广东省机场管理集团有限公司
信息安全服务项目

采购文件

采购方：广东省机场管理集团有限公司

2023 年 4 月

总　目　录

第一部分

邀 请 函

第一部分　邀请函

广东省机场管理集团有限公司（以下简称“采购方”）就信息安全服务项目进行国内公开采购，现邀请合格的供应商（以下简称“供应商”）提交密封报价文件。

1、 项目概况：

1.1 项目名称：信息安全服务项目。

1.2 项目地点：广州市。

1.3 项目内容：广东省机场管理集团有限公司信息安全服务。

1.4 资金来源：企业自筹资金。

2、 采购内容：

2.1 采购内容及限价

序号	服务内容	采购最高限价
1	广东省机场管理集团有限公司信息安全服务	人民币：壹佰贰拾万元

注：供应商必须对全部服务内容进行报价，报价包含所有税费。

2.2 服务内容

序号	服务目录	服务内容	服务对象	频率	单位	备注
1	安全托管服务	详见服务要求	集团云数据中心涉及到的资产	1	年	
2	漏洞扫描服务	详见服务要求	机场集团云数据中心涉及到的资产或指定的	12	次 / 年	
3	安全加固服务	详见服务要求	机场集团云数据中心涉及到的资产	1	年	
4	安全评估服务	详见服务要求	机场集团云数据中心涉及到的资产	1	次	
5	安全培训服务	详见服务要求	机场集团	3	次 / 年	
6	重保值守服务	详见服务要求	机场集团	3	次 / 年	
7	应急响应服务	详见服务要求	机场集团	1	年	

8	渗透测试服务	详见服务要求	机场集团	12	系统	
9	新上线系统评估	详见服务要求	机场集团	12	系统	
10	抽检服务	详见服务要求	机场集团	6	次/年	
11	安全巡检服务	详见服务要求	机场集团	4	次/年	
12	驻场服务	详见服务要求	机场集团	1	次/年	

3、 合格供应商资格条件（须对此项内容提供承诺函并加盖公章或电子签章）.：

3.1.供应商必须为具备本项目履约能力的在中华人民共和国境内注册的独立的企业法人，同时持有工商行政管理部门核发的营业执照，提供营业执照的复印件并加盖公章或电子签章。

3.2.供应商不得被列入国家企业信用信息公示系统的经营异常名录或严重违法失信企业名单，以“国家企业信用信息公示系统”网站（www.gsxt.gov.cn）查询为准，供应商需从“国家企业信用信息公示系统”网站截图并加盖公章或电子签章（未按格式要求截图或截图信息不清晰将作废标处理）。

3.3.供应商不得被列为“严重失信主体名单”，以“信用中国”网站（www.creditchina.gov.cn）查询为准，供应商需按采购文件给定的格式要求从“信用中国”网站截图并加盖公章（未按格式要求截图或截图信息不清晰将作废标处理）。

3.4.具有履行合同所必需的专业技术能力；

3.5.本项目不接受联合体报价。

3.6.已登记为本项目供应商。

3.7.供应商不得存在以下情形：

3.7.1 与采购人、采购人及其关联公司在本公告发布之日起前三年内发生各种诉讼和仲裁

3.7.2 供应商、法定代表人及项目负责人被列入广东省机场管理集团有限公司不予合作对象名单且在限制期内。

3.7.3 供应商、法定代表人及项目负责人存在国家、省市相关法律法规和行业有关规定不得参与采购活动的情形。

3.7.4 在本公告发布之日起前三年内，供应商因腐败或欺诈行为而被政府或业主宣布取消

报价资格

3.7.5 存在其它失信情况的。

3.8.供应商应对采购人以下“合作商不诚信行为”的确定条件进行响应，并提供承诺书：

3.8.1 参与本项目的供应商，有下列情形之一的，将被列入采购人不予合作对象名单：

3.8.1.1 通过向采购人提供不正当利益谋取成交；

3.8.1.2 借用他人名称、资质进行挂靠，或者将自己的名称、资质借给他人挂靠进行报价，或以其他方式弄虚作假，骗取成交；

3.8.1.3 采取不正当手段诋毁、排挤其他合作对象；

3.8.1.4 在采购过程与采购人相关工作人员私下进行协商谈判，损害采购人或其他供应商利益；

3.8.1.5 针对资格审查文件、采购文件或者在资格预审公示或成交候选人公示期间，故意捏造事实、伪造证明材料，恶意进行质疑，影响采购工作顺利推进；

3.8.1.6 存在围标串标行为；

3.8.1.7 采购人成交通知书发出后，报名人拒绝签订合同（因不可抗力原因不能履行合同的除外）；

3.8.1.8 自采购公告发布之日起前三年内与采购人以及关联公司发生诉讼或仲裁的供应商；

3.8.1.9 发生向采购人及其关联公司的有关工作人员行贿情形；

3.8.1.10 参与采购人非招标采购活动进行两次（含）以上无效异议的合作对象，因其无效异议对采购人以及关联公司造成经济损失、工作滞后的，可纳入非招标采购项目不予合作名单。具有下列情形之一的，应视为无效异议：

——异议主体不是供应商或其他利害关系人；

——供应商是法人的，异议书必须由其法定代表人或者授权代表签字并盖章；其他组织或者自然人投诉的，异议书必须由其主要负责人或者投诉人本人签字，并附有效身份证明复印件；

——异议人未提供必要的证明材料和明确的要求；

——异议人捏造事实、伪造材料或者以非法手段取得证明材料进行异议的，证据来源的合法性存在明显疑问，异议人无法证明其取得方式合法的，视为以非法手段取得证明材料；

——其他属无效异议的情形。

3.8.2 成交供应商在合同履行，项目实施、运行阶段，有下列情形之一的，列入不予合作对象名单：

3.8.2.1 不按采购文件要求，报价文件承诺的条件与采购人签订合同，或在合同签订中存在欺诈情形，违反采购文件规定，对采购人或关联公司不利；

3.8.2.2 违反合同约定，将承揽项目转包或违法分包给他人；

3.8.2.3 因成交供应商责任原因连续发生不安全事件、事故或造成恶劣不良影响；

3.8.2.4 使用的设备、材料以次充好或提供与合同不符的假冒伪劣产品等降低质量情形或造成不良影响；

3.8.2.5 因环保、噪音问题造成社会恶劣影响；

3.8.2.6 拖欠农民工工资，造成恶劣影响的，或发生上访维稳事件，或导致采购人或关联公司垫付农民工工资；

3.8.2.7 虚报工程量或设备、材料结算量，拒不接受第三方咨询单位按合同约定审定的工程造价，设备、材料数量，造成工程延误、设备材料到货期延误、结算滞后；

3.8.2.8 拒绝履行合同主要条款，造成合同无法正常履约；

3.8.2.9 因严重违约被采购人依法单方解除合同；

3.8.2.10 存在向采购人或关联公司相关工作人员行贿等不廉洁情形。

4、 报价登记及获取采购文件

登记时间为 2023 年 4 月 19 日至 2023 年 4 月 24 日（节假日除外）的上午 9：30～11：30，下午 14：00～16：00（北京时间），由供应商代表将登记函（详见采购文件格式一）及法定代表人证明书、法定代表人授权委托书（非法定代表人登记时提供）的电子版文件以邮件形式发送至采购方邮箱（lizexiong@gdairport.com）进行登记及获取采购文件，逾期可不受理。采购方将在收到邮件后 2 个工作日回复，并向供应商发出采购文件。

在规定的登记期间，登记的供应商不足 3 名时，采购方将发布公告延长接受登记时间。在延期登记时间内，已登记供应商的资料仍有效并可自行补充资料，未登记的申请单位可根据公告的约定参与登记。

若延长登记时间后，登记的供应商仍不足 3 名时，采购方将变更采购方式。

5、 报价文件的提交形式、地址和截止时间

1） 供应商可采取现场递交或邮寄两种方式递交项目报价文件（纸质版及电子版）。

2） 报价文件现场递交地址为：广州市白云区机场路 282 号机场管理集团办公楼 302 办公室，收件人：李先生。

3） 报价文件递交截止时间：2023 年 4 月 24 日，17:30。（邮寄方式递交的报价文件以文件到达时间为准）

4） 报价文件应按要求的时间、地点送达，逾期递交的报价文件恕不接受。

5） 采购方不接受以邮件、电话、传真等形式的报价。

6、 本项目不设未成交供应商经济补偿，准备报价文件和递交报价文件所发生的任何成本或费用由供应商自理。

7、 有关此次采购之事宜，可按下列联系方式向采购方咨询：

采购方：广东省机场管理集团有限公司

地　址：广东省广州市白云区机场路 282 号

联系人：李先生

电子邮箱：lizexiong@gdairport.com

8、 投诉监督

供应商可以对本次采购活动中的任何违法及不公平内容向集团公司纪检室投诉

第二部分

报 价 人（供应商） 须 知

第二部分 供应商（供应商）须知

目 录

一、说　明

1　项目说明

1.1　　广东省机场管理集团有限公司拟就信息安全服务项目进行国内采购，本项目采用综合评审方式确定成交供应商，广东省机场管理集团有限公司组织综合评审工作。

1.2　　采购范围

1）采购内容及限价：

序号	服务内容	采购最高限价
1	信息安全服务项目	人民币：壹佰贰拾万元

注：供应商必须对全部服务内容进行报价，报价应包含服务费、所有税费。

2）服务内容：

序号	服务目录	服务内容	服务对象	频率	单位	备注
1	安全托管服务	详见服务要求	集团云数据中心	1	年	
2	漏洞扫描服务	详见服务要求	机场集团云数据中心	12	次 / 年	
3	安全加固服务	详见服务要求	机场集团云数据中心	1	年	
4	安全评估服务	详见服务要求	机场集团云数据中心	1	次	
5	安全培训服务	详见服务要求	机场集团	3	次 / 年	
6	重保值守服务	详见服务要求	机场集团	3	次 / 年	
7	应急响应服务	详见服务要求	机场集团	1	年	
8	渗透测试服务	详见服务要求	机场集团	12	系统	

9	新上线系统评估	详见服务要求	机场集团	12	系统	
10	抽检服务	详见服务要求	机场集团	6	次 / 年	
11	安全巡检服务	详见服务要求	机场集团	4	次 / 年	
12	驻场服务	详见服务要求	机场集团	1	次 / 年	

1.3 采购要求

1.3.1 本项目技术服务进度要求：

明确工作时间要求：项目完成时间为合同签订之日起一年内。

1.3.2 供应商的项目报价应将相关服务分类报价，报价总和为本项目的项目总价。

1.3.3 供应商所提供的工作方案必须详细、完整、可靠、可行性强。

1.3.4 供应商报价中的服务费应是供应商为完成本项目的总服务费，包括但不限于“服务内容”中所列项目的费用。

1.3.5 供应商必须提交对采购文件实质性响应的项目报价文件。

1.4 现场考察

1.4.1 现场考察由供应商自行前往，采购方不统一安排。供应商若需相关数据，须自行测量。

2 定义

2.1 本文件中下列术语定义为：

服务： 指供应商提供信息安全服务相关技术支持。

供应商： 指与第 3 条规定的要求一致的、响应邀请函、参加报价的独立法人。

采购方： 广东省机场管理集团有限公司。

合同： 指由采购所产生的合同或合约文件。合同由广东省机场管理集团有限公司与成交供应商签订。

3 合格的供应商

3.1 合格的供应商要求见邀请函中的第 3 点。

4 合格的服务

4.1 合同中提供的所有服务，均应来自中华人民共和国或与之有正常贸易关系的国家和地区，本合同的支付仅限于对这些服务。

5 报价费用

供应商应承担所有编写项目报价文件和参加报价的所有费用，不论结果如何，采购方在任何情况下均无义务和责任承担这些费用。

二、采购文件

6 采购文件构成

6.1 要求提供的服务、评审过程和合同条件在采购文件中均有说明。采购文件包括：

第一部分 邀请函
第二部分 供应商须知
第三部分 合同条款
第四部分 项目报价文件格式
第五部分 用户需求书

6.2 供应商应认真阅读采购文件中所有的事项、格式、条款和规范等要求。供应商没有按照采购文件要求提交全部资料，或者项目报价文件没有对采购文件各方面都做出实质性响应的供应商的项目报价文件将被拒绝。

7 采购文件的澄清

7.1 采购方可以对已发出的采购文件进行必要的澄清或者修改。澄清或者修改的内容可能影响报价文件编制的，采购方将在递交报价文件截止时间前以书面形式（纸质版扫描件电子邮件发送）通知所有供应商，该通知内容作为采购文件的组成部分。

7.2 供应商对采购文件有异议的，应当在 XX 年 XX 月 XX 日 16：00 前以书面形式提出，纸质版加盖公章扫描件以电子邮件方式发送至采购方邮箱（lizexiong@gdairport.com）。采购方认为确有必要答复的，将于递交报价文件**截止时间**前以书面形式予以答复，同时将书面答复的纸质版扫描件向所有供应商发送，该答复作为采购文件的组成部分。

7.3 采购方可根据采购文件的澄清情况，顺延报价文件递交截止时间。

8 采购文件的修改

8.1 采购文件发出后，在**报价文件递交截止日期前**，采购方可对采购文件进行必要的澄清或修改。

8.2 采购文件的修改的纸质版扫描件以电子邮件方式发送给所有供应商，采购文件的修改内容作为采购文件的组成部分，具有约束作用。

8.3 采购文件的澄清、修改、补充等内容均以书面形式明确的内容为准。当采购文件、采购文件的澄清、修改、补充等在同一内容的表述上不一致时，以最后发出的书面文件为准。

8.4 为使供应商在编制报价文件时有充分的时间对报价文件的澄清、修改、补充等内容进行研究，采购方将酌情延长报价文件递交的截止时间，具体时间将在报价文件的修改、补充通知中予以明确。

9 采购语言及计量单位

9.1 采购方发出的采购文件采用中文。

9.2 采购文件中使用的计量单位都是公制系统。

三、项目报价文件的编制

10 项目报价文件

10.1 报价文件由商务部分、技术部分及价格部分组成。

10.2 报价文件的签署要求：报价文件所有需盖章或签字的部分均需供应商法定代表人或法定代表人授权委托代表盖章或签字，否则将被视为无效报价文件。

10.3 报价文件包括纸质文件一式 5 份，计算机文件一式 1 份。纸质版正本 1 份，封面标注“正本”字样，副本 4 份，封面标注“副本”字样。副本可为正本盖章签字后的复印件，若正本与副本不符的内容，以正本为准。

10.4 报价文件应做到清晰、完整，文本、图纸规格应当尽量统一。除非另有规定，否则报价文件的计量单位宜采用国际标准计量单位，尺寸齐全、准确，所有文字说明和文字标注以中文为准，报价均为人民币，时间均为北京时间。

11 商务部分（含资格审查文件）编制要求

11.1 商务部分由下列资料组成：

1) 封面：写明项目名称、报价文件、供应商名称及年月日；加盖供应商公章。
2) 目录。
3) 填妥并盖章的报价函（格式见附录 1）。
4) 企业营业执照复印件（盖公章）。
5) 法定代表人证明书及法定代表人授权书（格式见附录 3）
6) 广东省机场管理集团有限公司招标、采购管理平台合作商登记表（盖公章）。
7) 供应商没有因腐败或欺诈行为，与采购方无发生各种诉讼、仲裁和不良投诉的承诺函（盖公章）。
8) “国家企业信用信息公示系统”网站（www.gsxt.gov.cn）查询截图（盖公章）。
9) “信用中国”网站（www.creditchina.gov.cn）“失信惩戒”页面截图及下载的信用评估报告（盖公章）。
10) “中国执行信息公开网”网站截图并加盖公章。
11) 供应商认为有必要提供的其他资料

（注：事业单位不需要提供以上第 8）项内容。）

12 技术部分编制要求

12.1 技术部分（技术服务方案）内容包括：

1） 目录。
2） 项目说明书（项目概况及供应商对项目的理解）。
3） 本项目的工作方案，完工本项工作的具体举措，拟投入的设备设施、人员情况。
4） 项目工期计划。

5） 供应商认为有必要提供的其他资料。

12.2 报价文件密封要求：正副本报价文件用不透明包装物包装密封，外面标注“项目名称”、“供应商名称”及“报价文件”“供应商联系电话”“供应商邮箱”字样，外包装材料不应留有可在包封后添加或抽取报价文件的空隙，并在封口处加盖供应商公章。

13 计算机文件

13.1 供应商必须随报价文件同时提交一套无病毒计算机文件， 包括以下内容：

1） 一套 PDF 格式的报价文件盖章扫描件。

2） 一套 WORD 格式可编辑的报价文件电子版。

13.2 计算机文件需采用 U 盘装载，所有文件不做压缩处理、不设密码，装于独立的信封，信封上注明“计算机文件”，与报价文件一起密封包装。

14 知识产权和专利权

14.1 供应商应保证，采购方在中华人民共和国使用供应商在服务期间提供的成果的任何一部分时，免受第三方提出侵犯其专利权、商标或工业设计权的起诉。

14.2 报价已包括所有应支付的，对专利权和版权、设计或其他知识产权而需要向其他方支付的版税。

15 保密

15.1 如采购方向供应商提供图纸、详细资料、样品、模型、模件和所有其他资料，这些均被视为保密资料，仅被用于它所规定的用途，除非得到采购方的同意，不能向任何第三方透露。

16 报价文件有效期

16.1 ★项目报价文件应在邀请函规定的报价日后的 90 天有效期内保持有效。报价文件有效期比规定短的将被视为非响应报价而予以拒绝。

16.2 特殊情况下在原有报价文件有效期截止之前，采购方可征求供应商同意延长报价文件有效期。这种要求与答复均应以书面形式提交。供应商可以拒绝采购方的这种要求。

17 不允许偏离的条款

17.1 采购文件中的重要条款（带“★”号条款）不允许偏离，如项目报价文件中对重要条款有偏离，则是供应商的风险。

17.2 对供应商须知 17.1 条中任何条款的偏离将导致报价文件无效。

17.3 下述条款不应视作不可偏离：

1） 未加注“★”号的条款；

2） 用户需求书中已明确的供应商可提供其他优选报价文件部分。

17.4 项目报价文件中优于用户需求书要求部分不视作偏离，将不被拒绝，供应商对这种优于用户需

求书要求的情况必须单独说明。

四、项目报价文件的递交

18 项目报价文件的密封和标记

18.1 供应商应将项目报价文件应第三部分 12.2、13.2 要求密封和标记。

18.2 如果供应商递交的报价文件未按要求密封，采购方将拒绝接受其报价文件。

18.3 如果因密封不严，标记不清而造成报价文件过早启封、失密等情况，采购方概不负责。

19 递交报价文件截止时间

19.1 供应商应将正本和所有副本，由供应商代表按采购邀请函第 5 条要求于项目递交报价文件截止时间前送达报价地点。

19.2 采购方可以通过修改采购文件自行决定酌情延长截止期。在此情况下，采购方和供应商受截止期制约的所有权利和义务均应延长至新的截止日期。

20 迟交的项目报价文件

20.1 采购方将拒绝在截止时间后递交的任何项目报价文件。

五、综合评审过程

21 报价文件的递交

21.1 采购方在采购文件中规定的日期、时间和地点组织接收报价文件。

22 评审小组

22.1 本项目的评审工作由采购方内部组成评审小组完成。评审小组共 5-7 名成员。

23 项目报价文件的评审

23.1 评审小组将审查项目报价文件是否完整、供应商是否符合合格条件、报价有无计算上的错误、文件签署是否合格、项目报价文件的总体编排是否有序。

23.2 算术错误将按以下方法更正：

1) 如果总价与数量乘单价的积而得到的总价不一致，则以单价为准计算总价。
2) 如果用大写数值与用数字表示的数值不一致，以大写数值为准。

23.3 在详细评审之前，评审小组会要审查每份项目报价文件是否实质上响应了采购文件的要求。实质上响应的报价文件应该是与采购文件要求的全部主要条款（加“★”号）、条件和规格相符，没有重大偏离的报价文件。

23.4 如果项目报价文件实质上没有响应采购文件的要求，其报价文件将可能被拒绝。不满足下列情况之一的，其报价文件将可能被拒绝：

1) 完全符合邀请函中第 3 点“合格的供应商”要求；
2) 报价有效期符合采购文件规定；
3) 供应商递交一种报价方案和报价；
4) 报价没有超过最高限价；
5) 报价函必须有法定代表人或授权代表签字且加盖公章；
6) 报价文件必须有法定代表人或授权代表签字且加盖公章；
7) 法定代表人授权书必须有法定代表人和被授权人的签字或盖章。

23.5 如果通过初步评审的供应商少于 3 名，本次采购失败，采购方将修正采购文件后重新组织采购。

24 报价文件的详细评审

24.1 评审小组对通过初步评审的报价文件中的商务服务、技术方案等方面采用百分制综合评分，其构成及权重为：价格部分得分占 30%，商务技术部分得分占 70 %，详细评分标准如下：
1）商务技术评分表，满分 70 分。

序 号	项目	分值	评分标准
1	企业资质	3	供应商为国家信息安全漏洞共享平台(CNVD)技术组成员，提供官网查询链接及对应截图并加盖公章 得3 分，不具备不得分;
		2	供应商具备软件研发实力通过CMMI L5 认证得 2分（提供对应证书复印件并加盖公章），通过 CMMI L3 认证得 1分 （提供相关证书复印件并加盖公章），没有不得分;
		6	供应商具备中国网络安全审查技术与认证中心(CCRC)的安全服务资质认证,信息安全风险评估(一级)、信息安全应急处 理(一级)、信息系统安全集成服务(二级及以上)、信息安全运维服务(二级及以上)、软件开发服务资质等，每具备一个认证或资质得1 分,总分不超过6分（提供相关证书复印件并加盖公章）,不具备不得分;
2	运营能力	4	供应商具备国家信息安全服务（安全运营类一级）资质，安全运营平台的平台能力符合《面向云计算的安全运营中心能力要求》标准，每具备一项得2分，总分4分，不具备不得分。（提供相关证书复印件并加盖公章）
3	企业类似业绩	5	自2020年起(以合同签署时间或成交通知书发出时间为准),供应商完成过合同金额不低于100万元的信息安全服务类的项目案例,提供相关合同复印件; 每提供一个可得1分，总分不超过5分。 供应商须提供能证明本次采购业绩要求的合同件（从2020年1月1日至今的已验收通过的合同）。合同件须至少包含：合同买卖双方盖章页、合同签订日期
4	项目服务团队	10	（1）供应商为本项目指定的项目负责人具有以下资质的,每具备一项的得1分，总分不超过6分，提供对应人员的资质及3个月内的社保证明，没有则不得分: 信息系统项目管理师、CISAW-安全运维方向、PMP（项目管理专业人士资格认证）、CISSP（信息系统安全专业认证）、系统集成项目管理工程师、CCSK、ISO/IEC27001 Foundation、ITIL4 Foundation、CISP-PTE、CDPSE、Security+、PRINCE2 Foundation、CISM、信息安全工程师-中级(软考) （2）安服团队人员要求：为本项目投入的安全服务实施人员需要常

			驻广东省，需具备中国信息安全测评中心颁发的CISP-PTS国家注册信息安全渗透测试专家认证或CISP-PTE国家注册渗透测试工程师认证证书。（上述资质一人具有多个资质不可以累加，每一个人具备资质得0.5分，最高得4分） 注：要求提供相关证书复印件并加盖供应商公章,并提供服务人员近三个月社保缴纳证明的复印件（缴纳地点为广东省内），提供证明材料复印件并加盖供应商公章。如开具虚假证明一旦查实将取消报价资格。
5	整体服务水平	40	（1）横向对比供应商安全托管平台或工具的能力；对比优得 15-20 分；对比次之得 10-15 分；对比一般得 5-9 分；对比差得 1-5 分。 （2） 横向对比供应商整体安全服务方案；对比优得 15-20 分；对比次之得 10-15 分；对比一般得 5-9 分；对比差得 1-5 分。 注：供应商须针对本项目需求提供安全托管服务、安全服务方案，供评审综合评判。若不提供，此项不得分。

2）价格评审细则：价格分满分 30 分，各供应商的价格得分按如下标准计算：

（1）基准价：取所有通过初步评审的供应商报价的算术平均值作为基准价；

（2）当报价等于基准价时，价格得分为 30 分；

（3）当报价高于基准价时，按每高 1%的在 30 分基础上扣 1 分，不足 1%的按插值法计算，直至扣至 0 分；

（4）当报价低于基准价时，按每低 1%的 在 30 分基础上扣 0.5 分，不足 1%的按插值法计算，直至扣至 0 分；

（5）按上述方法计算的结果保存两位小数，第三位四舍五入。

25 综合得分计算

25.1 综合得分＝商务技术得分+价格得分。

26 成交供应商的确定

26.1 评审小组按综合得分从高到低排序，推荐综合得分最高的供应商为第一成交候选人，综合得分次高者为第二成交候选人，依次类推，评审小组将推荐总得分前 3 名的供应商为成交候选人。如出现总得分相同，价格低者排名靠前，若价格仍相同，则由评审小组投票，按少数服从多数原则确定供应商排名先后。

26.2 采购方根据评审小组的推荐，确定本项目成交供应商。

27 与采购方的接触

27.1 除供应商须知的相关规定外，从报价文件截至之日起至授予合同期间，未经采购方书面要求，供应商不得就与其项目报价文件有关的事项与采购方联系。

27.2 供应商试图对评审小组的评审或采购方授予合同的决定进行影响，都可能导致其报价文件被拒绝。

六、授予合同

28 资格后审

28.1 采购决定将考虑供应商的财务、服务能力等，其基础是审查供应商提交的资格证明文件和其它采购方认为必要的、合适的资料。

28.2 如果审查通过，则将合同授予符合第 33.1 条规定的供应商；如果审查没有通过，则取消其成交资格。在此情况下，评审小组将对技术和商务上充分满足采购文件要求的供应商中，综合得分次高的供应商能否满意地履行合同义务作类似的审查，或重新组织采购。

29 合同授予标准

29.1 采购方将把合同授予被确定为实质上响应采购文件的要求并具有履行合同能力的符合采购需求、综合得分最高的供应商。

30 授予合同时更改采购服务数量的权力

30.1 采购方在授予合同时有权在一定的幅度内对报价表中规定的服务数量予以增加或减少，但不得对单价或其它的条款和条件做任何实质改变。

31 接受和拒绝任何或所有报价文件的权力

31.1 采购方保留在签署合同之前任何时候根据评审小组的决定拒绝所有或任何报价文件，以及宣布所有或任何项目报价文件无效的权力，对受影响的供应商不承担任何责任，也无义务向受影响的供应商解释采取这一行动的理由。

32 成交通知书

32.1 在项目有效期期满之前，采购方将经过采购方确认的成交通知书以书面形式通知成交供应商。

32.2 成交通知书将是合同的一个组成部分。

33 签订合同

33.1 成交供应商在收到成交通知书后，应派遣其授权在合同上签字的代表与广东省机场管理集团有限公司签署合同。

33.2 合同的组成基于本采购文件的以下部分以及项目报价文件的相应的部分：

（1） 第三部分 合同条款
（2） 采购方的澄清文件

（4） 第五部分 用户需求书

（5） 供应商的报价文件

33.3 如果成交供应商没有按照上述第 33.1 条规定执行，采购方将有充分理由取消该成交决定。在此情况下，采购方可将合同授予其他满足采购要求的供应商，或重新组织采购。

34 成交结果通知

34.1 采购方将在广东省机场管理集团有限公司招标、采购管理平台(wz.gdairport.com)发布采购结果。

七、不予合作对象管理

（一） 参与非招标采购活动的供应商，有下列情形之一的，应列入采购人不予合作对象名单：

1.供应商通过向评审委员会成员、招标代理机构、采购人提供不正当利益谋取成交；

2.借用他人名称、资质进行挂靠，或者将自己的名称、资质借给他人挂靠进行报价，或以其他方式弄虚作假，骗取成交；

3.采取不正当手段诋毁、排挤其他合作对象；

4.在采购过程与采购人员、招标代理机构私下进行协商谈判，损害采购人或其他供应商利益；

5.供应商针对资格审查文件、采购文件或者在资格预审公示或成交候选人公示期间，故意捏造事实、伪造证明材料，恶意进行质疑，影响采购工作顺利推进；

6.存在围标串标行为；

7.采购人成交通知书发出后，供应商拒绝签订合同（因不可抗力原因不能履行合同的除外）；

8.自采购公告发布之日起前三年内与采购人以及关联公司发生诉讼或仲裁的单位；

9.供应商发生向各单位工作人员行贿情形；

10.参与采购人非招标采购活动进行两次（含）以上无效异议的合作对象，因其无效异议对采购人以及关联公司造成经济损失、工作滞后的，可纳入非招标采购项目不予合作名单。具有下列情形之一的，应视为无效异议：

1）异议主体不是供应商或其他利害关系人；

2）供应商是法人的，异议书必须由其法定代表人或者授权代表签字并盖章；其他组织或者自然人投诉的，异议书必须由其主要负责人或者投诉人本人签字，并附有效身份证明复印件；

3）异议人未提供必要的证明材料和明确的要求；

4）异议人捏造事实、伪造材料或者以非法手段取得证明材料进行异议的，证据来源的合法性存在明显疑问，异议人无法证明其取得方式合法的，视为以非法手段取得证明材料；

5）其他属无效异议的情形。

（二）成交供应商在合同履行，项目实施、运行阶段，有下列情形之一的，应列入不予合作对象名单：

1.不按采购文件要求，报价文件承诺的条件与采购人签订合同，或在合同签订中存在欺诈情形，违反采购文件规定，对采购人或关联公司不利；

2.违反合同约定，将承揽项目转包或违法分包给他人；

3.因成交供应商责任原因连续发生不安全事件、事故或造成恶劣不良影响；

4.使用的设备、材料以次充好或提供与合同不符的假冒伪劣产品等降低质量情形或造成不良影响；

5.因环保、噪音问题造成社会恶劣影响；

6.拖欠农民工工资，造成恶劣影响的，或发生上访维稳事件，或导致采购人或关联公司垫付农民工工资；

7.虚报工程量或设备、材料结算量，拒不接受第三方咨询单位按合同约定审定的工程造价，设备、材料数量，造成工程延误、设备材料到货期延误、结算滞后；

8.拒绝履行合同主要条款，造成合同无法正常履约；

9.因严重违约被采购人依法单方解除合同；

10.存在向采购人或关联公司相关人员行贿等不廉洁情形。

第三部分 合同条款

技术服务合同

项目编号：

项目名称：广东省机场管理集团有限公司信息安全服务项目

甲方：广东省机场管理集团有限公司

联系人：

地址：

乙方：

联系人：

地址：

签订地点：广州市

根据《中华人民共和国民法典》规定和《广东省机场管理集团有限公司信息安全服务项目采购文件》（项目编号：_____ ）的相关要求和评审结果，甲乙双方经友好协商，签订本合同。

一、合同标的

本合同的标的为乙方向甲方提供“广东省机场管理集团有限公司信息安全服务项目”（以下简称“信息安全服务项目”或“本项目”）服务。

1、服务内容：

甲方委托乙方向甲方提供信息安全服务,并提交相关的安全服务报告,具体的服务内容如下:

序号	服务项	服务内容	服务对象	服务周期/频 率

2、服务要求：

（1）服务内容要求

乙方须按照服务清单按时完成各项服务工作，并将报告发送给甲方，在服务过程中，甲方有权对乙方提供的服务质量问题提出意见和建议，乙方应按甲方的要求及时改进。

（2）服务团队要求

乙方需要成立项目服务团队，其中具有 PMP 或者 ITSS 项目管理资质人员不少于 1 人，所有项目参与人员应具备信息安全相关服务资质（CISP、CISAW 等）。项目经理须具备 5 年或以上信息安全服务经验，并具有项目管理资质证书。项目经理与技术服务人员必须为广州本地工作人员。

服务团队成员名单如下：

姓名	角色	职称	联系方式	备注

……	……	……	……	……

（3）服务期限要求

项目服务期限为一年，自本合同生效之日起算，乙方应在服务期限内完成本合同约定的全部服务内容，并提交相应服务报告。

3、服务方式：

（1）乙方负责提供相应服务报告初稿供甲方审阅，并按甲方意见进行核对、修改和完善；

（2）乙方修改完成并形成相应服务报告的正式文本后，向甲方提交各类《服务报告》正式文本纸质版一式三份。

（3）在服务程中，乙方应遵守国家法律法规及地方法规的有关规定。

（4）乙方在服务全过程中应确保甲方系统、数据可正常使用和安全，并解答甲方相关咨询，听取甲方相关建议或意见，按甲方要求履行合同、提供服务。

（5）乙方对甲方提供的任何技术资料、数据或其他工作成果负有保密义务，并妥善保管相关资料，不得泄露，并不得以任何形式提供给任何第三方或用于本合同以外的其它目的。

第二条 为保证乙方有效进行技术服务工作，甲方应当向乙方提供下列协作事项：

1、提供技术资料：甲方向乙方提供完成信息安全服务所需的网络应用需求、网络结构拓扑及说明、产品清单及配置、安全保护设施设计实施方案或改建实施方案、网络软件硬件和网络安全产品服务清单等必要的技术资料；

2、提供工作条件：甲方为乙方提供工作上必要的便利。

第三条 双方确定，按以下标准和方式对乙方提交的技术咨询工作成果进行验收：

1、乙方提交的技术咨询工作成果包含但不限于《安全评估报告》《漏洞扫描和修复报告》《新上线系统评估报告》《渗透测试报告》《安全加固报告》《安全运维报告》《安全抽检服务报告》等服务过程中的文档。

2、技术咨询工作成果的验收标准：验收报告经甲方确认并签字盖章。

第四条 技术服务报酬及支付方式为：

1、技术服务报酬总额为： 大写： （小写： 元）；

2、技术服务报酬由甲方分三期支付给乙方。

具体支付方式和时间如下：

（1）合同生效后，甲方收到乙方提供的合格发票后30个工作日内，向乙方支付合同总金额的30%，即人民币　　元整（小写：　　元）。

（2）乙方按要求完成半年度工作内容，甲方收到乙方提供的合格发票后30个工作日内，向乙方支付合同总金额的30%，即人民币　　元整（小写：　　元）。

（3）乙方完成全部服务内容，编制验收报告并经甲方签字确认后，甲方在收到乙方提供的合格发票后30个工作日内，向乙方支付合同总金额的40%，即人民币　　元整（小写：　　元）。

（4）乙方提供的发票必须为增值税专用发票。开具发票等相关的税费均由乙方承担，除合同约定的费用，甲方不再额外支付乙方其他费用。

甲方开票信息为：

名称：广东省机场管理集团有限公司

税号：91 440 000 190 488 448J

单位地址：广州市机场路282号

电话号码：86122784

开户银行：中国工商银行广州市机场支行

银行账号：360 206 520 900 039 6878

乙方的收款账户信息为：

开户银行：

账　　户：

账　　号：

第五条 双方确定，在本合同有效期内，甲方指定_____为甲方项目联系人，乙方指定本项目负责人_____为乙方项目联系人。项目联系人承担以下责任：

1、督促工作进度；

2、传递有关信息、资料；

3、合同双方一切未尽事宜的协调。

一方变更项目联系人的，应当及时以书面形式通知另一方。未及时通知并影响本合同

履行或造成损失的，应承担相应的责任。

第六条 违约责任

1、乙方未能按照本合同的约定和甲方的要求交付成果的，每逾期一天，乙方按本合同总金额的万分之五向甲方支付违约金；逾期 30 天以上（含）的，甲方有权单方解除本合同，乙方除应退还甲方已支付的费用并承担上述逾期违约金外，乙方还应按本合同总金额的 20%向甲方支付违约金，违约金不足以弥补甲方损失的，乙方还应补足。

2、乙方交付的成果未通过甲方验收的，乙方应根据甲方提出的意见和建议在甲方限定时间内予以返工并重新交付成果。乙方拒绝返工或返工后重新交付的成果质量仍然达不到甲方要求的，甲方有权单方解除本合同，乙方除应退还甲方已支付的费用并承担上述逾期违约金外，还应按本合同总金额的 20%向甲方支付违约金，违约金不足以弥补甲方损失的，乙方还应补足。

3、本合同履行期限内，乙方不得委托任何第三方完成本合同部分或全部委托事项，否则视为乙方根本违约，甲方有权解除合同，乙方除应退还甲方已支付的费用外，还应并有权要求乙方向甲方支付本合同总金额的 30%作为违约金，违约金不足以弥补甲方损失的，乙方还应补足。

4、乙方未按本合同约定的团队成员提供服务，更换项目负责人的，甲方有权解除合同，乙方除应退还甲方已支付的费用外，还应向甲方支付本合同总金额的 30%作为违约金；更换具有 PMP 或者 ITSS 项目管理资质人员的，甲方有权要求乙方支付本合同总金额的 10%作为违约金；更换项目组其他工作人员的，每更换 1 名，甲方有权要求乙方支付本合同总金额的 1%作为违约金。

第七条 双方因履行本合同而发生的争议，应协商解决。协商不成的，任何一方应向广州市白云区人民法院提起诉讼。

第八条 任何一方因不可抗力不能履行合同时，应在不可抗力事件结束后 1 日内向对方通报，以减轻可能给对方造成的损失，在取得有关机构的不可抗力证明或双方谅解确认后，允许延期履行或修订合同，并根据情况可部分或全部免于承担违约责任。

第九条 本合同一式肆份，甲方执贰份，乙方执贰份，具有同等法律效力。

第十条 本合同经双方法定代表人或其授权代表签字并加盖双方印章之日起生效。

（以下无正文）

合同签署页

甲方：广东省机场管理集团有限公司（盖章）

法定代表人或其授权代表：_____（签名或盖章）

年　　月　　日

乙方：_____（盖章）

法定或委托代理人：_____（签名或盖章）

年　　月　　日

第四部分 项目报价文件格式

附录 1

供 应 商 登 记 函

广东省机场管理集团有限公司:

我单位报名参加广东省机场管理集团有限公司信息安全服务项目的报价，严格遵守有关规定，并按采购文件的规定，准时报送报价文件。

供应商名称（公章）：

法定代表人或授权代表签字：

年　　月　　日

报价企业概况表

企业名称			
通讯地址			
营业执照	1、编 号	2、营业范围	3、发照单位
现在职工		注册资本金（万元）	
法人代表		项目联系人	
联系方式	手　　机： 邮政编码：	传　　真： E-mail：	

供应商名称（章）：

法定代表人或授权代表签字：

日期：　年　　月　　日

附录 2

附录 2-1

报 价 函

项目名称：广东省机场管理集团有限公司信息安全服务项目

致: 广东省机场管理集团有限公司

根据贵方为广东省机场管理集团有限公司信息安全服务项目采购的邀请函，作为经供应商正式授权代表供应商_____(供应商名称和地址)的报价文件书签名方代表_____ _____(签名人全名，职务)，在此提交项目报价文件，正本一份，副本四份。

签字人代表以此函申明并同意:

1) 对随附报价表所规定的采购内容的总价为含税价人民币_____元（大写：_____元）。
2) 供应商将承担按照采购文件的所有条款履行合同的责任和义务。
3) 供应商已详尽研究了所有采购文件包括修正文(如果有)，所有已提供的参考资料以及有关附件并完全明白，供应商必须放弃在此方面提出含糊意见或误解的一切权力。
4) 供应商之报价文件有效期为自报价之日起90 个日历日。
5) 供应商同意按照甲方可能提出的要求提供与其所递交报价文件有关的任何其它数据或信息。
6) 我方理解贵方不一定接受最低报价或任何贵方可能收到的报价文件。

本报价文件连同贵方成交通知书应构成对双方均有约束力的合同，直至正式合同编制完毕并生效。

供应商名称：_____（盖公章）

法定代表人或授权代表签名：_____

日期：_____

附录2-2

报价明细表

序号	采购内容	总价(含税价)	税率（%）	备注
1	XXX			
2	XXX			
合计				

供应商名称：_____（盖公章）

法定代表人或授权代表签名：_____

日期：_____

附录 3

三、资格性文件

3.1 报价函

（采购人）：

依据贵方采购项目名称_____（项目编号：_____）要求，我方代表（姓名、职务）经正式授权并代表（供应商名称、地址）提交下述文件，文件内附有对应于报价文件各册内容（文件格式采用贵方认可的办公软件制作）。

1. 价格部分；

2. 自查表；

3. 资格性文件；

4. 商务部分；

5. 技术部分；

6. 其他部分。

在此，我方声明如下：

1.同意并接受采购文件的各项要求，遵守采购文件中的各项规定，按采购文件的要求提供报价。

2.全部货物和相关服务的报价总价详见报价表。

3.综合评审有效期为报价截止日之日起 90 天，成交人的询价有效期延至合同验收之日。

4.我方已经详细地阅读了全部采购文件及其附件，包括澄清及参考文件(如果有的话)。我方已完全清晰理解采购文件的要求，不存在任何含糊不清和误解之处，同意放弃对这些文件所提出的质疑和质疑的权利。

5._____*(供应商名称)*_____作为供应商正式授权_____*(授权代表全名，职务)*_____代表我方全权处理有关本报价的一切事宜。

6.我方已毫无保留地向贵方提供一切所需的证明材料。

7.我方承诺在本次报价文件中提供的一切文件，无论是原件还是复印件均为真实和准确的，绝无任何虚假、伪造和夸大的成份，否则，愿承担相应的后果和法律责任。

8.我方明白并愿意在规定的综合评审时间和日期之后，报价有效期之内撤回报价，则报价保证金将被贵方没收

9.我方完全服从和尊重评委会所作的评定结果，同时清楚理解到报价最低并非意味着必定获得成交

资格。

10.我方如果成交，将保证履行采购文件以及采购文件修改书（如果有的话）中的全部责任和义务，按质、按量、按期完成《合同书》中的全部任务

11. 我方如果成交，我司严格保密本项目的成果文件内容，如因我司管理不善造成泄密情形的，我司接受采购人对我司的“三年内不得参加广东省机场集团及其下属单位的招标和非招标采购活动”的处罚。

12.我方同意按采购文件规定向采购代理机构缴纳采购费，就本次采购应由我方交纳的服务费将按随附于本报价文件的承诺书支付。

供应商：

地址：

传真：

电话：

电子邮件：

供应商法定代表人（或法定代表人授权代表）：

供应商名称：

开户银行：

帐号：

日期：

3.2 法定代表人/负责人资格证明书及授权委托书

（1）法定代表人/负责人资格证明书

致：（采购人）：

_____同志，现任我单位_____职务，为法定代表人，特此证明。

签发日期：　　单位：　　（盖章）

附：代表人性别：　　年龄：　　身份证号码：

联系电话：

营业执照号码：　　经济性质：

主营（产）：

兼营（产）：

进口物品经营许可证号码：

主营：

兼营：

说明：1.法定代表人为企业事业单位、国家机关、社会团体的主要行政负责人。

2.内容必须填写真实、清楚、涂改无效，不得转让、买卖。

3.将此证明书提交对方作为合同附件。

（为避免废标，请供应商务必提供本附件）

法定代表人身份证复印件正反面

（2）法定代表人/负责人授权委托书

致：（采购人）：

兹授权_____同志，为我方签订经济合同及办理其他事务代理人，其权限是：_____。

授权单位：　　（盖章）　　法定代表人 ：　　（签名或盖私章）

有效期限：至　　年　　月　　日　　签发日期：

附：代理人性别：　　年龄：　　职务：　　身份证号码：

联系电话：　　手机：

营业执照号码：　　经济性质：

主营（产）：

兼营（产）：

进口物品经营许可证号码：

主营：

兼营：

说明：1.法定代表人为企业事业单位、国家机关、社会团体的主要行政负责人。

2.内容必须填写真实、清楚、涂改无效，不得转让、买卖。

3.将此证明书提交对方作为合同附件。

4.授权权限：全权代表本公司参与上述采购项目的响应，负责提供与签署确认一切文书资料，以及向贵方递交的任何补充承诺。

5.有效期限：与本公司报价文件中标注的报价有效期相同，自本单位盖公章之日起生效。

6.询价签字代表为法定代表人，则本表不适用。

代理人身份证复印件正反面

3.3 营业执照（或法律法规规定的其他主体证明文件）复印件。

3.4 报名资格与诚信承诺函

致：XXXX 公司（采购方）

在研究并完全理解了广东省机场管理集团有限公司 XXXXXX 项目竞价文件后，我司完全同意并接受项目采购文件的所有内容，同时向贵司承诺我司完全符合采购文件第一部分 采购函合格供应商资格条件，并完全响应采购方“合作商不诚信行为”的确定条件。承诺如有造假行为，我司愿意无条件接受采购方的以下处理：

1.取消本项目报价、成交资格，并在相关网站公示。

2.由采购方没收报价/合同履约保证金（如有）。

3.严格按照《广东省机场管理集团有限公司采购合作对象管理办法》接受处罚，按规定禁止参加广东省机场管理集团有限公司本部、各全资、控股公司及集团公司所属非法人实体单位的所有采购项目。

4.自行承担被取消项目资格的所有后果和责任。

5.其他行政处理决定。

供应商名称：_____（盖公章）

法定代表人或授权代表签名：_____

日期：_____

3.5 采购文件响应承诺书

致：广东省机场 XXX 公司（采购方单位）

我司保证提交的XXXX公司XXXXXX项目报价文件所有内容与贵司（单位）的采购文件要求条款完全响应，在此，我方声明如下：

1.同意并接受采购文件的各项要求，遵守采购文件中的各项规定，按采购文件的要求提供报价。

2.报价有效期为报价截止日之日起 XX 天，成交人的报价有效期延至合同验收之日。

3.我方已经详细地阅读了全部竞价采购文件及其附件，包括澄清及参考文件(如果有的话)。我方已完全清晰理解竞价文件的要求，不存在任何含糊不清和误解之处，同意放弃对这些文件所提出的质疑和质疑的权利。

4. *（供应商名称）* 作为供应商正式授权 *（授权代表全名，职务）* 代表我方全权处理有关本报价的一切事宜。

5.我方已毫无保留地向贵方提供一切所需的证明材料。

6.我方承诺在本次报价文件中提供的一切文件，无论是原件还是复印件均为真实和准确的，绝无任何虚假、伪造和夸大的成份，否则，愿承担相应的后果和法律责任。

7.我方如果成交，将保证履行采购文件以及采购文件修改书（如果有的话）中的全部责任和义务，按质、按量、按期完成《合同书》中的全部任务。

8.我司成交后，将保证严格按照竞价采购文件要求提供货物/服务。

9. 我方如果成交，我司严格保密本项目的成果文件内容，如因我司管理不善造成泄密情形的，我司接受采购人对我司的“三年内不得参加广东省机场集团及其下属单位的非招标采购活动”的处罚。

供应商名称：

地址：

传真：

电话：

电子邮件：

供应商法定代表人（或法定代表人授权代表）：

供应商单位名称：

开户银行：

帐号：

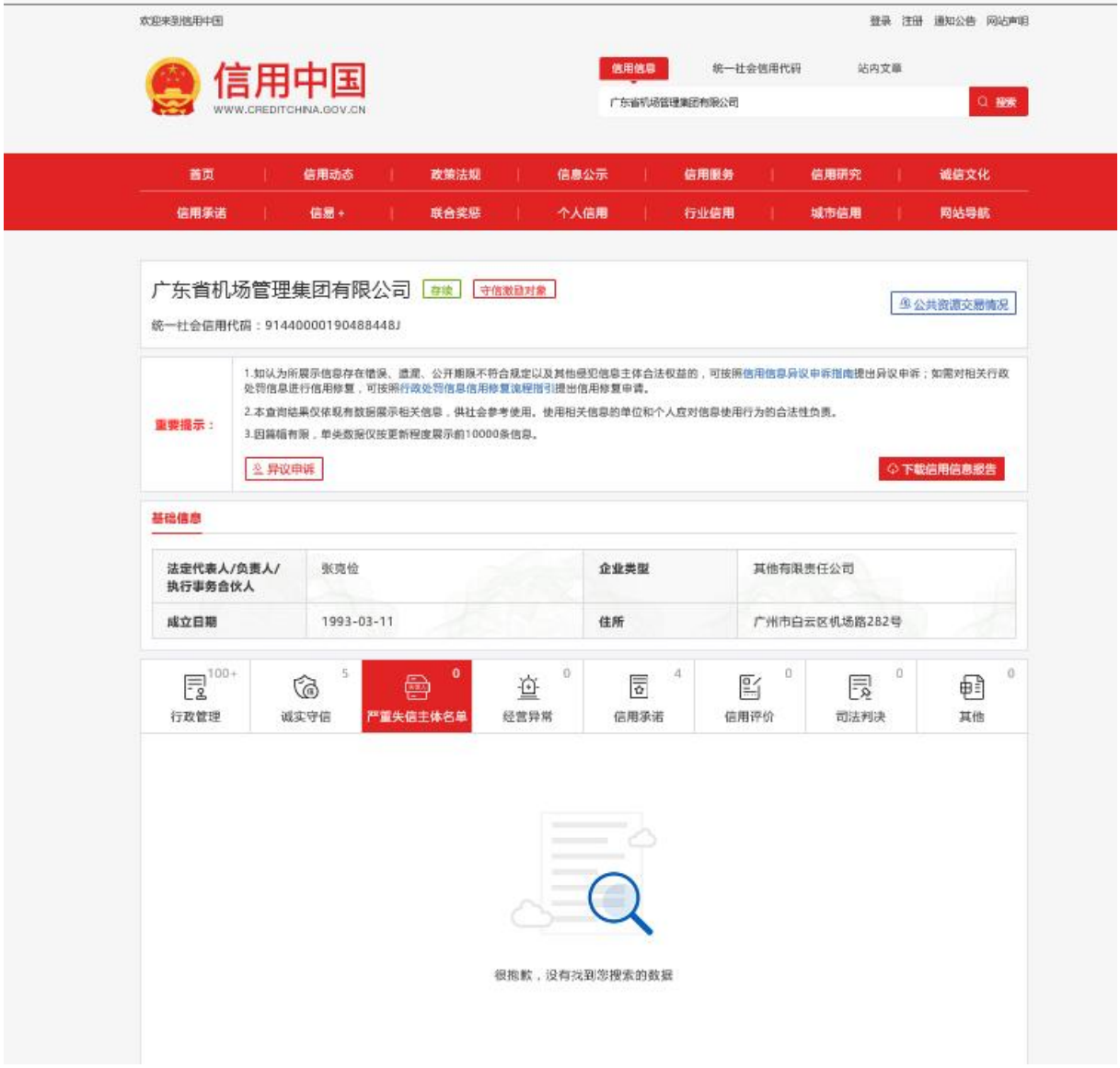
日期：

3.6“国家企业信用信息公示系统”网站（www.gsxt.gov.cn）格式

（经营异常名录或严重违法失信企业名单）

注：供应商须按上述格式要求截图并加盖公章，截图清晰显示单位名称及查询结果。

3.7“信用中国”网站（www.creditchina.gov.cn）截图格式



注：供应商须按上述格式要求截图并加盖公章，截图清晰显示单位名称及严重失信主体名单信息。

3.8 报价承诺书

（采购人名称）：

本供应商已详细阅读了（项目名称）采购文件，自愿参加上述项目报价，现就有关事项向采购人郑重承诺如下：

1.本供应商自愿在采购文件规定的时限内按照采购文件及采购合同、用户需求书、技术规范等要求完成采购任务，按时按质完成服务。服务质量按照报价文件的承诺并满足采购文件要求。

2.遵守中华人民共和国的法律法规规定，自觉维护市场经济秩序。否则，同意被废除报价资格并接受处罚。

3.保证报价文件内容无任何虚假。若评审过程中查出有虚假，同意作无效报价文件处理，若成交之后查出有虚假，同意废除成交资格，存在此款虚假行为的，同意按采购方公司制度进行处罚。

4.保证报价文件不存在低于成本的恶意报价行为。

5.保证按照采购文件及成交通知书规定提交履约担保并商签采购合同，对采购文件第五部分《合同书》中的条款项下的内容完全响应，不作任何的偏离。

6.保证按照采购合同约定完成采购合同范围内的全部内容，否则，同意接受采购方对供应商违约处理。

7.保证成交之后不转包，若分包将征得询价人同意并遵守相关法律法规。

8.保证成交之后按采购文件要求配置承诺的资源，否则，同意接受违约处罚。

9.保证成交之后密切配合采购人开展工作，接受采购人的监督管理。

10.保证按采购文件及采购合同约定的原则处理采购调整事宜,不发生签署采购合同之后恶意索赔的行为。

本供应商在规定的报价有效期限内，将受采购文件的约束并履行报价文件的承诺。

供应商名称（加盖公章或电子签章）：

日期：　　年　　月　　日

附录 4

组织机构和人员

4.1 现场主要人员安排

供应商应列出拟在本项目中任职的主要管理人员和专业人员的安排，应包括项目负责人、专业负责人、投入本项目的主要人员等，详见如下表格（各表格可按供应商的情况扩展与扩充）：

本项目主要管理与技术人员安排（表一）

序号	职务	姓名	年龄	性别	职称	专业	主要资历简述
1	项目负责人						
2	项目实施人员						
3	主要人员						
4	其它主要人员（*） ……						

*指除表中提到的人员外，供应商认为有必要加入的其他方面的本项目主要管理与技术人员。

主要人员简历与经验（表二）

（至少列写 4 人）

姓名		性别		年龄		职务职称	
时 间	简历与经验简述						

注：项目负责人及专业负责人业绩须提供证明材料。

附录 5

供应商的类似业绩

项目	项目规模及内容	签订时间	合同价	备注

注：近 3 年内业绩（以合同签订日期为准）。

附录 6

企业资质证书表

供应商应列出资质证书，应附上相关证明材料。详见如下表格（各表格可按供应商的情况扩展与扩充）：

序号	证书名称	获奖时间	颁发单位备注
1			
2			
3			
……			

注：提供资质证书复印件。

附录 7

资格审查和报价文件有效性审查表

（注：采购单位可根据项目合格供应商资格要求进行调整）

项目名称：

序号	供应商名称 审查项目			
1	供应商为在中华人民共和国境内注册的独立的企业法人，并提供营业执照的复印件。			
2	广东省机场管理集团有限公司招标、采购管理平台供应商登记表并加盖公章			
3	供应商近三年没有因腐败或欺诈行为而被政府或业主宣布取消报价资格；同时，供应商（包括其关联公司）近三年未与广东省机场管理集团有限公司其下属的全资、控股公司、非法人实体单位发生各种诉讼或仲裁。（须就此项内容提供承诺函并加盖供应商公章）。			
4	供应商出具本采购公告发布后未被列入系统相关名录的截图并加盖公章。			
……				
5	有法定代表人证明书及法人授权书			
6	报价函有法定代表人或授权代表签字且加盖公章；			
7	报价有效期符合采购文件规定（90 个日历日）；			
8	报价没有超过最高限价；			
9	供应商递交一种报价方案和报价；			
结论	是否通过并进入下一阶段评审			

注：1.每一项目符合的打“〇”，不符合的打“×”，并在备注中说明理由。出现一个“×”的结论为“不通过”。

2.表中全部条件满足为“符合”的结论为“通过”，同意进入下一阶段评审。

3.若专家意见不一致时，则按少数服从多数的原则决定该供应商是否通过资格及有效性审查，进入下一阶段评审。

4.结论一栏应写“通过”“不通过”。

第五部分 用户需求书

1. 服务内容清单

序号	服务目录	服务内容	服务对象	频率	单位	备注
1	安全托管服务	详见服务要求	集团云数据中心	1	年	
2	漏洞扫描服务	详见服务要求	机场集团云数据中心	12	次/年	
3	安全加固服务	详见服务要求	机场集团云数据中心	1	年	
4	安全评估服务	详见服务要求	机场集团云数据中心	1	次	
5	安全培训服务	详见服务要求	机场集团	3	次/年	
6	重保值守服务	详见服务要求	机场集团	3	次/年	
7	应急响应服务	详见服务要求	机场集团	1	年	
8	渗透测试服务	详见服务要求	机场集团	12	系统	
9	新上线系统评估	详见服务要求	机场集团	12	系统	
10	抽检服务	详见服务要求	机场集团	6	次/年	
11	安全巡检服务	详见服务要求	机场集团	4	次/年	
12	驻场服务	详见服务要求	机场集团	1	次/年	

2. 评估依据:

服务过程中参考以下的国家技术标准,并结合机场集团的具体业务情况和上级主管部门的要求,包含如下:

- 《信息安全等级保护管理办法》
- 《信息安全技术 信息系统安全等级保护定级指南》(GB/T 22240-2008)
- 《信息安全技术 信息系统安全等级保护基本要求》(GB/T 22239-2008)
- 《信息系统安全等级保护测评要求》
- 《信息系统安全等级保护实施指南》
- 《信息系统安全等级保护测评过程指南》
- 《计算机信息系统安全保护等级划分准则》(GB17859-1999)
- 《信息安全技术 信息系统通用安全技术要求》(GB/T20271-2006)
- 《信息安全技术 网络基础安全技术要求》(GB/T20270-2006)
- 《信息安全技术 操作系统安全技术要求》(GB/T20272-2006)
- 《信息安全技术 数据库管理系统安全技术要求》(GB/T20273-2006)

- 《信息安全技术 服务器技术要求》(GB/T21028-2007)
- 《信息安全技术 终端计算机系统安全等级技术要求》(GA/T671-2006)

3. 服务的内容要求

3.1 安全托管服务

通过将广东机场集团安全设备接入安全托管中心，依托于安全能力平台和 MSSP 安全服务平台实现有效协同的“人机共智”模式，围绕资产、脆弱性、威胁、事件四个要素为广东机场集团提供 7*24H 的安全托管服务，扩展持续有效的安全运营能力，保障可承诺的风险管控效果；

服务类	服务类型	内容及要求
服务内容要求	资产识别与梳理	供应商需借助安全工具对采购方资产进行识别和梳理，并在后续服务过程中根据识别的资产变化情况触发资产变更等相关服务流程，确保资产信息的准确性和全面性
		供应商需结合安全工具发现的资产信息，首次进行服务范围内资产的全面梳理（梳理的信息包含支撑业务系统运转的操作系统、数据库、中间件、应用系统的版本，类型，IP 地址；应用开放协议和端口；应用系统管理方式、资产的重要性以及网络拓扑），并将信息录入到安全运营平台中进行管理；当资产发生变更时，安全专家对变更信息进行确认与更新
	安全现状评估	蠕虫病毒事件：供应商需确认文件是否被感染，定位失陷的代码并进行修复
		针对漏洞利用攻击行为、Webshell 上传行为、Web 系统目录遍历攻击行为、SQL 注入攻击行为、信息泄露攻击行为、口令暴力破解攻击行为、僵尸网络攻击行为、系统命令注入攻击行为及僵尸网络攻击行为进行分析评估，判断攻击行为是否成功以及业务风险点
		失陷主机分析：供应商需对失陷主机进行分析研判（如后门脚本类事件），并给出修复建议
		潜伏威胁分析：供应商需分析内网主机的非法外联威胁行为，判断是否存在潜伏威胁，并给出解决建议。含：对外攻击、APT C&C 通道、隐藏外联通道等外联威胁行为
	问题处置	供应商需对发现的问题进行处置，包含内网脆弱性问题，病毒类事件，入侵行为，勒索、挖矿类事件等

	脆弱性管理	脆弱性扫描与验证：供应商需提供不少于每月一次针对服务范围内的资产的系统脆弱性和 Web 漏洞进行全量扫描，并针对发现的脆弱性进行验证，验证脆弱性在已有的安全体系发生的风险及分析发生后可造成的危害
		优先级排序：供应商需提供客观的修复优先级指导，不能以脆弱性危害等级作为唯一的修复优先级排序依据。排序依据包含但不限于资产重要性、漏洞等级以及威胁情报（漏洞被利用的可能性）三个维度
		脆弱性验证：提供脆弱性验证服务，针对发现的脆弱性问题进行验证，验证脆弱性在已有的安全体系发生的风险及分析发生后可造成的危害。针对已经验证的脆弱性，自动生成工单，安全专家跟进修复状态，各个处理进度透明，方便采购方清晰了解当前脆弱性的处置状态，将脆弱性处理工作可视化
		修复建议：针对存在的漏洞提供修复建议，能够提供精准、易懂、可落地的漏洞修复方案
		服务催单：针对服务平台生成的工单，采购方可按需催单，用户可在服务平台上采用邮件等方式提醒安全专家加快协助处置，督促供应商第一时间处理
		脆弱性复测：需提供脆弱性复测措施，及时检验脆弱性真实修复情况。供应商要支持采购方可按需针对指定脆弱性问题，指定资产等小范围进行，降低脆弱性复测时的潜在影响范围
		脆弱性状态总览：对发现的脆弱性建立状态总览机制，自动化持续跟踪脆弱性情况，清晰直观地展示脆弱性的修复情况，遗留情况以及脆弱性对比情况，使得采购方可做到脆弱性的可视、可管、可控
		最新漏洞预警与排查：供应商需实时抓取互联网最新漏洞与详细资产信息进行匹配，对最新漏洞进行预警与排查。预警信息中包含最新漏洞信息、影响资产范围。
		最新漏洞处置指导：一旦确认漏洞影响范围后，安全专家提供专业的处置建议，处置建议包含两部分，补丁方案以及临时规避措施。
		最新漏洞复测与状态跟踪：由供应商对该最新漏洞建立状态追踪机制；跟踪修复状态，遗留情况。
	威胁管理	结合大数据分析、人工智能、云端专家提供安全事件发现服务：依托于安全防护组件、检测响应组件和安全平台，将海量安全数据脱敏，包括脆弱性信息、共享威胁情报、异常流量、攻击日志、病毒日志等数据，经由大数据处理平台结合人工智能和云端安全专家使用多种数据分析

		算法模型进行数据归因关联分析，实时监测网络安全状态,发现各类安全事件，并自动生成工单
		实时监测网络安全状态，对攻击事件自动化生成工单，及时进行分析与预警。攻击事件包含境外黑客攻击事件、暴力破解攻击事件、持续攻击事件
		实时监测网络安全状态，对病毒事件自动化生成工单,及时进行分析与预警。病毒类型包含勒索型、流行病毒、挖矿型、蠕虫型、外发 DOS 型、C&C 访问型、文件感染型、木马型
		供应商需针对每一类威胁，进行深度分析验证，分析判断是否存在其他可疑主机，将深度关联分析的结果通过邮件、微信等方式告知用户
		结合威胁情报，供应商需排查是否对用户资产造成威胁并通知用户，协助及时进行安全加固
		供应商需每月主动分析病毒类的安全事件：提供病毒处置工具，并针对服务范围内的业务资产使用病毒处置工具进行病毒查杀，对于服务范围外的业务资产，安全专家协助用户查杀病毒
		供应商需每月主动分析攻击类的安全事件：通过攻击日志分析，发现持续性攻击，立即采取行动实时对抗，当用户无防御措施时，提供攻击类安全事件的处置建议
		供应商需每月主动分析漏洞利用类的安全事件并验证该漏洞是否利用成功，提供工具协助处置
		供应商需每月主动分析失陷类的安全事件并协助用户处置，并提供溯源服务
		策略调配：新增资产、业务变更策略调优服务，业务变更时策略随业务变化而同步更新
		策略定期管理：供应商需每月对安全组件上的安全策略进行统一管理工作，确保安全组件上的安全策略始终处于最优水平，针对威胁能起到有效的防护效果
		实时针对异常流量分析、攻击日志和病毒日志分析，经过海量数据脱敏、聚合发现安全事件。
	事件管理	基于主动响应和被动响应流程，对页面篡改、通报、断网、webshell、黑链等各类严重安全事件客户可以在平台上直接发起服务咨询，云端进行紧急响应和处置

		针对分析得到的勒索病毒、挖矿病毒、篡改事件、webshell、僵尸网络等安全事件，通过工具和方法对恶意文件、代码进行根除，帮助采购方快速恢复业务，消除或减轻影响
		加固建议指导：结合现有安全防御体系，指导用户进行安全加固、提供整改建议、防止再次入侵
服务平台和用户 Portal		
		支持面向采购方的安全态势展示，展示出当前采购方遭受的威胁事件信息以及脆弱性信息统计，并支持服务专家按照资产类别、威胁类型进行定制化筛选查看，能直观感受到采购方当前的风险态势情况。
		服务平台支持面向采购方的安全报告与交付物管理，可生成、导出、下载各类安全报告，包括但不限于《安全服务值守日报》、《特殊时期值守报告》、《安全运营周报》、《安全运营月报》。 所有可导出报告支持按照自定义模块进行导出，可自定义模块必须包括但不限于事件管理、攻击威胁（外部攻击趋势、TOP5 攻击 IP 等）、脆弱性管理（漏洞、弱密码）。
		支持展示出当前工单数量和工单处置状态，使得采购方能详细查看服务处置过程，查看安全事件闭环效果，掌握当前专家服务进度，监督服务质量。
		支持展示出当前需要采购方审批的工单及其具体情况，使得采购方能完成与服务人员的协同处置，共同确保安全威胁和事件得到准确处置。
		平台支持对不同设备上报的日志进行格式泛化，以统一格式存储到大数据平台，为安全规则配置提供标准格式的数据。
	Use case（安全规则）管理	支持自定义配置安全规则，包括配置源算子、解析规则算子、关联规则算子、Flinksql 算子、union 算子、标签算子、kafka 算子、搜索引擎目的算子、自定义算子。通过组合不同算子，形成安全规则。
		支持所有安全日志均经过安全规则筛选，生成威胁告警信息。
		供应商服务平台已支持的安全检测规则应超过 1000 个，且覆盖内网脆弱性问题，病毒类事件，入侵行为，勒索、挖矿类事件等；
		为了保证安全监测的效果，供应商的服务平台应具备检测规则的自定义功能，以满足日益复杂的安全趋势所带来的安全需求
	报告中心	支持配置报告模板和下载报告文件，报告的类型有 pdf 格式报告和 word 格式报告。
		支持根据不同场景，灵活选择不同的组件组合形成新的报告模板，以便于采购方查看不同场景和维度的服务报告。可从时间范围，开始时间，

		结束时间、漏洞攻击，网络流量，恶意攻击，脆弱性等维度组合新的报告模板。下载报告时，选择相应场景的模板进行下载即可。
	平台管理	供应商在本项目使用服务工具应当支持将收集的安全日志上传到安全运营服务平台上，并支持在该平台上对服务工具进行管理
		平台应支持配置采购方的业务信息，将业务设置为高中低三个不同的等级。在每个业务下，配置业务的资产 IP 范围。
		服务平台应支持为采购方设置白名单，包括自动封锁白名单，策略白名单等。
		支持重大活动保障时期的备战阶段、实战阶段、演练结束三个阶段的指导性工作流程。
		平台支持使用 finebi 平台，自定义配置统计数据，包括告警数据，工单数据，工单平均处置时长等数据，来统计当前平台的运营效率，直观体现出当前运营能力，同时可对服务专家处置效率进行考核。
服务质量监督		业务安全状态监控： 供应商需为采购方提供服务监控门户（或用户 Portal，区别于安全感知大屏），在门户中采购方可查看业务和资产安全状态信息，使得采购方能直观感受到当前的业务和资产安全状态，展示纬度至少包括服务资产安全评级、服务运营状态及成果、安全风险概览、最新情报。
		服务质量监控： 供应商提供的服务监控门户（或用户 portal）应具备服务质量可视化展示，供应商能通过可视化的数据，清晰的了解安全专家的服务水平，至少包括脆弱性闭环率、脆弱性平均响应时长、脆弱性平均闭环时长、威胁闭环率、威胁平均响应时长、威胁平均闭环时长、事件闭环率、事件平均闭环时长，已验证供应商所承诺的服务 SLA。
服务水平协议 SLA		通过 SLA 对安全事件服务水平作出承诺： 1） 从安全日志产生到事件通告给采购方的时间方面，按照国家标准对安全事件的分类分级指南，重大安全事件通告时间小于 30 分钟，一般事件的通告时间少于 1 小时。 2）在未配备供应商的边界防护服务组件和终端防护服务组件的情况下，运营服务对于重大安全事件的遏制影响和处置完成时间小于 8 小时，对于一般事件的遏制影响和处置完成时间小于 24 小时。 2） 安全事件经过服务人员的确认后，各类安全事件的判断准确率不低于 99%。 3） 在配备了供应商的边界防护服务组件和终端防护服务组件的情况下，安全事件的闭环处置比例达到 100%。

	4） 对于重大事故应启动应急响应机制，工作时间 15 分钟之内云端专家进行响应，非工作时间 30 分钟之内云端专家进行响应，省会 2 小时上门处置，省内 8 小时上门处置。
	通过 SLA 对安全威胁服务水平作出承诺： 1） 从安全日志产生到威胁通告给采购方的时间方面，重大威胁的通告时间少于 1 小时，一般威胁的通告时间少于 2 小时。 2）在未配备供应商的边界防护服务组件和终端防护服务组件的情况下，高级威胁和一般威胁的处置完成时间少于 24 小时； 2） 安全威胁经过服务人员的确认后，高级威胁和一般威胁的判断准确率不低于 99%。 3） 在配备了供应商的边界防护服务组件和终端防护服务组件的情况下，高级威胁和一般威胁的闭环处置比例达到 100%。
	通过 SLA 对安全漏洞服务水平作出承诺： 1） 高危可利用漏洞从完成漏扫后发现到推送漏洞报告的时间少于 2 个工作日。 2） 高危可利用漏洞经服务人员确认后的准确率不低于 99%。 3） 高危可利用漏洞的防护率达到 99%。 4） 工作时间 15 分钟之内云端专家进行响应，非工作时间 30 分钟之内云端专家进行响应；
服务交付物	交付物名称：《安全服务运营报告》，报告频率：每周一次 交付物名称：《首次威胁分析与处置报告》，报告频率：一次 交付物名称：《事件分析与处置报告》，报告频率：按需触发，不限次数 交付物名称：《安全通告》，报告频率：按需触发，不限次数 交付物名称：《综合分析报告/运营月报》，报告频率：每月一次 交付物名称：《季度汇报 PPT》，报告频率：每季度一次 交付物名称：《年度汇报 PPT》，报告频率：每年一次 成交后采购方有权要求成交方严格按照上述频率要求提供服务交付物，确保满足采购方安全需求。如成交方未能按时提供，采购方有权终止服务合同，中间产生任何费用由成交方自行承担。
服务频率	7*24 小时持续专家服务，威胁发现及时响应，周期 1 年
服务覆盖资产数量	500 个服务端主机资产

3.2 漏洞扫描服务

主机漏洞扫描服务，使用漏洞扫描工具对企业网络中的 IT 资产开放的端口服务、漏洞进行扫描检测，检测的资产范围包含服务器、网络设备、安全设备。
web 应用漏洞扫描，涵盖对 SQL 注入、跨站脚本、表单风险、Cookie 安全、CGI 漏洞进行检测，识别无效链接、错误配置等，并生成检测报告。

服务类	技术类型	内容及要求
漏洞扫描	服务流程	**1、 漏洞扫描应按照以下要求实施：** **漏洞扫描服务流程：** ➢ 供应商应对漏洞扫描的目标对象进行全面梳理和识别，识别内容包含但不限于资产类型、IP 地址、业务部门、责任人、用途、操作系统、数据库、中间件等 ➢ 供应商应提交漏洞扫描工具的情况（包括但不限于：设备厂商、设备型号、漏洞库、销售许可证等）、漏洞扫描工作方案（包括但不限于：目标对象、扫描时间、风险规避措施等）及漏洞扫描申请，采购方授权后，方可进行 ➢ 供应商应对漏洞扫描结果进行人工验证，保证漏洞扫描结果的真实性 ➢ 供应商应提交针对性的解决方案，保证漏洞修复可落地。
	服务工具要求	**1、 漏洞扫描工具支持对象应包含但不限于：** ➢ 网络设备：路由器、交换机、防火墙等 ➢ 操作系统：windows、linux、UNIX 等 ➢ 数据库：Oracle、MS SQL、Mysql 等 ➢ 中间件：Apache、Tomcat、weblogic 等 **2、 漏洞扫描参数应包含但不限于：**版本漏洞、开放端口、开放服务、空/弱口令账户、安全配置等 **3、** 供应商提供的漏洞扫描工具应具备对高可利用漏洞的管理（需提供截图证明并加盖原厂商公章） **4、** 供应商提供的漏洞扫描工具应具备对扫描出或已修复的漏洞，具备一键复测功能（需提供截图证明并加盖原厂商公章） **5、** 支持越权漏洞检测技术能力（提供第三方权威机构出具的关于越权漏洞检测方法的证明文件并加盖原厂公章） **6、** 支持漏洞自动化防护技术能力（提供第三方权威机构出具的关于漏洞自动化防护方法的证明文件并加盖原厂公章）
服务频率	1 年 12 次	
服务交付	《漏洞扫描服务报告》	

物	

3.3 安全加固服务

通过自动化工具或人工对未过保的安全设备进行配置加固（涵盖身份认证、资源授权、访问控制、安全审计、恶意代码防范、资源控制、紧急补丁修复）

服务类	服务类型	内容及要求
服务内容	网络设备安全加固	对网络设备的管理员进行分级管理，权限更高的管理员的帐号和口令的管理要求必须保证是最严格等级，同时对其他管理员的帐号和口令的复杂度进行优化 对网络设备的登录帐号进行加固，使其满足一定强度的认证要求，并对不同级别的授权策略进行优化 网络设备的服务配置方面，必须遵循最小化服务原则，关闭网络设备不必要的所有服务，修复网络服务或网络协议自身存在的安全漏洞以降低网络的安全风险 针对网络设备管理设置访问安全限制策略，只允许特定主机访问网络设备 根据安全级别要求，开启网络设备必需的监控日志记录，并支持一定周期的日志本地存储或外置存储
	主机操作系统加固	对主机操作系统的管理员进行分级管理，确保不同管理员的帐号和口令的管理要求差异化，同时对帐号和口令的复杂度进行严格要求 确保主机操作系统的登录帐号达到一定强度的认证要求，并对不同级别的授权策略进行优化 主机操作系统的网络服务、进程和启动项配置方面，必须遵循最小化服务原则，关闭主机操作系统不需要的所有服务，降低网络服务或网络协议自身存在的安全漏洞带来的安全风险 严格把控每个文件/文件夹的访问权限，只允许授权的帐户访问此文件/文件夹 针对主机操作系统管理设置访问安全控制策略，只允许特定主机访问网络设备 按照安全级别要求，开启主机操作系统必需的监控日志记录，并支持一定周期的日志本地存储或外置存储
	数据库加固	根据数据库管理员的分级管理策略制定差异化的管理员帐号和口令的管理要求，对帐号和口令的复杂度进行优化配置 针对数据库的登录帐号进行一定强度的认证要求，以及对不同级别的

		授权策略进行优化调整 针对数据库管理设置访问安全访问限制策略，只允许特定主机访问网络设备 关闭不必要的服务，加固 TCP/IP 协议栈，使用加密通信协议 根据安全级别要求，开启数据库必需的监控日志记录，并支持一定周期的日志本地存储或外置存储
	中间件及常见网络服务安全加固	完成针对应用的管理员分级管理，不同管理员的帐号和口令的管理要求实现差异化，同时对帐号和口令的复杂度进行优化 针对应用的登录帐号进行一定强度的认证要求和不同级别的授权策略优化 根据安全级别要求，开启中间件及常见网络服务必需的监控日志记录，并支持一定周期的日志本地存储或外置存储
服务交付物	《安全加固方案》	《安全加固报告》的具体内容应包含： 1）对加固过程的详细记录 2）对加固结果的详细记录 3）对未能实施加固（残余风险）的风险项进行详细说明，并提出安全补救措施和安全专家建议，为管理人员的后期维护提供参考
服务频率	4 次/年	

3.4 安全评估服务

针对用户的信息系统及支撑信息系统的网络设备、安全设备、中间件、数据库等信息化资产，根据资产识别、脆弱性评估、威胁评估、防护能力评估的输出结果进行安全分析，为用户提供符合业务需求的安全整改建议。

服务类	技术类型	内容及要求
风险评估	资产识别	1、 依据相关国家标准或国际标准，对采购方的信息资产进行全面梳理和识别，识别内容包含但不限于资产类型、IP 地址、业务部门、责任人、用途、操作系统、数据库、中间件等 2、 资产识别方式包含但不限于：自研工具扫描探测、人工访谈调研和实地核查等 3、 资产类别应按照相关规范分类，包含但不限于以下几大类： ➢ 业务应用—业务信息系统，如 OA 系统、门户网站等 ➢ 网络结构—网络拓扑结构图 ➢ 文档和数据—业务信息系统相关文档、数据库数据、设计方案、操作手册、业务数据等

		➢ 软硬件资产—服务器设备、安全设备、存储设备、应用软件、操作系统、中间件、数据库、网络设备等 ➢ 物理环境—机房 ➢ 组织管理—方针、规章制度等 ➢ 人力资源资产--组织架构、岗位职责等 4、 依据相关规范，供应商应根据资产识别结果，科学、合理的对资产进行重要性赋值，明确资产价值 5、 供应商应针对资产识别情况及问题及时汇报
	脆弱性识别	1、 依据相关国家标准或国际标准，根据资产识别结果，采用不同手段对资产进行全面的脆弱性识别，及时发现、处置脆弱性，避免或降低脆弱性被威胁利用的几率造成的影响 2、 脆弱性分类应至少包括但不限于以下三类： ➢ 技术性弱点—系统、程序、设备存在的漏洞或缺陷，如网络结构设计问题和代码漏洞 ➢ 操作性弱点—软件和系统配置、操作中存在的缺陷，包括人员在日常工作中的不良习惯，审计和备份的缺乏 ➢ 管理性弱点--策略、程序、规章制度、人员意识、组织结构等方面的不足 3、 脆弱性识别方式包含但不限于:自研工具自动探测、人工访谈调研、文档审阅和实地核查等 4、 **漏洞扫描应按照以下要求实施：** **漏洞扫描服务流程：** ➢ 供应商应对漏洞扫描的目标对象进行全面梳理和识别，识别内容包含但不限于资产类型、IP 地址、业务部门、责任人、用途、操作系统、数据库、中间件等 ➢ 供应商应提交漏洞扫描工具的情况（包括但不限于：设备厂商、设备型号、漏洞库、销售许可证等）、漏洞扫描工作方案（包括但不限于：目标对象、扫描时间、风险规避措施等）及漏洞扫描授权申请，采购方授权后，方可进行 ➢ 供应商应对漏洞扫描结果进行人工验证，保证漏洞扫描结果的真实性 ➢ 供应商应提交针对性的解决方案，保证漏洞修复可落地 **漏洞扫描工具支持对象应包含但不限于：** ➢ 网络设备：路由器、交换机、防火墙等 ➢ 操作系统：windows、linux、UNIX 等

		➢ 数据库：Oracle、MS SQL、Mysql 等 ➢ 中间件：Apache、Tomcat、weblogic 等 **漏洞扫描参数应包含但不限于：**版本漏洞、开放端口、开放服务、空/弱口令账户、安全配置等 5、 **基线核查应按照以下要求实施：** **基线核查服务流程：** ➢ 供应商应对基线核查的资产进行全面梳理和识别，识别内容包含但不限于资产类型、IP 地址、业务部门、责任人、用途、操作系统、数据库、中间件等 ➢ 供应商应提交基线核查的标准，会同采购方各接口人进行沟通确认 ➢ 依据相关标准或规范，供应商应结合采购方制定的基线核查标准、上级单位的基线核查标准、行业基线核查标准及行业最佳实践等，目标对象进行核查，目标对象包括但不限于：网络设备、操作系统、数据库及中间件等 ➢ 供应商应组织相关人员对结果进行确认后，分析提交科学、合理的整改建议 **基线核查应包含但不限于以下内容：** ➢ 网络设备： OS 安全、帐号和口令管理、认证和授权策略、网络与服务、访问控制策略、通讯协议、路由协议、日志审核策略、加密管理、设备其他安全配置等 ➢ 操作系统：系统漏洞补丁管理、帐号和口令管理、认证、授权策略、网络与服务、进程和启动、文件系统权限、访问控制、通讯协议、日志审核功能、剩余信息保护、其他安全配置等 ➢ 数据库：漏洞补丁管理、帐号和口令管理、认证、授权策略、访问控制、通讯协议、日志审核功能、其他安全配置等 ➢ 中间件：漏洞补丁管理、帐号和口令管理、认证、授权策略、通讯协议、日志审核功能、其他安全配置等 6、 渗透测试应按照以下要求实施： 1）供应商应确定目标对象后提供渗透测试服务方案和渗透测试申请，内容必须包括但不限于： ➢ 渗透测试方法和流程 ➢ 渗透测试工具 ➢ 渗透测试面临的风险和规避措施 ➢ 渗透测试时间和地点

		➢ 渗透测试人员（资质、经验等其他证明） 2）采购方授权后，供应商应通过模拟黑客攻击行为通过本地或远程方式对目标对象进行非破坏性的入侵测试 3）渗透测试应至少包括以下方面的工作内容： ➢ WEB 应用系统渗透 ➢ 主机操作系统渗透 ➢ 数据库系统渗透 7、 供应商应将发现的脆弱性及时向采购方反馈，并在后续提出可落地的整改建议或方案。
	威胁识别	1、 依据相关国家标准或国际标准，对存在脆弱性的资产进行威胁的全面识别，及时发现潜在威胁的原因，避免或降低威胁发生的几率 2、 威胁来源应至少包括但不限于以下四类： ➢ 人员威胁——包括故意破坏和无意失误 ➢ 系统威胁——系统、网络或服务的故障 ➢ 环境威胁——电源故障、污染、液体泄漏、火灾等 ➢ 自然威胁——洪水、地震、台风、滑坡、雷电等 3、 通过技术手段识别服务器中可能存在被植入的后门程序、潜伏未触发的病毒木马等安全威胁 4、 供应商应对威胁利用率极高的风险提出整改建议，配合采购方及时处置
	防护能力评估	1、 依据相关国家标准或国际标准，对采购方现有的防护能力进行评估，评估内容包含但不限于： ➢ 预防控制措施情况，如：已有安全策略和防护程序情况、软件版本和补丁管理、安全域和访问控制、管理体系建设及落实、安全意识培训等 ➢ 检测控制措施情况，如：网络入侵检测能力、主机入侵检测能力、安全事件报告流程 ➢ 响应控制措施，如：应急响应机制、系统备份与恢复机制、安全事件响应能力等 2、 根据识别结果的现状，提出建设性意见，避免重复采购相关设备或服务。
	风险分析	1、 供应商应组织专家团队，对存在和潜在的风险进行全面分析，保证风险分析的科学性、合理性及风险处置的可操作性 2、 供应商应在风险分析完成后，组织召开相关会议，将风险评估实施过程全生命周期发现的情况或问题统一反馈，并提出可落地的建议

		或方案。
	可落地建设方案	1、 根据资产识别、脆弱性评估、威胁评估、防护能力评估的输出结果进行风险分析之后，通过自研平台输出风险评估报告，风险评估报告中应符合业务需求的安全整改建议。
服务工具要求	**一、 脆弱性检测工具要求** **1、 系统&WEB 漏洞扫描：** 支持对通用系统漏洞进行扫描，如：远程缓冲区溢出漏洞、远程拒绝服务攻击漏洞和远程代码执行漏洞等 支持行业通用标准 OWASP，支持通用 WEB 漏洞检测，如：SQL 注入、XSS、目录遍历、本地/远程文件包含漏洞、安全配置错误、已知漏洞组件包含、敏感信息泄露等 支持信息泄漏类漏洞检测，如：mail 地址、敏感目录暴露、内部 ip 地址、会话令牌、源码、数据库备份文件、SVN 文件、系统重要配置、日志文件向外网泄漏等 支持对新爆发的 0day 漏洞检测，如：struts s2-045 漏洞等 **2、 基线配置核查功能：** 支持多种规范库，如：等保基线规范、行业基线规范等 支持主流网络、安全设备：CISCO、华为、Juniper 等路由和交换设备，其他厂商设备：下一代防火墙、入侵检测设备、入侵防御设备等 支持主流操作系统：微软 Windows 系列操作系统，如 Windows server 2012 R2/2016/2019 等；各类 Linux 系列操作系统，Redhat、Ubuntu、Debian 等；各类 Unix 系列操作系统，Solaris、AIX、HP-UX、BSD 等 支持主流数据库：微软 MSSQL 系列，SQL Sever 2012/2014/2016 等；甲骨文 Oracle 系列，Oracle 12c/18c/19c 等其他数据库，MySQL、DB2、Sybase、Informix 等 常见中间件及网络服务应用：Web 服务类，IIS10.0、Apache、Tomcat、Weblogic、Nginx、WebSphere 等 DNS 服务类，MAIL、Proxy、POP3、SMTP 等 **3、 弱口令扫描能力：** 支持通用字典和行业专有字典，进行弱口令猜解 支持对多种服务协议弱口令猜解，如：ftp\rdp\ssh\telnet\Mysql\Mssql 等远程服务 **二、 服务平台要求：** 1、为了保障风险评估整体交付过程中的标准化，遵循风险评估规范的流程，本次服务检测工具和服务平台之间需有联动措施，提高服务效率。检测工具检测出来的结果可同步到服务平台，服务平台统一分析与展示 2、该平台具有的功能模块包括： ➢ 资产梳理：自带资产发现引擎，对采购方内部网络资产及发布在互联网上的资	

	产进行探测识别，结合第三方工具进行异构交叉验证后，并通过平台进行自动去重，最终交付人员实地核查，保证资产台账真实有效，交付人员结合业务真实情况通过服务平台对资产进行赋值并自动生成资产识别表； ➢ 弱点分析：通过脆弱性检测工具对资产实现漏洞扫描、WEB 漏洞扫描、基线核查、弱口令检测及渗透测试等工作后，将检测结果同步至服务平台，自动生成脆弱性识别表，为风险分析提供数据； ➢ 风险分析：根据相关标准和规范，服务平台集成威胁知识库、风险分值自动计算功能，对资产识别、弱点分析输出的结果进行综合分析； ➢ 报告生成：服务平台自动生成风险评估报告，风险评估报告全面展示各关键阶段的服务内容及存在的风险，并提供可落地的修复建议，指导后期安全规划建设，辅助采购方决策层决策整体安全建设； 3、成交后采购方有权要求成交方提供演示平台对服务平台进行功能演示（提供演示平台登录界面截图证明并加盖原厂公章），确保满足采购方安全需求。演示功能包含：资产梳理、弱点分析、风险分析、报告生成功能。发现虚假应标的行为将予以废标处理并保留对该供应商追究相关责任的权利。
服务频率	1 年 1 次，覆盖全量资产
服务交付物	《安全风险评估报告》

3.5 安全培训服务

提供不限于网络安全设备的配置使用、等保的知识培训、日常网络安全意识培训。

服务类	技术类型	内容及要求
意识培训	网站访问安全	了解日常访问网站时的注意事项，知道如何安全使用浏览器
	电子邮件安全	了解在使用电子邮件过程中，如何保障其安全以及防范钓鱼邮件方法
	通信安全	了解连接网络连接、短信通讯等相关的安全注意事项，提高员工在通讯时的防诈骗意识
	移动设备安全	了解在使用手机、U 盘等移动设备过程中的注意事项
	物理环境安全	了解工作环境安全和计算机的安全保密意识，提高员工日常工作中的安全意识
	IT 人员信息安全	帮助 IT 运维用户了解当前信息泄露、由于安全意识不足导致网站被攻击的风险，如撞库、勒索、挖矿等，增强员工安全意识，养成良好安全习惯

	密码安全	帮助企业员工更好地认知到密码安全的重要性，帮助员工具备更好的密码安全意识和良好习惯
	安全事件案例与视频	通过分析海量的安全事件案例，让客户理解信息安全的重要性，帮助客户建立良好的信息安全意识习惯，实战视频使员工对每个主题涉及的信息安全知识与预防措施有感性和理性的认知，从而细化员工的信息安全知识
意识验证	模拟钓鱼测试（可选）	通过模拟邮件钓鱼测试，帮助客户发现弱安全意识人员
	实战钓鱼测试（可选）	搭建钓鱼网站、邮件钓鱼等组合方式帮助客户筛选出安全意识薄弱人员，针对性提升信息安全意识
	现场实战演示（可选）	通过现场演示点击链接文件导致用户电脑被黑客控制加强学员对信息安全意识不足导致危险的直观认知
服务工具	服务期间，要求供应商使用自研的信息安全意识培训教材包、信息安全意识培训素材包、安全意识验证教材包	
服务频率	1 年内提供 3 次安全培训服务	
服务交付物	《信息安全培训教材》 《信息安全培训记录》	

3.6 重保值守服务

针对国家重大活动、重要节日期间提供远程或现场值守服务，分析安全设备日志及流量，及时发现异常攻击流量，并进行下一步的防御措施，形成值守报告。（春节、建党、国庆）

服务类	服务类型	内容及要求
重保值守服务内容	响应事件范围	供应商应在采购方遇到重大节日或者重要时期提供线上及线下的值守服务，保障采购方在重要时期的网络安全，避免出现安全事件。 供应商应提供以下保障服务: ➢ 提供现场保障人员； ➢ 提供安全值守方案； ➢ 基于现有网络安全设备进行安全监测值守； ➢ 补充必要的安全设备； ➢ 应对突发安全事件； ➢ 提供防守及溯源报告； ➢ 提供重保值守的总结
服务频率	大于 3 次，至少覆盖春节、国庆、建党等重要时期，涵盖国家及省内组织的攻防演	

	练；
服务交付物	《安全事件总结报告》 《安全值守报告》

3.7 应急响应服务

对于各类可能发生的安全事件，如 web 入侵：网页挂马、主页篡改、Webshell；系统入侵：病毒木马、勒索软件、远控后门；网络攻击：DOS 攻击、ARP 欺骗。提供全面的应急支撑服务，包含现场应急和远程技术支持。

服务类	服务类型	内容及要求
服务内容	响应事件范围	供应商应在采购方遇到重大或突发事件后按照要求的服务响应级别采取相关的措施和行动。帮助采购方正确应对安全事件，降低安全事件带来的损失和影响，并将业务以及网络恢复到正常状态 本次采购的应急响应包含但不限于以下几类安全事件： ● WEB 安全事件 针对 B/S 类信息系统或网站遭受恶意入侵，利用网站进行反动信息、赌博、黄色等信息发布，传播危害国家安全、社会稳定和公共利益的内容的安全事件，包括但不限于：篡改、暗链、挂马、Webshell 等 ● 恶意程序事件 针对遭受的各类恶意程序事件进行快速处置，包括不限于病毒事件/木马事件、蠕虫事件、僵尸网络事件、勒索病毒事件、挖矿病毒事件等 ● 网络攻击事件 针对采购方由于信息系统的配置缺陷、协议缺陷、程序缺陷，造成的信息系统异常的安全事件进行应急响应 ● 信息破坏事件 针对采购方信息系统中的信息被篡改、假冒、泄漏、窃取等而导致的信息安全事件进行应急响应，包括但不限于系统配置遭篡改、数据库内容篡改、网站内容篡改事件、信息数据泄露事件等 供应商应按以下要求及时提供应急响应服务: ➢ 接到事件报告 ➢ 根据事件级别进行不同级别的响应方式，包括电话、现场等 ➢ 协调其他外部资源进行处理

		➢ 安全事件溯源分析服务 ➢ 编制应急响应情况报告，说明事件原因、处置措施等
	响应时间要求	供应商应提供 7*24 应急响应服务，提供应急响应服务方案 安全事件要求应急团队须在 5 分钟内，对信息安全事件做出响应，并严格按照采购方信息安全等级要求迅速到达现场并解决问题： ➢ 特别重大事件（Ⅰ级），5 分钟作出响应，提供远程 7*24 小时响应服务、1 小时到达现场进行应急响应服务 ➢ 重大事件（Ⅱ级），10 分钟作出响应，提供远程 7*24 小时、2 小时到达现场进行应急响应服务 ➢ 较大突发事件（Ⅲ级），30 分钟作出响应，提供远程 7*24 小时响应服务、4 小时到达现场进行应急响应服务 ➢ 一般性突发事件（Ⅳ级），30 分钟作出响应，提供远程 7*24 小时响应服务、远程无法解决时，在 4 小时到达现场进行应急响应服务 每次故障处理完毕 3 个工作日内提供详细的故障处理报告
服务频率	1 年内提供不少于 6 次安全应急响应服务	
服务交付物	《应急响应报告》 《安全加固报告》	

3.8 渗透测试服务

可提供黑盒和白盒测试，采用自动化漏洞扫描工具和人工对系统进行安全测试，提供针对操作系统、数据库、web 服务以及 web 应用的渗透服务，挖掘系统、数据库、web 框架等漏洞，例如 XSS、SQL 注入、跨站脚本、弱口令、缓冲区溢出、文件上传、认证会话管理、文件包含、敏感信息泄漏、未授权访问等。

服务类	技术类型	内容及要求
渗透测试	服务要求	1、供应商应保证采购方信息系统正常运行前提下，模拟黑客攻击行为通过远程或本地方式对信息系统进行非破坏性的入侵测试，查找针对应用程序的各种漏洞，帮助采购方理解应用系统当前的安全状况，发现在系统复杂结构中的最脆弱链路并针对安全隐患提出解决办法，切实保证信息系统安全 2、供应商应在得到客户授权后方可开始实施渗透工作。
	服务方案	1、供应商应根据采购方安全需求及重要业务系统结构，设计针对性的渗透测试方案，并提交至采购方进行评审 2、供应商应在采购文件技术部分详细说明渗透测试的实施流程、渗透

		测试方法、实施过程中用到的工具、实施过程中可供考量的具体工作指标及各阶段输出成果 3、供应商提供的渗透测试方案必须包括但不限于： ➢ 渗透方法和流程 ➢ 渗透测试风险评估和控制方案 ➢ 渗透测试须采用国内外商业检测工具或自有检测工具 ➢ 提供渗透测试所面临的主要风险及相应的风险规避措施
	服务内容	1、采购方授权后，供应商应通过模拟黑客攻击行为通过本地或远程方式对目标对象进行非破坏性的入侵测试 2、渗透测试应至少包括但不限于以下范围的漏洞： ➢ WEB 应用系统渗透 ➢ 主机操作系统渗透 ➢ 数据库系统渗透 3、渗透测试内容包括但不限于： ➢ 身份验证类 ➢ 会话管理类 ➢ 访问控制类 ➢ 输入处理类 ➢ 信息泄露类 ➢ 第三方应用类 4、供应商渗透测试人员应针对使用不同技术手段发现不同纬度的漏洞，并进行验证，形成记录和报告 5、供应商应编写渗透测试报告并提交给采购方，报告应该阐明采购方业务系统中存在的安全隐患以及专业的漏洞风险处置建议
服务频率	1 年 12 个系统	
服务交物	《渗透测试报告》	

3.9 新上线系统评估

针对服务范围内，新开发上线的业务系统，进行网络、应用及配置层面的安全评估，识别业务系统潜在的漏洞及风险，提供解决方案建议，避免系统带病上线。

服务类	技术类型	内容及要求
渗透测试	服务要求	针对在服务周期内上线的业务系统提供上线前的综合安全评估，评估内容包括系统的网络及应用配置安全、系统的业务逻辑安全，识别业

		务系统潜在的安全漏洞。
	服务内容	1、采购方授权后，供应商应通过模拟黑客攻击行为通过本地或远程方式对目标对象进行非破坏性的入侵测试 2、配置项目检查至少包含以下内容： ➢ 网络设备： OS 安全、帐号和口令管理、认证和授权策略、网络与服务、访问控制策略、通讯协议、路由协议、日志审核策略、加密管理、设备其他安全配置等 ➢ 操作系统：系统漏洞补丁管理、帐号和口令管理、认证、授权策略、网络与服务、进程和启动、文件系统权限、访问控制、通讯协议、日志审核功能、剩余信息保护、其他安全配置等 ➢ 数据库：漏洞补丁管理、帐号和口令管理、认证、授权策略、访问控制、通讯协议、日志审核功能、其他安全配置等 ➢ 中间件：漏洞补丁管理、帐号和口令管理、认证、授权策略、通讯协议、日志审核功能、其他安全配置等 3、渗透测试内容包括但不限于： ➢ 身份验证类 ➢ 会话管理类 ➢ 访问控制类 ➢ 输入处理类 ➢ 信息泄露类 ➢ 第三方应用类 4、供应商评估测试人员应针对使用不同技术手段发现不同纬度的漏洞，并进行验证，形成记录和报告 5、供应商应编写评估测试报告并提交给采购方，报告应该阐明采购方业务系统中存在的安全隐患以及专业的漏洞风险处置建议
服务频率	1 年 12 个系统	
服务交物	《新上线系统评估测试报告》 《新上线系统评估复测报告》	

3.10 抽检服务

协助机场管理集团落地对下属机场的监管职责，定期对下属机场进行网络安全抽样检查，验证机场的网路安全建设效果，检查范围包括不限于：合规基线检查、高危漏洞检查、弱口令检查；

服务类	技术类型	内容及要求
抽检服务	服务要求	1、 依据机场管理对支线机场的管理要求,采用不同手段对支线机场指定资产进行合规性检查、高危漏洞检查、弱口令检查，及时发现、处置脆弱性，避免或降低脆弱性被威胁利用的几率造成的影响 2、 抽检方式包含但不限于:自研工具扫描探测、人工渗透测试、文档审阅和实地核查等 3、 **抽检应按照以下要求实施：** **抽检服务流程：** ➢ 供应商在采购方下发抽检任务后，提交扫描工具的情况（包括但不限于：设备厂商、设备型号、漏洞库、销售许可证等）、扫描或者渗透攻击工作方案（包括但不限于：目标对象、扫描时间、风险规避措施等）及漏洞扫描授权申请，采购方授权后，方可进行 ➢ 供应商应对扫描结果进行人工验证，保证扫描结果的真实性 **漏洞扫描工具支持对象应包含但不限于：** ➢ 指定的业务系统或者网站 ➢ 网络设备：路由器、交换机、防火墙等 ➢ 操作系统：windows、linux、UNIX 等 ➢ 数据库：Oracle、MS SQL、Mysql 等 中间件：Apache、Tomcat、weblogic 等。
服务频率	1 年 6 次	
服务交付物	《XX 机场安全抽检报告》	

3.11 安全巡检服务

对机房及网络中主机服务器、安全设备等对象的运行状态、硬件资源占用状态、系统日志、安全日志、安全策略、授权状态、配置备份等进行巡检，分析可能存在的安全风险，并提出合理建议。

服务类	服务类型	服务项	服务描述
安全巡检服务	安全巡检	日常巡检	驻场运维人员需定期查看设备（包含但不限于：防火墙、AC、数据库审计、IDS、IPS、WAF、防病毒、VPN、堡垒机、态势感知）的运行状况、分析设备运行日志，发现网络中潜在的安全

			威胁并及时进行处理，输出巡检结果及维护记录。
		设备升级	驻场运维人员需在设备系统软件或特征库新版本发布后，协助用户完成设备系统的升级，实现对新的安全威胁进行检测。
		配置备份	驻场运维人员需定期对安全设备配置进行备份，为防止在设备在配置策略或升级补丁过程中出现系统异常的情况，均应在配置之前进行一次完整的系统备份，以便在系统发生故障后能够迅速恢复正常；
		故障处置	驻场运维人员需对信息安全产品发生的故障进行处置，输出设备故障处理报告。
	采购方支持服务	技术支持服务	1、供应商人员按需对安全设备(包含但不限于 AF、AC、VPN、态势感知、潜伏威胁探针、数据库审计等)等相关产品的实施方案或部署变更方案的编写，实施或变更方案要具备一定的风险说明，如网络或业务中断时长、并说明回退操作或措施 2、完成协助采购方对日常网络故障问题进行诊断与处理、以及软件升级及设备变更等现场服务
		应急资源保障	1、当采购方发生故障问题需要产品专家、研发、或安全专家协助时，驻场人员主动为采购方升级服务响应级别，采取专人专线，并第一时间协调专家、研发进行远程支持；紧急情况需要现场支持，则由区域产品专家进行现场支持。
		关键保障服务	1、在业务关键期、重要活动、重大会议期前完成事前安全巡检、事中值守保障、事后总结汇报的工作 2、驻场人员提前完成与采购方需求沟通，并制定安全巡检方案，针对采购方的安全产品由驻场人员主动联系相关厂商进行安全设备的巡检和优化工作
服务工具	巡检工作周期内，要求供应商使用自研工具： 1、主机漏洞扫描工具 2、WEB 漏洞扫描工具 3、弱口令扫描工具 4、基线核查工具 5、应急响应之病毒查杀工具 6、应急响应之流量分析工具		
服务频率	安全巡检至少 4 次；		
服务交	《安全巡检报告》每季度一次		

付物	《应急响应报告》按需提供 《设备实施方案》按需提供 《设备软件升级方案》按需提供 《设备部署变更方案》按需提供

3.12 驻场服务

提供专人，以驻点采购方指定地点的方式提供安全服务，协助业主完成自身及监管单位下发的网络安全任务。

服务类	服务类型	服务项	服务描述
驻场服务	安全检查	日常检查	驻场服务人员需定期查看网络安全设备告警状态，结合网络安全风险评估，分析整体网络运行的安全情况，识别网络内的潜在安全风险，为采购方提供风险处置意见，协助调整网络安全策略，规避网络安全风险。
		事件响应	关注网络安全日志及告警，关注监管单位的预警和通告，实时处理网络安全事件，响应监管单位下发的要求。
	采购方支持服务	技术支持服务	供应商人员按需响应采购方的网络安全事件处置需求，包括不限于执行定向网络安全检查，执行网络安全任务，协助安全设备厂商进行设备的上下架，调整对应的网络安全策略等。
服务工具	驻场工作周期内，要求供应商使用自研工具： 1、基础的扫描工具； 2、病毒查杀工具； 3、流量分析工具；		
服务频率	每周驻场 2 天以上；		
服务交付物	《安全驻场服务报告》每季度一次 《XX 安全任务执行报告》按需		