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

采购人：广东省机场管理集团有限公司

2020 年 12 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“采购人”）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“报价人”）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：集团本部信息安全服务。

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	数量	采购最高限价
1	信息安全服务	1 项	人民币：玖拾叁万元
合计			人民币：玖拾叁万元

注：1）报价人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	服务项	服务内容说明	服务对象	服务周期/频率	备注
1	安全评估服务	详见服务要求	集团本部涉及到的资产	1 次/年	
2	漏洞管理服务	详见服务要求	集团本部涉及到的资产	6 次/年	
3	新系统上线评估服务	详见服务要求	集团本部涉及到的资产	2 个系统/年	
4	渗透测试服务	详见服务要求	集团本部指定系统	2 个系统/年	
5	安全加固服务	详见服务要求	集团本部涉及到的资产	1 年	
6	安全运维及应急服务	详见服务要求	集团本部涉及到的资产	1 年	
7	安全培训服务	详见服务要求	集团本部涉及到的资产	1 次/年	
8	重点时期的安全值守服务	详见服务要求	集团本部	2 次/年	
9	安全态势感知服务	详见服务要求	集团本部	1 年	包括安全态势感知平台硬件工具

10	工单服务	详见服务要求	集团本部	1 年	包括工单系统软件或硬件
11	等级保护（二级）测评及技术整改服务	详见服务要求	财务系统、OA 系统、物资网、官网、邮件系统	5 个系统	
12	网站云防护	详见服务要求	物资网、官网	1 年	

3、 合格报价人资格条件：

3.1 在中华人民共和国境内注册的独立的企业法人，并提供加盖公章的营业执照的复印件。

3.2 报价人近三年没有因腐败或欺诈行为而被政府或业主宣布取消投标资格；同时，报价人（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报价人公章，格式样版见附录 3）。

3.3 报价人出具本采购公告发布后未被列入以下系统相关名录的截图并加盖公章：

1）国家企业信用信息公示系统（http://www.gsxt.gov.cn/）的经营异常名录或严重违法失信企业名单（截图格式要求详见附录 8）；

2）信用中国（http://www.creditchina.gov.cn/）的失信被执行人或企业经营异常名录（截图格式要求详见附录 9）；

3）中国执行信息公开网（http://zxgk.court.gov.cn/）的全国法院失信被执行人名单（截图格式要求详见附录 10）。

3.4 法定代表人（或负责人）为同一人或者存在控股、管理关系的不同单位，不得参加同一项目报价，否则全部取消资格。

3.5 未被广东省机场管理集团有限公司或其下属机构列入拒绝合作名单。

3.6 本项目不接受联合体报价。

4、 报价登记及获取采购文件

登记时间为 2020 年 12 月 24 日至 2020 年 12 月 31 日（节假日除外）的上午 9：30～11：30，下午 14：00～16：00（北京时间），由报价人代表将登记函（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人邮箱（lizexiong@gdairport.com）进行登记及获取采购文件，逾期可不受理。采购人将在收到邮件后 2 个工作日回复，并向报价人发出采购文件。

在规定的登记期间，登记的报价人不足 3 名时，采购人将发布公告延长接受登记时间。在延期登记时间内，已登记报价人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，登记的报价人仍不足 3 名时，采购人将变更采购方式。

5、 报价文件的提交形式、地址和截止时间

1） 报价人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：2020 年 12 月 31 日，16:30。（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） 采购人不接受以邮件、电话、传真等形式的报价。

6、 本项目不设未成交报价人经济补偿，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报价人自理。

7、 有关此次采购之事宜，可按下列联系方式向采购人咨询：

采购人：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

报价人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 报价人（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	数量	采购最高限价
1	信息安全服务	1 项	人民币：玖拾叁万元
合计			人民币：玖拾叁万元

2）服务内容：

序号	服务项	服务内容说明	服务对象	服务周期/频率	备注
1	安全评估服务	详见服务要求	集团本部	1 次/年	
2	漏洞管理服务	详见服务要求	集团本部	6 次/年	
3	新系统上线评估服务	详见服务要求	集团本部	2 个系统/年	
4	渗透测试服务	详见服务要求	集团本部指定系统	2 个系统/年	
5	安全加固服务	详见服务要求	集团本部	1 年	
6	安全运维及应急服务	详见服务要求	集团本部	1 年	
7	安全培训服务	详见服务要求	集团本部	1 次/年	
8	重点时期的安全值守服务	详见服务要求	集团本部	2 次/年	
9	安全态势感知服务	详见服务要求	集团本部	1 年	包括安全态势感知平台硬件工具
10	工单服务	详见服务要求	集团本部	1 年	包括工单系统软件或硬件

11	等级保护（二级）测评及技术整改服务	详见服务要求	财务系统、OA 系统、物资网、官网、邮件系统	5 个系统	
12	网站云防护	详见服务要求	物资网、官网	1 年	

注：1、报价人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。

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定之日起一年内

1.3.2 报价人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 报价人所提供的工作方案必须详细、完整、可靠、可行性强。

1.3.4 报价人报价中的服务费应是报价人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 报价人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 现场考察由报价人自行前往，采购人不统一安排。报价人若需相关数据，须自行测量。

2 定义

2.1 本文件中下列术语定义为：

服务： 指报价人提供信息安全服务相关技术支持。

报价人： 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。

采购人： 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报价人签订。

3 合格的报价人

3.1 合格的报价人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

报价人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，采购人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 报价人须知
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 报价人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。报价人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报价人的项目报价文件将被拒绝。

7 采购文件的澄清

7.1 采购人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，采购人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）通知所有报价人，该通知内容作为采购文件的组成部分。

7.2 报价人对采购文件有异议的，应当在 2020 年 12 月 31 日 16：30 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人邮箱（lizexiong@gdairport.com)。采购人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报价人发送，该答复作为采购文件的组成部分。

7.3 采购人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**，采购人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发送给所有报价人，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 为使报价人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，采购人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 报价文件由商务文件和技术文件两部分组成。各部分文件应分别编制，并密封包装。

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报价人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。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 商务文件（含资格审查文件）编制要求

11.1 商务文件由下列资料组成：

1） 封面：写明项目名称、商务文件、报价人名称及年月日；加盖报价人公章。
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） 报价人没有因腐败或欺诈行为，与采购人无发生各种诉讼、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）报价人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 技术文件编制要求

12.1 技术文件（技术服务方案）内容包括：

1） 目录。
2） 项目说明书（项目概况及报价人对项目的理解）。
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） 报价人认为有必要提供的其他资料。

6） ……

12.2 商务文件及技术文件密封要求：供应商应确保商务文件及技术文件密闭封装，可单独封装亦可合并封闭，用不透明包装物包装密封，外面标注“项目名称”、“报价人名称”及“报价文件”“报价人联系电话”“报价人邮箱”字样，若单独封装，应分别标注“商务文件”、“技术文件”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，并在封口处加盖报价人公章。

13 计算机文件

13.1 报价人必须随技术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 格式或 PPT 格式制作的电子版商务文件（资质文件和证书等可用扫描以图片方式保存）和技术文件。

2) 一套 WORD 格式的电子版文本文件。

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”，与报价文件正本一起密封包装。

14 知识产权和专利权

14.1 报价人应保证，采购人在中华人民共和国使用报价人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 如采购人向报价人提供图纸、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，除非得到采购人的同意，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，采购人可征求报价人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。报价人可以拒绝采购人的这种要求。

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，则是报价人的风险。

17.2 对报价人须知 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报价人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，报价人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 报价人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 如果报价人递交的报价文件未按要求密封，采购人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，采购人概不负责。

19 递交报价文件截止时间

19.1 报价人应将正本和所有副本，由报价人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 采购人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，采购人和报价人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 采购人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 采购人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人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、报价人是否符合合格条件、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“合格的报价人”要求；
2) 报价有效期符合采购文件规定；
3) 报价人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报价人少于 3 名，本次采购失败，采购人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 20%，商务技术部分得分占 80 %，详细评分标准

如下：

1）商务技术评分表

序号	项目	分值	评分标准
1	企业资质	3	投标人为国家信息安全漏洞共享平台(CNVD)技术组成员，同时也是国家信息安全漏洞共享平台(CNVD)用户组成员的 3 分，只具备一项得 1 分，不具备不得分；
		3	投标人具备软件研发实力需通过 CMMI L3 认证的得 1 分，CMMI5 的得 3 分；没有不得分；
		3	投标人同时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）、软件开发服务资质的得 3 分，具备其中部分的得 1 分，不具备不得分；
2	财务状况履约能力	3	2019 年盈利超过 6 亿元得 3 分，2019 年盈利有盈利得 1 分，其它 0 分 (需提供 2019 年度经第三方审计的财务报表)
3	企业 类似 业绩	5	自2017年起(以合同签署时间或中标通知书发出时间为准)，投标人完成过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。 注：要求提供以合同关键页复印件或中标通知书复印件为准
4	项目负责人	4	报价人为本项目指定的项目负责人需同时具有以下资质的，全部具备的得4分，不完全具备，但有两项以上的的2分，一项的得1分，没有，不得分： CISSP 资质； CISA 资质； CISAW 资质； CCSK 资质； PMP 项目管理证书； 软考系统集成管理管理师； 软考系统集成项目管理工程师；
5	项目团队实力	6	具有 CISP，得 1 分； 具有 CISSP，得 1 分； 具有 PMP，得 1 分； 具有 Security+证书，得 1 分。 本项合计最高得 6 分，一人拥有多个证书不重复计分。须提供该项目人员在本公司任职的相关证明材料（如社保参保证明、单位代缴个人所得税税单等）复印件。
6	安全服务能力要求	40	提供的服务满足用户需求书中的服务要求，对用户需求书中的“▲”项进行实质响应，完全满足得满分，一个“▲”号项不满足扣2分，扣完为止。

7	本地服务支撑能力	3	报价人总部设在广东省，得3分； 投标人总部不在广东省，但在广东省设有固定的自有技术服务机构得1分； 其余不得分 提供营业执照复印件或租赁合同。上述两项不重复计算。
10	服务方案内容广度、深度、可行性	10	1、报价文件对该项目具有深入的理解、分析透彻，预测合理；评估科学、合理；报价方案内容论述完整、全面、清楚；质量管理及保证措施合理；合理化建议针对性和可操作性强。满足询价文件用户需求书对咨询服务方案的广度、深度和可行性要求的，得7-10分； 2、报价文件对该项目程具有一定的理解、分析准确，预测合理；评估有一定的科学、合理性；报价方案内容论述完整；质量管理及保证措施合理；合理化建议有一定可操作性。基本满足询价文件用户需求书对咨询服务方案的广度、深度和可行性要求的，3-6分； 3、报价文件难以满足询价文件用户需求书对咨询服务方案的要求，可行性差，实施难度大的，得0-3分。
总分		80	

2）价格评审细则：价格分满分 20 分，各报价人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报价人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 20 分；

（3）当报价高于基准价时，按每高 1%的在 20 分基础上扣 1.5 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 20 分基础上扣 1 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 成交报价人的确定

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报价人为第一成交候选人，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 名的报价人为成交候选人。如出现总得分相同，评审价低者排名靠前，若评审价仍相同，则由评审小组投票，按少数服从多数原则确定报价人排名先后。

26.2 采购人根据评审小组的推荐，确定本项目成交报价人。

27 与采购人的接触

27.1 除报价人须知的相关规定外，从报价文件截至之日起至授予合同期间，未经采购人书面要求，报价人不得就与其项目报价文件有关的事项与采购人联系。

27.2 报价人试图对评审小组的评审或采购人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 采购决定将考虑报价人的财务、服务能力等，其基础是审查报价人提交的资格证明文件和其它采购人认为必要的、合适的资料。

28.2 如果审查通过，则将合同授予符合第 33.1 条规定的报价人；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报价人中，综合得分次高的报价人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 采购人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、综合得分最高的报价人。

30 授予合同时更改采购服务数量的权力

30.1 采购人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 采购人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，对受影响的报价人不承担任何责任，也无义务向受影响的报价人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，采购人将经过采购人确认的成交通知书以书面形式通知成交报价人。

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 成交报价人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） 采购人的澄清文件
（4） 第五部分 用户需求书
（5） 报价人的报价文件

33.3 如果成交报价人没有按照上述第 33.1 条规定执行，采购人将有充分理由取消该成交决定。在此情况下，采购人可将合同授予其他满足采购要求的报价人，或重新组织采购。

34 成交结果通知

34.1 采购人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，并于公示完毕后 14 个工作日内向成交报价人发出《成交通知书》。

第三部分

合 同 条 款

合同编号：

信息安全服务采购合同

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

委托方（甲方）：广东省机场管理集团有限公司

受托方（乙方）：

签订时间：　年　月

签订地点：广州市

本合同甲方委托乙方就广东省机场管理集团有限公司信息安全服务项目提供技术服务，并支付技术服务报酬。双方经过平等协商，在真实、充分地表达各自意愿的基础上，根据《中华人民共和国合同法》的规定，达成如下协议，并由双方共同恪守。

第一条 乙方进行技术服务的内容、要求和方式：

1、服务内容：

甲方委托乙方对安保公司提供信息安全服务，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，乙方应按甲方的要求进行及时的改进。

（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。

（3）服务期限要求

项目服务期限为一年，自　　年　月　日至　　年　月　日，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；

（2）乙方完成相应服务报告正式文本的修改，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）乙方对甲方为完成实施信息安全服务而提供的任何技术资料、数据或其他工作成果负有保密义务，应妥善保管，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、乙方提交技术咨询工作成果的内容：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》、《信息安全管理体系制度》、《信息安全技术体系标准》等服务过程中的文档。

2、技术咨询工作成果的验收标准：经甲方组织的评审会评审通过。

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：_____；

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）合同签订后，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　　万元整（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　　万元整（小写：　　元）。

（3）乙方完成全部服务内容，并按甲方要求办理完结算手续，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 40%，即人民币　万元整（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：

公司名称： 广东省机场管理集团有限公司

纳税人识别号： 91 440 000 190 488 448J

开户银行： 工商银行广州市机场支行

银行帐号： 360 206 520 900 039 6878

公司地址： 广东省广州市白云区机场路 282 号

联系电话： 020-86134626

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

（一）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和支付上述逾期违约金外，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。

（二）乙方应确保交付的成果通过甲方验收，否则甲方有权拒收，乙方应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和支付上述逾期违约金外，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。

（三）本合同履行期限内，乙方不得委托任何第三方完成本合同委托事项，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。

四）乙方未经甲方同意未按项目报价文件提供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；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、调解解决。协商、调解不成的，任何一方可向广州市白云区人民法院提起诉讼。

第八条 任何一方由于不可抗力原因不能履行合同时，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 陆 份，甲方执 叁 份，乙方执 叁 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。

第十一条 本合同到期后，若双方无异议，则合同自动顺延一年。

附件：《用户需求书》

（本页为盖章页，无正文）

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）

法定代表人或其授权代表：_____（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。

报价人名称（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：	

报价人名称（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：信息安全服务项目

致: 广东省机场管理集团有限公司

根据贵方为信息安全服务项目采购的邀请函，作为经报价人正式授权代表报价人_____ _____(报价人名称和地址)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) 报价人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) 报价人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, 报价人必须放弃在此方面提出含糊意见或误解的一切权力。
4) 报价人之报价文件有效期为自报价之日起90 个日历日。
5) 报价人同意按照采购人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。

S

报价人名称： _____（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				

报价人名称：_____（盖公章）

法定代表人或授权代表签名：_____

日期：_____

附录 3 诚信承诺函及企业声明

3.1 诚信承诺函

致：广东省机场管理集团有限公司

我司承诺我司（包括独立法人及关联公司和自然人）不存在以下情况，如有造假行为，我公司愿意无条件接受采购人的以下处理：

1.近三年，我司没有因腐败或欺诈行为而被政府或业主宣布取消投标资格；

2.近三年，我司（包括其关联公司）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；

3.我司非联合体报价。

上述承诺如有造假行为，我司愿意无条件接受采购人的以下处理：

1.取消本项目报价、成交资格，并在相关网站公示；

2.由采购人没收合同履约保证金；

3.三年至六年内停止或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.对不良行为予以纪录，并进行公告；

5.报广东省机场管理集团有限公司备案；

6.其他行政处理决定。

报价人名称：_____（盖公章）

法定代表人或授权代表签名：_____

日期：_____

3.2 企业声明

企业声明

致：

我公司就参加信息安全服务项目，作出郑重声明：

在项目采购、实施、运行过程中严格遵守贵公司相关管理规定。承诺如违反，将自愿接受：通报批评，记录不良行为，列入黑名单，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。特此声明！

报价人名称：_____（盖公章）

法定代表人或授权代表签名：_____

日期：_____

附录 4

4.1 法定代表人证明书

法定代表人证明书

报价人名称：

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_____（报价人名称）的法定代表人。

特此证明。

报价人名称：_____（盖公章）

法定代表人：_____（签字或盖章）

日期：_____

附件：法定代表人身份证正反面复印件并加盖报价人公章。

4.2 法定代表人授权书

法人授权委托书

致：广东省机场管理集团有限公司

本人_____（姓名）系_____（报价人名称）的法定代表人，现委托_____（姓名）为我司代理人。代理人根据授权，以我司名义签署、澄清、说明、补正、递交、撤回、修改项目编号为__的 （项目名称）____报价文件、签订合同和处理有关事宜，其法律后果由我司承担。

授权委托期限：自_____年___月___日至_____年___月___日止。

代理人无转委托权。特此委托。

报价人：_____（公章）

法定代表人：_____（签字或盖章）

代理人：_____（签字）性别：_____ 年龄：

代理人身份证号码：_____职务：_

授权委托日期： _____

附：代理人的身份证正反面复印件并加盖报价人公章。

附录 5

组织机构和人员

5.1 现场主要人员安排

报价人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（各表格可按报价人的情况扩展与扩充）：

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，报价人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 6

报价人的类似业绩

项目	项目规模及内容	完工时间	合同价	备注

注：近 3 年内业绩（以合同签订日期为准）。

附录 7

企业资质证书表

报价人应列出资质证书，应附上相关证明材料。详见如下表格（各表格可按报价人的情况扩展与扩充）：

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。

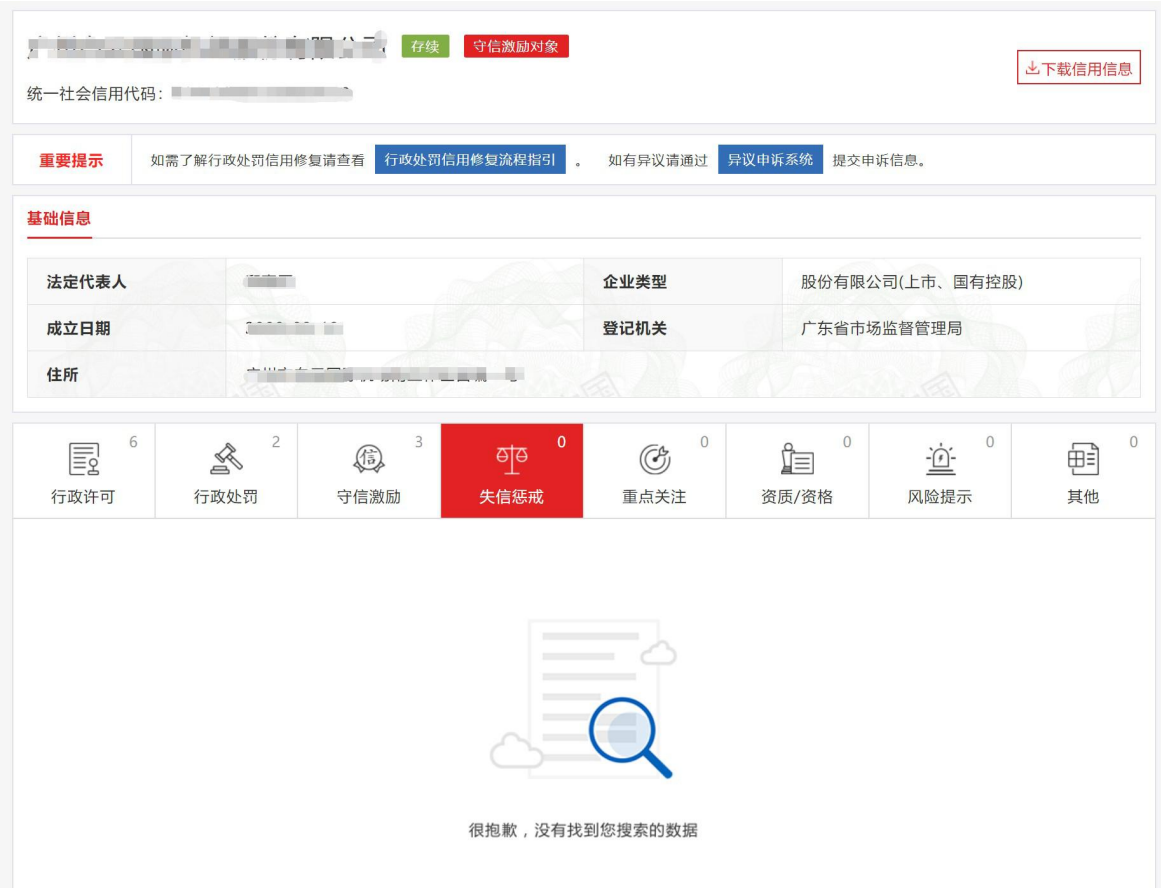
附录 8

国家企业信用信息公式系统网站（www.gsxt.gov.cn）截图格式要求

注：报价人须按上述格式要求截图并加盖公章，截图清晰显示报价人单位名称及列入严重违法失信企业名单信息，否则将被认定为无效报价文件。

附录 9

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



注：报价人须按上述格式要求截图并加盖公章，截图清晰显示报价人单位名称及列入信息，否则将被认定为无效报价文件。

附录 10

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报价人资格要求进行调整）

项目名称：

序号	报价人名称 审查项目			
1	报价人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、采购管理平台报价人登记表并加盖公章			
3	报价人近三年没有因腐败或欺诈行为而被政府或业主宣布取消投标资格；同时，报价人（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报价人公章）。			
4	报价人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	报价人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报价人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

用户需求书

一、项目概况

考虑到广东省机场管理集团有限公司（以下简称“机场集团”）业务发展的安全性和管理需要，业务向数据集中、应用分布化发展，机场集团新建管控类的业务的云平台和一体化平台，建设至今，云平台和一体化平台已初步建设完成，云平台和一体化平台安全稳定的运转关系到机场集团正常的办公和生产管理工作。

随着云平台和一体化平台初步建设完成后，机场集团对云平台的关注点转向第二阶段，即业务运营保障阶段，即如何保障机场集团业务本身的安全性和稳定性，进而确保业务的正常运转。集团目前尚未对系统安全状况进行过整体评估，为加快推进信息安全安全工作常态化，稳步提升信息安全防护能力，项目计划为集团本部信息化工作提供信息安全服务。

二、项目内容、规模

2.1 服务标准

序号	服务项	服务内容说明	服务对象	服务周期/频率	备注
1	安全评估服务	详见服务要求	集团本部涉及到的资产	1 次/年	
2	漏洞管理服务	详见服务要求	集团本部涉及到的资产	6 次/年	
3	新系统上线评估服务	详见服务要求	集团本部涉及到的资产	2 个系统/年	
4	渗透测试服务	详见服务要求	集团本部指定系统	2 个系统/年	
5	安全加固服务	详见服务要求	集团本部涉及到的资产	1 年	
6	安全运维及应急服务	详见服务要求	集团本部涉及到的资产	1 年	
7	安全培训服务	详见服务要求	集团本部涉及到的资产	1 次/年	
8	重点时期的安全值守服务	详见服务要求	集团本部	2 次/年	
9	安全态势感知服务	详见服务要求	集团本部	1 年	包括安全态势感知平台硬件工具
10	工单服务	详见服务要求	集团本部	1 年	包括工单系统软件或硬件
11	等级保护（二级）测评及技术整改服务	详见服务要求	财务系统、OA 系统、物资网、官网、邮件系统	5 个系统	

12	网站云防护	详见服务要求	物资网、官网	1 年	
13	信息安全体系建设	详见服务要求	集团本部	1 项	

2.2、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）

2.3 服务的内容要求

2.3.1 安全评估服务

安全评估服务重点参考等级保护的要求，并结合机场集团的实际情况开展评估工作，评估的内容包含物理机房、网络情况、主机配置情况、数据安全保障情况、应用安全情况等，具体要求包含但不限于如下：

物理机房评估内容：对单位物理机房的环境进行实地考察，评估单位物理机房的位置选择情况、物理访问控制措施、防盗器和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应和电磁防护；

网络评估内容：对单位的网络情况进行实地调研，评估单位网络安全区域划分和 IP 地址划

分是否合理、访问控制策略的粒度是否合理、网络各个区域的安全防护措施、网络设备的安全配置情况和策略配置情况；

主机评估内容：对单位的服务器进行登陆评估，评估服务器的安全配置、访问控制情况、端口开放情况、恶意代码的防范、弱口令的情况、安全漏洞情况等；

应用评估内容：对单位的应用进行安全评估，评估应用系统的登陆控制情况、应用审计情况、安全漏洞情况等；

数据评估内容：对单位的系统数据的安全性进行评估，评估数据类型、重要性及其备份情、应急恢复的情况；

2.3.2 漏洞管理服务

制定可行的漏洞检查工作计划，在不影响或低影响的前提下，对单位的服务器、网络设备进行漏洞扫描，挖掘网络中可能存在的漏洞隐患，并协助最终用户制定漏洞的修复计划，对于可以修复的漏洞，配合最终用户进行修复，对于修复可能造成不良影响的漏洞，提出风险的规避建议，并进行记录，掌握漏洞的安全风险发展趋势。

漏洞管理服务使用的漏洞管理工具要求如下：

要求项	要求内容
检查方法	基线检查和变更检查支持远程检查、SSH、TELNET、SMB 等多种方式
	▲基线检查和变更检查支持离线检查；（提供截图并盖章）
	▲漏洞扫描支持指定登录用户名和口令进行本地漏扫检查（提供截图并盖章）
	▲基线检查和变更检查支持跳转机跳转；（提供截图并盖章）
支持目标系统	主机类：Windows、Unix、Solaris、HP-Unix、AIX、Linux 等 网络设备：华为、H3C、Cisco、Juniper、中兴等 防火墙：华为、天融信、H3C、Fortigate、Cisco、Juniper、迪普防火墙等 数据库：Mysql、DB2、Oracle、Sqlserver、Sybase 等 中间件：Tomcat、IIS、Webservices、Apache、Weblogic、Resin、Nginx 等 虚拟化平台：VMware ESXi、VMware Center、XenServer
资产管理	资产管理：支持添加、修改、删除资产；对资产的基本属性进行维护；资产可以增加自定义属性
	资产支持视图管理，可对资产按不同类别进行分类管理
	▲系统支持对 IP 对象的自动发现功能；并智能识别对象系统类型（提供截图并盖章）
漏洞管理	漏洞扫描支持无害扫描
	支持识别出主机上运行的服务和端口
	▲支持 CVE、CNVD、CNNVD、BugTraq 等编号，拥有完备的知识体系（提供截图并盖章）
	内置不同的漏洞模板针对 Unix、Windows 操作系统、网络设备和防火墙等模板，同时支持用户自定义扫描范围和扫描策略
	支持高级数据分析，可对同一 IP 的两次扫描结果进行风险对比分析，并可在线查看同一 IP 的多次历史扫描结果
WEB 漏扫	支持常见的 WEB 应用弱点检测，支持主流安全漏洞扫描，如：SQL 注入、跨站脚本攻击、网页木马、系统命令执行漏洞、信息泄露、资源位置预测漏洞、目录遍历漏洞、配置不当漏洞、弱密码、内容欺骗漏洞、外链、暗链等类型漏洞

要求项	要求内容
	支持所有的应用服务器，如：IIS、Websphere、Weblogic、Apache、Tomcat 等，支持所有的 WEB 应用编程语言，如：ASP、JSP、.NET、J2EE、PHP、JS、HTML 等
安全基线违规管理	支持违规列表：显示系统内所有的违规信息情况，以列表方式呈现
	支持违规详细查看：在安全基线违规列表中，选择某个违规信息，可进一步查看该违规的详细信息
	在违规列表中支持查询功能，输入相关查询字段进行查询

2.3.3 新系统上线评估服务

新系统上线评估服务主要针对新设计开发的系统进行评估，评估依据参考等级保护的要求和新系统的使用安全要求，主要包含但不限于如下方面的评估：

物理机房评估内容：对新系统部署的机房环境进行实地考察，评估新系统部署的位置选择情况、物理访问控制措施、防盗器和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应和电磁防护；

网络评估内容：对新系统的网络设计进行评估，评估新系统网络安全区域划分和 IP 地址划分是否合理、访问控制策略的粒度是否合理、网络各个区域的安全防护措施、网络设备的安全配置情况和策略配置情况；

主机评估内容：对新系统的服务器进行登陆评估，评估新系统的安全配置、访问控制情况、端口开放情况、恶意代码的防范、弱口令的情况等；

应用评估内容：对新系统的应用进行安全评估，评估新系统的登陆控制情况、应用审计情况、安全漏洞情况等；

数据评估内容：对新系统数据的安全性进行评估，评估数据类型、重要性及其备份情、应急恢复的情况；

漏洞风险评估：在新系统上线前进行系统漏洞和 WEB 漏洞的安全评估，并在漏洞修复进行二次复测，确保新上线的系统不存在高风险漏洞；

2.3.4 渗透测试服务

指派具备高技能和高素质的安全攻防人员发起、并模拟常见黑客所使用的攻击手段对机场集团指定目标系统进行模拟入侵。渗透测试的对象为机场集团指定系统。

渗透测试的内容包含系统信息的采集、口令爆破、登陆安全、账号安全、系统漏洞渗透、WEB 漏洞渗透等。

2.3.5 安全加固服务

安全整改加固工作对通过安全评估服务、漏洞扫描等工作中发现的安全漏洞、安全弱点、安全风险，通过多方面的安全加固措施进行修补。特别对问题源头进行整改与加固，以最大限

度的降低风险，安全加固应包含但不限于以下内容：

- 配置核查结果的服务器安全加固
- 漏洞扫描的服务器安全加固
- 边界安全策略的安全加固
- 其它评估类工作（一体化信息安全风险评估、等级保护测评等）发现/公布的漏洞，以及国家、行业等上级及外部单位安全通告公布的安全漏洞，协助整改加固。

2.3.6 安全运维及应急服务

提供集团本部年度的安全运维服务，对于集团公司管理人员提出的安全服务要求和安全技术工作进行实时响应，包含安全事件的应急和其他安全技术工作的配合。

根据安全事件对集团本部的影响，定义不同的安全风险等级，进行不同级别的安全响应。

当出现信息安全事件时，第一时间对信息安全事件进行应急支持，提供设备或者技术支持，帮助问题解决，并对事件发生的原因进行分析。

1、远程技术应急支持：10 分钟内对安全事件进行响应，对于能够解决的信息安全事件，远程协助进行处理，对于不能远程解决的事情，提供现场的应急支持。

2、现场技术应急支持：100 分钟内到达事件现场，优先协助对事件进行处置，恢复业务，并对事件发生的原因进行分析，编写事件的分析报告，提出有效的安全建议。

2.3.7 安全培训服务

依据机场集团的要求，对指定的人员进行信息安全培训，培训内容包含但不限于以下两部分内容。

信息安全意识类培训：包含最新的信息安全政策法规、信息安全事件案例的分享、员工信息安全意识培训等；

信息安全技术类培训：包含操作系统安全管理培训、安全防护的产品培训、安全攻击工具的使用培训、渗透测试类攻防培训等；

培训时长：根据具体情况定，每次培训不少于 2 小时，不超过 6 小时。

培训讲师要求：要求培训讲师至少是讲师或以上级别的专家，具有至少 5 年信息安全工作和培训的经验，有过不少于 10 场 100 人以上的培训经验。

培训台账：每次培训完成后针对培训内容须建立培训台账，形成纸质的或电子的培训记录。

2.3.8 重点时期的安全值守服务

在国庆、两会等重要时期，依据集团要求派遣人员到客户端进行值守，在值守过程中，针对客户现有安全现状进行梳理，发现网络中的安全薄弱面，进行修补。在值守期间，针对突发性安全事件进行及时响应和处置。

2.3.9 安全态势感知服务

提供一套态势感知平台，实现集团本部信息安全的监测，态势感知平台要求如下：

功能项	功能细项	功能指标要求
大屏可视	综合安全态势大屏	支持大屏展示综合安全态势，包括资产态势、脆弱性态势、网络攻击态势、安全事件态势、外连态势、横向威胁态势、设备运行态势；支持页面跳转到对应态势大屏，并具备大屏告警能力。
	安全事件态势	支持大屏展示安全事件态势，包括安全事件、事件等级分布、安全事件态势、安全事件 TOP5、威胁面最大的事件 TOP10、事件类型 TOP5、风险业务/终端 TOP5。
	脆弱性态势	▲支持大屏展示业务脆弱性态势，包括漏洞风险态势、漏洞类型 TOP5、高危漏洞 TOP5、业务总览、脆弱性业务 TOP5、实时脆弱性监测（需提供截图证明并加盖原厂商公章）。
	资产态势	支持大屏展示资产态势，包括服务器操作系统分布、服务器开放服务 TOP5、最新资产动态、最近变动资产。
	3D 网络攻击态势	支持 3D 大屏展示网络攻击态势，包括攻击次数、遭受攻击资产组、攻击源地址、攻击源 IP、攻击手段排行、遭受攻击服务器排行；支持境外、境内切换
	横向威胁态势	▲支持大屏展示横向威胁态势，包括业务与终端访问、发起威胁终端 TOP5、遭受威胁业务 TOP5、访问趋势图；支持不同颜色标注横向攻击、违规访问、可疑行为、风险访问等行为（需提供截图证明并加盖原厂商公章）。
	设备运行态势	支持大屏展示探针、AF 接入平台状态，显示设备在线、离线、CPU、磁盘使用情况，进行实时流量监测，及时发现设备异常。
	大屏轮播	▲支持不同视角展示全网安全态势，包括综合安全态势、分支安全态势、安全事件态势、网络攻击态势、外连风险态势、横向威胁态势、脆弱性态势、资产态势、正常横向访问监控态势、正常外连监控态势、设备运行态势等 13 个独立的大屏展示功能；支持大屏轮播，可自定义播放顺序（需提供截图证明并加盖原厂商公章）。
脆弱性感知	脆弱性总览	支持业务脆弱性风险分布展示，包括不同严重级别业务分布，漏洞类型分布，漏洞整体态势等。
	弱密码	▲支持检测 15 类以上常见协议的弱密码，包括 HTTP、FTP、LDAP、VMWARE、ORACLE、VNC 等协议，检测信息包含账号、密码、服务器、所属分支和业务、类型、最近发现时间等；支持筛选管理员账号与是否登录成功，并支持导出弱密码报告（需提供截图证明并加盖原厂商公章）。
处置中心	风险业务视角	▲支持业务视角维度展示安全风险，包括攻击阶段分布、风险等级趋势、事件描述、遭受的外部攻击、脆弱性风险、行为画像、开放端口等（需提供截图证明并加盖原厂商公章）。
	风险终端视角	支持终端维度展示终端 IP、所属分支、所属终端组、风险等级、安全事件标签、处理状态、联动状态；风险等级包含已失陷、高危、中危、低危。
	风险安全域视角	▲支持安全域维度展示安全风险，包括安全域列表、安全域评分、事件类型 TOP5、IP 地址、IP 类型、风险等级、关键风险（需提供截图证明并加盖原厂商公章）。
分析中心	威胁分析	支持外部威胁分析，包括高危攻击、残余攻击、暴力破解、成功的事中攻击、邮件威胁、文件威胁、外部风险访问。
		▲支持横向威胁分析，包括横向威胁总览、横向攻击、违规访问、可疑行为、风险；其中横向风险总览包括发起横向威胁主机 TOP5、遭受

		横向威胁 TOP5、横向威胁类型分布、横向威胁趋势（需提供截图证明并加盖原厂商公章）。
		▲支持外连威胁分析，包括对外威胁总览、对外攻击、APTC&C 通信、可疑行为、隐蔽通信、违规访问、服务器风险访问；其中外连威胁总览包括外连威胁主机类型分布、存在外连威胁 IP TOP5、外连目标地区（国外）TOP5、外连威胁类型分布、非正常时间段外连主机 TOP5、外连威胁趋势（需提供截图证明并加盖原厂商公章）。
	可疑DNS分析	▲支持 DNS 异常分析，包括 DNS 通道、DGA 域名、灰域名与高风险注册地域名，其中高风险注册地域名可自定义国家和地区；并支持导出可疑 DNS 列表（需提供截图证明并加盖原厂商公章）。
	威胁情报	▲支持威胁情报关联分析，内置威胁情报数量不少于 120W；支持展示威胁情报命中数、今日命中数、命中威胁情报类别 TOP10、命中趋势、活跃威胁情报 TOP20 等（需提供截图证明并加盖原厂商公章）。
		支持自定义威胁情报，可定义域名、IP、URL、文件 MD5、确定性等级、威胁等级、事件类型、危害描述、处置建议等信息（需提供截图证明并加盖原厂商公章）。
	访问核查	▲支持源 IP、目的 IP、源端口、目的端口、起始时间等维度定义核查任务；支持统计每天访问频次及访问成功和失败次数（需提供截图证明并加盖原厂商公章）。
	文件威胁分析	▲支持文件威胁分析，可展示文件分析过程、文件检测趋势、恶意文件 TOP5；支持恶意文件的详情分析，包括支持记录恶意文件感染的主机、所属分支、文件名、病毒名称、传输协议等；支持导出文件威胁分析结果（需提供截图证明并加盖原厂商公章）。
	挖矿专项检测	支持挖矿专项检测，可实时查看挖矿各个攻击阶段，包括感染挖矿病毒、与控制端建立通信、获取挖矿任务、尝试挖矿、挖矿成功等；支持挖矿币种分布、挖矿风险态势、受影响主机等维度分析统计
	UEBA 异常行为分析	▲支持对数据库登录地点、登陆时间、访问表、访问数据量、访问数据库频率等进行持续学习和监控，判断是否存在数据异常行为，发现非常见用户登录、非常见地址访问、非常见时间段访问、非常见数据库表访问、数据库频繁访问、数据库表访问量过大等异常行为（需提供截图证明并加盖原厂商公章）。
		▲支持不同场景下数据库异常模型的算法编辑，可选择稀有值检测算法、ZScore 异常检测算法、箱线图异常检测算法；可将不同类型的算法应用到不同的资产（需提供截图证明并加盖原厂商公章）。
		支持对服务器主动外连的地址进行持续学习和监控，判断设备是否存在外联异常，发现主机外联非常用地址；判断设备是否存在外连下载文件、外发文件等异常行为。
		支持对终端外发数据进行持续学习和监控，判断是否存在外发数据异常、外发数据到不常用地址等异常行为。
		支持对访问服务器的地址、端口、时间段、地点的异常监控，判断是否存在访问异常、非常用地址和非常用时间通过高风险协议如 ssh、rdp 等协议访问业务服务器等异常行为。
	邮件深度检测	支持邮件威胁分析，可展示收件人 TOP5、发件人账号 TOP5、恶意邮件类型分布、危害和处置建议；支持对恶意邮件详情分析，包含收件人账号、恶意邮件数量、发件人账号、附件名称、病毒名称、恶意链接名称等，并支持导出分析结果
	横向访问分析	▲支持横向访问服务器流量分析，包括 TOP5 应用流量趋势、TOP5 协议趋势；支持服务器视角和来访分支视角，其中服务器视角可展示服务器 IP、总流量、源 IP 数量、应用 TOP10、协议端口 TOP10、连接失败数、最大并发，并支持以表格形式导出数据（需提供截图证明并加盖原厂商公章）。

		支持横向访问最活跃的源主机分析，可按访问 IP 次数排序和按访问次数排序，支持展示源 IP 地址、目标 IP 数、首次请求时间、最近请求时间、日志数等，并支持以表格形式导出数据
	外连分析	▲支持对服务器外连流量分析，包括 TOP5 应用流量趋势、TOP5 协议趋势；支持地域视角和服务器视角，其中地域视角可展示国家地区、源 IP 数、总流量、上下行流量与占比、应用 TOP10、协议端口 TOP10、最近活跃时间，并支持以表格形式导出数据（需提供截图证明并加盖原厂商公章）。
		支持展示对外连接总览，以全国地图形式展示当前服务器与终端的外连国家信息，包括外连国家 TOP5、外连服务器 TOP5、外连趋势等；支持对外连的详情展示，包括访问源、访问源属性、访问目标、应用类型 TOP3、服务、流量大小和访问次数等并支持以表格形式导出数据
	外对内流量分析	支持外部对内部的业务流量分析，包括 TOP5 应用流量趋势、TOP5 协议趋势；支持地域视角和服务器视角展示，其中服务器视角可展示服务器 IP、访客地域 TOP5、总流量、上下行流量与占比、应用 TOP10、协议端口 TOP10、最近活跃时间，并支持以表格形式导出数据
报告中心	主机安全风险报告	支持导出主机安全风险报告，报告内容包括业务与终端风险摘要、业务风险与终端详情分析，提供危害解释和参考解决方案；适用于日常处理安全问题的运维人员。
	脆弱性感知报告	支持导出脆弱性风险报告，报告内容包含脆弱性检测总览、业务脆弱性详情分析等，提供危害解释和参考解决方案。
	摘要报告	支持导出摘要报告，报告内容包含总体摘要、安全感知详情、UEBA 行为画像、安全规划建设建议等，从整体展示安全状况，快速了解业务和网络的安全风险。
	综合风险报告	支持导出完整综合风险报告，报告内容包括平台说明、安全风险概括、业务与终端安全详情分析、安全规划建设建议等。
	等级保护管理服务	▲支持对等级保护建设整改过程中系统定级、差距评估、备案、整改、测评过程中产生的文档结论进行统计归档，并使用可视化的统一界面进行展现与管理，最大程度发挥安全措施的保护能力（需提供截图证明并加盖原厂商公章）。

2.3.10 工单服务

提供一套工单系统，实现集团本部安全问题处置的工单管理。工单系统要求如下：

功能项	功能指标要求
开发要求	支持根据客户要求进行二次开发
系统平台	提供事件流程及表单管理、服务级别判定提醒功能；
	提供服务请求流程及表单管理、服务级别判定提醒功能；
	提供变更流程及表单管理功能；
	支持服务数据长期保存；
	支持通过短信、APP 提醒、微信等有效通讯方式通知运维管理相关这人的
	集运维管理、任务管理、情报管理于一体。
	支持与单位目前的监测设备对接。
	支持工单数据输出到其他平台使用。
类别管理	支持对事件类别、服务请求类别和变更类别统一管理。
客户管理	支持对多级客户和多个联系人信息进行管理，支持对客户服务协议、服务级别进行管理，。
服务目录管理	支持对服务目录项信息进行管理。
用户管理	支持对组织结构、用户信息、角色信息、授权信息进行统一管理。角色权限信息支持自定义。

运维管理	支持对事件流程、操作、主单信息、子单信息进行管理。
	支持对服务请求流程、操作、主单信息、子单信息进行管理。
	支持对变更流程、操作、主单信息、子单信息进行管理。
	支持事件单、服务请求单、变更单根据流程自动流转。
	支持事件单根据服务级别要求自动提醒升级。
	支持事件关联变更的运维管理要求。
统计报表	系统应支持对事件单、服务请求单、变更单分别根据不同的服务级别指标进行统计。
支持移动端	支持事件、服务请求、变更消息提醒； 支持事件、服务请求、变更流转情况的查看； 支持事件、服务请求、变更的发起和处理； 支持情报库和知识库的查询和管理。

2.3.11 等级保护（二级）测评及技术整改服务

对集团指定系统开展等级保护测评和技术整改工作，确保相应系统通过等级保护二级测评。

2.3.12 网站云防护

为集团物资网和官网提供给云防护服务，包含如下：

服务项	服务内容	描述
服务内容	云平台网站托管服务	为单个网站提供：主机资源 2 核 2G；云硬盘 100G；BGP 带宽：5M，并配备一个公网 IP。
	网站安全监测服务	要求服务提供商提供 0day 漏洞、WebShell 漏洞和网页篡改监测服务，并提供 7*24 不间断的持续监测,通过微信、短信或邮件的方式 推送告警。
	网站安全防御服务	云平台为每个网站单独配备一套 50M 带宽的防御吞吐量的虚拟化 WEB 应用防火墙
	网站安全检测服务	在网站托管前提供一次安全漏洞扫描检测，并提供网站整改技术支持。服务期间每半年提供一次漏洞扫描并提供检测报告。中间件版本升级时由服务提供商提供一次安全漏洞扫描检测。
	安全专家人工服务	在国家重大活动期间，提供重点保障服务，提供专门的安全漏洞检测，24 小时安全值守和应急响应服务。
		安全培训服务、安全评估服务
		服务期内提供免费的安全技术咨询服务，协助网站等保备案。
	云主机备份	提供 100G 备份空间，保证用户数据的安全性。
	IPV6 改造服务	提供 IPV6 地址，出口带宽，并提供 IPV6 地址映射到 IPV4。

托管云平台要求：

▲云厂商拥有 ITSS 私有云服务能力符合性评估二级认证，提供相应的证书复印件

▲为保障云平台的领先性和成熟度，云平台厂商入围 2016 X86 服务器虚拟化魔力象限，提供证明材料

▲为保障云平台的领先性和成熟度，云平台厂商入围 Gartner 2019 年《超融合基础设施全球魔力象限》，提供证明材料

▲为保障云平台的领先性和成熟度，云平台厂商 2018 年在中国超融合软件市场占有率为前三名（需提供 IDC 市场报告证明）

2.4、服务成果要求

序号	服务项	服务文档成果	报告要求
1	安全评估服务	《安全评估报告》	每次一份
2	漏洞管理服务	《漏洞扫描和修复报告》	每次一份
3	新系统上线评估服务	《XXX 系统安全上线评估报告》	每个系统一份
4	渗透测试服务	《XXX 系统渗透测试报告》	每个系统一份
5	安全加固服务	《安全加固报告》	每次一份
6	安全运维及应急服务	《安全运维报告》 《安全应急报告》	每次一份
7	安全培训服务	《安全培训课件》	每次一份
8	重点时期的安全值守服务	《安全值守报告》	每次一份
9	安全态势感知服务	《安全态势感知》	每月一份
10	工单服务	/	/
11	等级保护（二级）测评及技术整改服务	《XXX 系统等级保护测评报告》	每个系统一份
12	网站云防护	《网站月度巡检报告》	每次一份

三、项目方案设计要求

技术方案书要求包括但不限于以下内容：

1.总述

对本项目的理解分析，以及工作背景，目标说明等。

2.工作方案

1）项目总体工作思路

说明投标人展开本项目工作的思路，包括工作方式、方法等内容进行阐述。

2）整体工作计划

对项目整体工作进度安排、工作关键点、里程碑等进行阐述。工作计划须明确每位项目成员在项目实施每个阶段承担的具体工作。投标人必须承诺完全按照工作计划所列的技术服务人员配置和时间安排开展项目实施工作。

3）主要工作内容

对本项目中各项工作如何开展进行详细阐述。要求工作方式可行，能够切实落地。

4）风险与质量控制

对项目风险控制措施和质量保障措施进行阐述。

四、项目工期

项目总工期为一年。

除去非驻场的文档编制工作，要求投标人技术服务人员驻集团本部现场工作服务时间不得少于 100 人/日。

五、服务团队要求

投标人必须保证从事本项目工作的相关人员具备完成合同规定的工作所需的资历和技能，并向甲方如实提供相关人员专业经验和水平的证明材料，以及其他的投标人认为有必要提供的资料。

投标人需要成立项目服务团队。

若投标人需要更换核心服务人员，应提前以书面方式通知招标人项目总负责人，只有获得招标人项目总负责人的正式批准后方能进行更换。

六、安全保密要求

服务提供方须与招标人签署相关保密协议，同时要求提供服务方与其服务人员就本次服务签署的保密协议。

针对本服务项目，要求服务人员的变动率不得超过 20%，确需变更应提前通知招标人并获得批准后方可进行。服务过程中所有原始资料和数据均须妥善保管，仅限在项目组内为本服务项目所用，不得以任何方式外泄或用于其它用途，服务人员须及时删除存储在电脑中或纸质的数据和文件材料。