理测评（配置管理）。

物联网扩展测评：

（1）安全物理环境测评（感知节点设备物理防护）；

（2）安全区域边界测评（接入控制、入侵防范）；

（3）安全计算环境测评（感知节点设备安全、网关节点设备安全、抗数据重放、数据融合处理）；

（4）安全运维管理测评（感知节点管理）。

工业控制系统扩展测评：

（1）安全物理环境测评（室外控制设备物理防护）；

（2）安全通信网络（网络架构、通信传输）

（3）安全区域边界测评（访问控制、拨号使用控制、无线使用控制）；

（4）安全计算环境测评（控制设备安全）；

（5）安全建设管理测评（产品采购和使用、外包软件开发）。

四、实施要求：

（一）供应商必须承诺对本项目技术文件以及由用户提供的所有内部资料、技术文档和信息予以保密。

（二）供应商应加强本项目资料的保密管控，必须针对本项目建立项目纸质、声音、影像、图像、电子等各种形态资料及其载体的保密管控措施，记录资料由生成到销毁整个生命周期内的使用日志，并根据实际工作情况及时对制度进行调整。供应商应加强本项目在用户工作场所使用设备，特别是笔记本电脑、移动存储介质等便携设备使用的保密管理。接入系统网络内使用的设备，必须遵守该系统关于终端安全管理、移动存储介质管理等要求。

（三）供应商为用户提供信息安全规划、方针、策略和管理制度体系咨询服务，配合用户，为被测信息系统安全整改和加固提供咨询和技术服务。

（四）测评过程中，应针对关键设备、重点网段和高危漏洞进行渗透测试，形成相应的实施和分析报告。

（五）依据《网络安全等级保护测评机构管理办法》相关规定：“属于异地测评项目的，测评机构应从项目管理系统中生成测评项目基本情况表，并于测评项目实施前报送或传至被测评网络备案公安机关”。属于异地测评项目的,成交供应商应在合同签订前提交审核通过的《测评项目基本情况表》。如出现不能按时提交或备案不通过的，视为成交供应商不具备签订合同的基本条件，采购人有权按评审排名依序顺延。

**行李管理系统安全等级保护测评内容**

“重庆机场行李系统”是重庆江北国际机场限公司的重要信息系统，为了提升系统的安全保护能力，加强信息安全管理，根据《网络安全等级保护管理办法》、《网络安全技术信息系统安全等级保护基本要求》等法规和标准的要求，需要进行相应的等级测评工作。重庆机场“行李系统”按照最新的等级保护三级要求进行等级测评。通过测评，准确反映以上信息系统的安全防护能力现状，对发现的问题进行深入分析，提出安全整改建议，最终出具信息系统等级保护测评报告。

一、测评系统基本情况

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 被测信息系统 | 安全保护等级 | 网络及设备 | 主机设备情况 | 系统架构 |
| 行李系统 | 3 | 内部网络1  网络设备：49  安全设备：2 | 服务器：33台  终端：22台 | B/S |

二、测评主要流程

测评分预测评和回归测试，预测评提供差距分析报告和整改建议方案，指导采购人完成三级等保安全整改。完成整改后进行不符合项回归性测试，出具最终测评报告。

三、测评内容

（一）测评范围主要包括：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等方面。

（二）测评质量保证：测评中应严格按照GB/T 28449-2018《信息系统安全等级保护测评过程指南》标准的要求实施，加强质量监督和复查，保证测评工作质量。

技术测评：

（1）安全物理环境测评（物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护）；

（2）安全通信网络测评（网络架构、通信传输、可信验证）；

（3）安全区域边界测评（边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证）；

（4）安全计算环境测评（身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护）；

（5）安全管理中心测评（系统管理、审计管理、安全管理、集中管控）。

管理测评：

（1）安全管理制度测评（安全策略、管理制度、制定和发布、评审和修订）；

（2）安全管理机构测评（岗位设置、人员配备、授权和审批、沟通和合作、审核和检查）；

（3）安全管理人员测评（人员录用、人员离岗、安全意识教育和培训、外部人员访问管理）；

（4）安全建设管理测评（定级和备案、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统支付、等级测评、服务供应商选择）；

（5）安全运维管理测评（环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理、外包运维管理）。

云计算扩展测评：

（1）安全物理环境测评（基础设施位置）；

（2）安全通信网络测评（网络架构）；

（3）安全区域边界测评（访问控制、入侵防范、安全审计）；

（4）安全计算环境测评（身份鉴别、访问控制、入侵防范、镜像和快照保护、数据完整性和保密性、数据备份恢复、剩余信息保护）；

（5）安全管理中心测评（集中管控）；

（6）安全建设管理测评（云服务商选择、供应链管理）；

（7）安全运维管理测评（云计算环境管理）。

移动互联扩展测评：

（1）安全物理环境测评（无线接入点的物理位置）；

（2）安全区域边界测评（边界防护、访问控制、入侵防范）；

（3）安全计算环境测评（移动终端管控、移动应用管控）；

（4）安全建设管理测评（移动应用软件采购、移动应用软件开发）；

（5）安全运维管理测评（配置管理）。

物联网扩展测评：

（1）安全物理环境测评（感知节点设备物理防护）；

（2）安全区域边界测评（接入控制、入侵防范）；

（3）安全计算环境测评（感知节点设备安全、网关节点设备安全、抗数据重放、数据融合处理）；

（4）安全运维管理测评（感知节点管理）。

工业控制系统扩展测评：

（1）安全物理环境测评（室外控制设备物理防护）；

（2）安全通信网络（网络架构、通信传输）

（3）安全区域边界测评（访问控制、拨号使用控制、无线使用控制）；

（4）安全计算环境测评（控制设备安全）；

（5）安全建设管理测评（产品采购和使用、外包软件开发）。

四、实施要求：

（一）供应商必须承诺对本项目技术文件以及由用户提供的所有内部资料、技术文档和信息予以保密。

（二）供应商应加强本项目资料的保密管控，必须针对本项目建立项目纸质、声音、影像、图像、电子等各种形态资料及其载体的保密管控措施，记录资料由生成到销毁整个生命周期内的使用日志，并根据实际工作情况及时对制度进行调整。供应商应加强本项目在用户工作场所使用设备，特别是笔记本电脑、移动存储介质等便携设备使用的保密管理。接入系统网络内使用的设备，必须遵守该系统关于终端安全管理、移动存储介质管理等要求。

（三）供应商为用户提供信息安全规划、方针、策略和管理制度体系咨询服务，配合用户，为被测信息系统安全整改和加固提供咨询和技术服务。

（四）测评过程中，应针对关键设备、重点网段和高危漏洞进行渗透测试，形成相应的实施和分析报告。

（五）依据《网络安全等级保护测评机构管理办法》相关规定：“属于异地测评项目的，测评机构应从项目管理系统中生成测评项目基本情况表，并于测评项目实施前报送或传至被测评网络备案公安机关”。属于异地测评项目的,成交供应商应在合同签订前提交审核通过的《测评项目基本情况表》。如出现不能按时提交或备案不通过的，视为成交供应商不具备签订合同的基本条件，采购人有权按评审排名依序顺延。

**生产调度系统安全等级保护测评内容**

“重庆机场生产调度系统”是重庆江北国际机场限公司的重要信息系统，为了提升系统的安全保护能力，加强信息安全管理，根据《网络安全等级保护管理办法》、《网络安全技术信息系统安全等级保护基本要求》等法规和标准的要求，需要进行相应的等级测评工作。“重庆机场生产调度系统”按照最新的等级保护三级要求进行等级测评。通过测评，准确反映以上信息系统的安全防护能力现状，对发现的问题进行深入分析，提出安全整改建议，最终出具信息系统等级保护测评报告。

一、测评系统基本情况

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 被测信息系统 | 安全保护等级 | 网络及设备 | 主机设备情况 | 系统架构 |
| 重庆机场生产调度系统 | 3 | 内部网络1  网络设备：若干  安全设备：若干 | 服务器：24  终端：若干 | B/S |

二、测评主要流程

测评分预测评和回归测试，预测评提供差距分析报告和整改建议方案，指导采购人完成三级等保安全整改。完成整改后进行不符合项回归性测试，出具最终测评报告。

三、测评内容

（一）测评范围主要包括：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等方面。

（二）测评质量保证：测评中应严格按照GB/T 28449-2018《信息系统安全等级保护测评过程指南》标准的要求实施，加强质量监督和复查，保证测评工作质量。

技术测评：

（1）安全物理环境测评（物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护）；

（2）安全通信网络测评（网络架构、通信传输、可信验证）；

（3）安全区域边界测评（边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证）；

（4）安全计算环境测评（身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护）；

（5）安全管理中心测评（系统管理、审计管理、安全管理、集中管控）。

管理测评：

（1）安全管理制度测评（安全策略、管理制度、制定和发布、评审和修订）；

（2）安全管理机构测评（岗位设置、人员配备、授权和审批、沟通和合作、审核和检查）；

（3）安全管理人员测评（人员录用、人员离岗、安全意识教育和培训、外部人员访问管理）；

（4）安全建设管理测评（定级和备案、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统支付、等级测评、服务供应商选择）；

（5）安全运维管理测评（环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理、外包运维管理）。

云计算扩展测评：

（1）安全物理环境测评（基础设施位置）；

（2）安全通信网络测评（网络架构）；

（3）安全区域边界测评（访问控制、入侵防范、安全审计）；

（4）安全计算环境测评（身份鉴别、访问控制、入侵防范、镜像和快照保护、数据完整性和保密性、数据备份恢复、剩余信息保护）；

（5）安全管理中心测评（集中管控）；

（6）安全建设管理测评（云服务商选择、供应链管理）；

（7）安全运维管理测评（云计算环境管理）。

移动互联扩展测评：

（1）安全物理环境测评（无线接入点的物理位置）；

（2）安全区域边界测评（边界防护、访问控制、入侵防范）；

（3）安全计算环境测评（移动终端管控、移动应用管控）；

（4）安全建设管理测评（移动应用软件采购、移动应用软件开发）；

（5）安全运维管理测评（配置管理）。

物联网扩展测评：

（1）安全物理环境测评（感知节点设备物理防护）；

（2）安全区域边界测评（接入控制、入侵防范）；

（3）安全计算环境测评（感知节点设备安全、网关节点设备安全、抗数据重放、数据融合处理）；

（4）安全运维管理测评（感知节点管理）。

工业控制系统扩展测评：

（1）安全物理环境测评（室外控制设备物理防护）；

（2）安全通信网络（网络架构、通信传输）

（3）安全区域边界测评（访问控制、拨号使用控制、无线使用控制）；

（4）安全计算环境测评（控制设备安全）；

（5）安全建设管理测评（产品采购和使用、外包软件开发）。

四、实施要求：

（一）供应商必须承诺对本项目技术文件以及由用户提供的所有内部资料、技术文档和信息予以保密。

（二）供应商应加强本项目资料的保密管控，必须针对本项目建立项目纸质、声音、影像、图像、电子等各种形态资料及其载体的保密管控措施，记录资料由生成到销毁整个生命周期内的使用日志，并根据实际工作情况及时对制度进行调整。供应商应加强本项目在用户工作场所使用设备，特别是笔记本电脑、移动存储介质等便携设备使用的保密管理。接入系统网络内使用的设备，必须遵守该系统关于终端安全管理、移动存储介质管理等要求。

（三）供应商为用户提供信息安全规划、方针、策略和管理制度体系咨询服务，配合用户，为被测信息系统安全整改和加固提供咨询和技术服务。

（四）测评过程中，应针对关键设备、重点网段和高危漏洞进行渗透测试，形成相应的实施和分析报告。

（五）依据《网络安全等级保护测评机构管理办法》相关规定：“属于异地测评项目的，测评机构应从项目管理系统中生成测评项目基本情况表，并于测评项目实施前报送或传至被测评网络备案公安机关”。属于异地测评项目的,成交供应商应在合同签订前提交审核通过的《测评项目基本情况表》。如出现不能按时提交或备案不通过的，视为成交供应商不具备签订合同的基本条件，采购人有权按评审排名依序顺延。

**离港系统安全等级保护测评内容**

“重庆机场离港系统”是重庆江北国际机场限公司的重要信息系统，为了提升系统的安全保护能力，加强信息安全管理，根据《信息安全等级保护管理办法》、《信息安全技术网络安全等级保护基本要求》等法规和标准的要求，需要进行相应的等级测评工作。“重庆机场离港系统”按照最新的等级保护三级要求进行等级测评。通过测评，准确反映以上信息系统的安全防护能力现状，对发现的问题进行深入分析，提出安全整改建议，最终出具信息系统等级保护测评报告。

一、测评系统基本情况

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 被测信息系统 | 安全保护等级 | 网络及设备 | 主机设备情况 | 系统架构 |
| 离港系统 | 3 | 内部网络1  网络设备：若干  安全设备：若干 | 服务器：18余台  终端：约695台 | C/S |

二、测评主要流程

测评分预测评和回归测试，预测评提供差距分析报告和整改建议方案，指导采购人完成三级等保安全整改。完成整改后进行不符合项回归性测试，出具最终测评报告。

三、测评内容

（一）测评范围主要包括：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等方面。

（二）测评质量保证：测评中应严格按照GB/T 28449-2018《信息系统安全等级保护测评过程指南》标准的要求实施，加强质量监督和复查，保证测评工作质量。

技术测评：

（1）安全物理环境测评（物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护）；

（2）安全通信网络测评（网络架构、通信传输、可信验证）；

（3）安全区域边界测评（边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证）；

（4）安全计算环境测评（身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护）；

（5）安全管理中心测评（系统管理、审计管理、安全管理、集中管控）。

管理测评：

（1）安全管理制度测评（安全策略、管理制度、制定和发布、评审和修订）；

（2）安全管理机构测评（岗位设置、人员配备、授权和审批、沟通和合作、审核和检查）；

（3）安全管理人员测评（人员录用、人员离岗、安全意识教育和培训、外部人员访问管理）；

（4）安全建设管理测评（定级和备案、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统支付、等级测评、服务供应商选择）；

（5）安全运维管理测评（环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理、外包运维管理）。

云计算扩展测评：

（1）安全物理环境测评（基础设施位置）；

（2）安全通信网络测评（网络架构）；

（3）安全区域边界测评（访问控制、入侵防范、安全审计）；

（4）安全计算环境测评（身份鉴别、访问控制、入侵防范、镜像和快照保护、数据完整性和保密性、数据备份恢复、剩余信息保护）；

（5）安全管理中心测评（集中管控）；

（6）安全建设管理测评（云服务商选择、供应链管理）；

（7）安全运维管理测评（云计算环境管理）。

移动互联扩展测评：

（1）安全物理环境测评（无线接入点的物理位置）；

（2）安全区域边界测评（边界防护、访问控制、入侵防范）；

（3）安全计算环境测评（移动终端管控、移动应用管控）；

（4）安全建设管理测评（移动应用软件采购、移动应用软件开发）；

（5）安全运维管理测评（配置管理）。

物联网扩展测评：

（1）安全物理环境测评（感知节点设备物理防护）；

（2）安全区域边界测评（接入控制、入侵防范）；

（3）安全计算环境测评（感知节点设备安全、网关节点设备安全、抗数据重放、数据融合处理）；

（4）安全运维管理测评（感知节点管理）。

工业控制系统扩展测评：

（1）安全物理环境测评（室外控制设备物理防护）；

（2）安全通信网络（网络架构、通信传输）

（3）安全区域边界测评（访问控制、拨号使用控制、无线使用控制）；

（4）安全计算环境测评（控制设备安全）；

（5）安全建设管理测评（产品采购和使用、外包软件开发）。

四、实施要求：

（一）供应商必须承诺对本项目技术文件以及由用户提供的所有内部资料、技术文档和信息予以保密。

（二）供应商应加强本项目资料的保密管控，必须针对本项目建立项目纸质、声音、影像、图像、电子等各种形态资料及其载体的保密管控措施，记录资料由生成到销毁整个生命周期内的使用日志，并根据实际工作情况及时对制度进行调整。供应商应加强本项目在用户工作场所使用设备，特别是笔记本电脑、移动存储介质等便携设备使用的保密管理。接入系统网络内使用的设备，必须遵守该系统关于终端安全管理、移动存储介质管理等要求。

（三）供应商为用户提供信息安全规划、方针、策略和管理制度体系咨询服务，配合用户，为被测信息系统安全整改和加固提供咨询和技术服务。

（四）测评过程中，应针对关键设备、重点网段和高危漏洞进行渗透测试，形成相应的实施和分析报告。

（五）依据《网络安全等级保护测评机构管理办法》相关规定：“属于异地测评项目的，测评机构应从项目管理系统中生成测评项目基本情况表，并于测评项目实施前报送或传至被测评网络备案公安机关”。属于异地测评项目的,成交供应商应在合同签订前提交审核通过的《测评项目基本情况表》。如出现不能按时提交或备案不通过的，视为成交供应商不具备签订合同的基本条件，采购人有权按评审排名依序顺延。