信息管理系统等级保护整改

招标文件

项目编号：HZ2018-370

海政招标
HAIZHENG TENDERING

甲级政府采购代理机构

采　　购　　人：海南医学院第一附属医院

招标代理机构：海南海政招标有限公司

二〇一八年八月

目　录

第一章 投标邀请函

受海南医学院第一附属医院的委托，海南海政招标有限公司就信息管理系统等级保护整改（项目编号：HZ2018-370）所需的货物及相关服务组织公开招标，欢迎合格的投标人前来投标。有关事项如下：

一、招标项目

1、名称：信息管理系统等级保护整改

2、用途：海南医学院第一附属医院工作需要

3、技术要求：见“用户需求书”

4、本项目预算为：￥2,108,249.60 元。超过采购预算金额的投标文件按无效投标处理。

二、投标人资格要求

1、在中华人民共和国注册，具有独立承担民事责任能力（企业需提供营业执照、税务登记证、组织机构代码证复印件或者三证合一复印件，事业单位需提供事业单位法人证书）；

2、具有良好的商业信誉和健全的财务会计制度（需提供近一年内任意三个月的纳税证明或者会计师事务所出具的近一个年度财务审计报告）；

3、有依法缴纳社会保障资金的良好记录（需提供近一年内任意三个月的社保缴费记录复印件）；

4、参加政府采购活动前三年内，在经营活动中没有重大违法记录（提供声明函）；

5、购买本项目招标文件并缴纳投标保证金。

三、招标文件的获取

1、时间：2018 年 8 月 8 日至 2018 年 8 月 15 日 9：00-17：00（节假日除外）；

2、标书发售地点：http://218.77.183.48。

3、标书售价： 300 元/套（售后不退）。**报名费用在开标现场缴纳**。

4、投标人提问截止时间：2018 年 8 月 17 日 17:00:00（北京时间）。

5、保证金到账截止日期： 2018 年 8 月 28 日前 10:30:00（北京时间），投标保证金支付形式：网上支付，支付地址为：http://218.77.183.48/htms。保证金单据上必须注明项目编号以及项目名称（如有分包，则同时注明包号）。投标保证金为￥10,000 元。

四、投标截止时间、开标时间及地点

1、递交投标文件时间：2018 年 8 月 28 日上午 10：15- 10：30；

2、开标时间：2018 年 8 月 28 日上午 10：30；

3、开标地点：海口市国兴大道海南省公共资源交易服务中心（省政务中心旁会展楼）二楼 205 开标室；

4、投标截止日期前，必须在网上上传 PDF 格式电子投标文件（使用 WinRAR 加密压缩），并在开标时提交电子版、纸质版投标文件；

5、招标结果请查询：http//www.hizw.gov.cn、www.ccgp-hainan.gov.cn、www.ccgp.gov.cn、http://ztb.hainan.gov.cn/index.php

五、招标代理机构联系方式

地址：海口市蓝天路名门广场北区 B 座 1-5 号 3002

电话： 0898-68500660、68500116；传真：0898-68500661； 财务：0898-68555187

项目联系人： 李爱乾 公司邮箱：hnhzzb@163.com

六、采购人联系方式

1、联系人：黄女士

2、联系方式：0898-66513992

3、地址：海口市龙华路 31 号

海南海政招标有限公司

二〇一八年八月

第二章 投标人须知

投标人须知前附表

条款号	名称	编列内容
1.1	项目名称	信息管理系统等级保护整改
1.2	采购人	海南医学院第一附属医院
1.3	招标代理机构	海南海政招标有限公司
4.2	是否接受联合体投标	不接受
11.1	投标有效期	60日历天
12.1	投标文件数量	正本壹份，副本肆份。
16.1	评标委员会的组成	评标委员会由采购人代表、专家组成，成员人数为5人，其中技术、经济等方面的专家从省综合评标专家库中随机抽取。
23.1	招标服务费	海南海政招标有限公司根据项目预算按计价格[2002]1980号文相关规定向中标人收取中标服务费
24.1	答疑会	不召开
	需要补充的其他内容	

一、总则

1. 名词解释

1.1 项目名称：见投标人须知前附表 1.1 款

1.2 采购人：见投标人须知前附表 1.2 款

1.3 招标代理机构：见投标人须知前附表 1.3 款

1.4 投标人：已从海南海政招标有限公司购买招标文件并向海南海政招标有限公司提交投标文件的投标人。

2. 适用范围

本招标文件仅适用于海南海政招标有限公司组织的本次投标活动。

3. 合格的投标人

3.1 凡有能力按照本招标文件规定的要求交付货物和服务的投标单位均为合格的投标人。

3.2 投标人参加本次招标活动应当符合《中华人民共和国政府采购法》第二十二条的规定，并具备本招标文件第一章的“投标人资格要求”规定的条件。

3.3 本项目如为信息系统采购项目，供应商不得为该整体项目或其中分项目前期工作提供过设计、编制、管理等服务的法人及附属单位。

3.4 单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的政府采购活动。除单一来源采购项目外，为项目提供整体设计、规范编制或者项目管理，监理、检测等服务的供应商，不得再参加该采购项目的其他采购活动。

3.5 投标人在本项目招标公告前三年内被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单，以及存在其他不符合《中华人民共和国政府采购法》第二十二条规定条件的情况的投标人不得参与投标。

两个以上的自然人、法人或者其他组织组成一个联合体，以一个供应商的身份共同参加政府采购活动的，联合体任意成员存在不良信用记录的，视同联合体存在不良信用记录。

3.6 本章 3.5 款的信用记录以“信用中国”网站（www.creditchina.gov.cn）或中国政府采购网（www.ccgp.gov.cn）上公布的信用记录为准。

4.联合体投标

4.1 联合投标时，联合体各方之间应当签订共同投标协议，明确约定联合体各方承担的工作和相应的责任，并将共同投标协议连同投标文件一并提交。联合体各方签订共同投标协议后，不得再以自己名义单独在同一项目中投标，也不得组成新的联合体参加同一项目投标。联合体中至少有一方完全满足投标人资格要求的特定条件。

4.2 本项目是否接受联合体投标：见投标人须知前附表 4.2 款。

5. 投标费用和解释权

5.1 无论招标投标过程中的做法和结果如何，投标人均自行承担所有与参加投标有关的全部费用。

5.1 本招标文件由海南海政招标有限公司负责解释。

二、招标文件

6. 招标文件的组成

6.1 招标文件由六部分组成，包括：

第一章 投标邀请书

第二章 投标人须知

第三章 用户需求书

第四章 合同条款

第五章 投标文件内容和格式

第六章 评审方法

请仔细检查招标文件是否齐全，如有缺漏，请立即与招标代理机构联系解决。

6.2 投标人必须详阅招标文件的所有条款、文件及表格格式。投标人若未按招标文件的要求和规范编制、提交招标文件，将有可能导致招标文件被拒绝接受，所造成的负面后果由投标人负责。

7. 招标文件的澄清、修改或补充

7.1 投标人在收到招标文件后，若有疑问需要澄清，应及时以书面形式向海南海政招标有限公司提出，海南海政招标有限公司将以书面形式进行答复，同时海南海政招标有限公司有权将答复内容分发给所有购买了此招标文件的投标人。

7.2 海南海政招标有限公司可以指定媒体上公告的方式修改/补充招标文件。修改/补充通知作为招标文件的组成部分，对投标人起同等约束作用。

7.3 当招标文件与修改/补充公告的内容相互矛盾时，以海南海政招标有限公司最后发出的修改/补充公告为准。

7.4 为使投标人有足够的时间按招标文件的修改/补充要求修正投标文件，海南海政招标有限公司有权决定推迟投标截止日期和开标时间。

三、投标文件

8. 投标文件的组成

8.1 投标文件应按“第五章 投标文件内容和格式”要求编制。

8.2 若投标人未按招标文件的要求提供资料，或未对招标文件做出实质性响应，将可能导致投标文件被视为无效。

9. 投标报价

9.1 报价均须以人民币为计算单位。

9.2 报价应包括全部货物、服务的价格及相关税费、运输到指定地点的装运费用（如有）、安装调试（如有）、培训（如有）、售后服务等其它有关的所有费用。

9.3 投标人应按开标一览表的要求报价，不能提供有选择的报价。

9.4 中标候选人的报价如超过预算且采购人不能支付的，采购人有权拒绝而递选下一个顺位的候选人。

10. 投标保证金

10.1 投标保证金是参加本项目投标的必要条件，保证金支付要求见第一章。为避免资金在途不能及时到账造成投标无效，建议投标人提前在投标截止时间一个工作日前办理保证金支付手续。

10.2 若投标人不按规定提交投标保证金，其投标文件将被拒绝接受。

10.3 投标保证金的退还

10.3.1 中标人的投标保证金在其与采购人签订了合同后五个工作日内无息退还。

10.3.2 落标的投标人的投标保证金将在海南海政招标有限公司发出中标通知书五个工作日内无息退还。

10.3.3 如投标保证金为海南海政招标有限公司收取，则中标结果公告期满后，投标人应把投标保证金退还申请函（必须注明项目名称、金额以及退还的银行账户）传真到0898-68555187，以便办理投标保证金退还手续。

1）如投标保证金为海南省公共资源交易服务中心、三沙市公共资源交易服务中心、儋州市公共资源交易服务中心收取，未中标方的投标保证金待中标结果公示期满后由代理机构工作人员办理退款，中标方的投标保证金待和采购单位签订合同并送达代理机构提交电子招投标系统后由代理机构工作人员操作办理退款。

如投标保证金已缴纳但未在电子招投标系统中提交关联，则和投标保证金收取单位联系办理退款手续，退款时请提供如下材料（加盖公章）：(1)退款申请书；(2)法人代表及经办人身份证（复印件）；(3)授权委托书；(4)电汇单（复印件）；(5)开户许可证（复印件）。

2）三亚市人民政府政务服务中心收取，未成交的供应商，保证金将在成交通知书发出之日起5个工作日内，由招标代理机构在全国公共资源交易平台（海南省）·三亚市系统中操作退还保证金。成交的供应商，保证金将在采购合同签署后5个工作日内，由招标代理机构在全国公共资源交易平台（海南省）·三亚市系统中操作退还保证金。

如投标保证金已缴纳但未在电子招投标系统中提交关联，则和投标保证金收取单位联系办理退款手续，退款时请提供如下材料（加盖公章）：(1)退款申请书；(2)法人代表及经办人身份证（复印件）；(3)授权委托书；(4)电汇单（复印件）；(5)开户许可证（复印件）。

3）如投标保证金为海口市公共资源交易中心收取，未中标方的投标保证金待中标通知书发放后由海口市公共资源交易中心相关工作人员操作办理退款。中标方的投标保证金待合同原件及电子版合同送达海口市公共资源交易中心后由海口市公共资源交易中心相关工作人员操作办理退款。

联系电话：

海南省公共资源交易服务中心：0898-66529867

三沙市公共资源交易服务中心：0898-66860296

儋州市公共资源交易服务中心：0898-23335693

三亚市人民政府政务服务中心：0898-38860835

海口市公共资源交易服务中心：0898-65250512

10.4 发生下列情况之一，投标保证金将不予退还：

（1）投标人在投标有效期内撤回其投标文件的；

（2）投标人不按本章规定签订合同；

（3）投标人提供虚假材料谋取中标、成交的；

（4）与采购人、其它投标人或者招标代理机构恶意串通的；

（5）向采购人、招标代理机构、评标委员会成员行贿或者提供其他不正当利益的；

11．投标有效期

11.1 投标有效期：见投标人须知前附表 11.1 款，有效期短于此规定的投标文件将被视为无效。

11.2 在特殊情况下，海南海政招标有限公司可于投标有效期满之前，征得投标人同意延长投标有效期，要求与答复均应以书面形式进行。投标人可以拒绝接受这一要求而放弃投标，投标保证金将尽快无息退还。同意这一要求的投标人，无需也不允许修改其投标文件，但须相应延长投标保证金的有效期。受投标有效期制约的所有权利和义务均应延长至新的有效期。

12．投标文件的数量、签署及形式

12.1 投标文件数量：见投标人须知前附表 12.1 款。投标文件须固定装订。

12.2 投标文件须按投标文件的要求执行，每份投标文件均须在封面上清楚标明“正本”或“副本”字样，“正本”和“副本”具有同等的法律效力；“正本”和“副本”之间如有差异，以正本为准。

12.3 投标文件正本中，文字材料需打印或用不褪色墨水书写。投标文件的正本须经法人代表或授权代表签署和加盖投标人公章。

12.4 投标文件不得涂改和增删，如要修改错漏处，修改处必须由法人代表或授权代表签名、或盖公章。

四、投标文件的递交

13. 投标文件的密封及标记

13.1 投标人应将投标文件正本和所有副本分别密封在两个报价专用袋（箱）中（正本一包，副本一包），并在报价专用袋（箱）上标明“正本”、“副本”字样，封口处应加盖骑缝章。封皮上均应写明：

致：海南海政招标有限公司

项目名称：xxxxxxxxxxxxxxxx

项目编号：HZxxxx-xxx （如分包则注明包号）

注明：“请勿在开标时间之前启封”

投标单位名称、联系人姓名和电话

13.2 投标文件未按上述规定书写标记和密封者，海南海政招标有限公司不对投标文件被错放或先期启封负责。

14. 投标截止时间

14.1 投标人须在投标截止时间前将投标文件送达招标代理机构规定的地点。

14.2 若招标代理机构推迟了投标截止时间，应以公告的形式通知所有投标人。在这种情况下，招标代理机构、采购人和投标人的权利和义务均应以新的截止时间为准。

14.3 在投标截止时间后递交的投标文件，海南海政招标有限公司将拒绝接受。

14.4 在规定时间内提交投标文件的投标人不足 3 家，不得开标，本次招标失败。

五、开标及评标

15. 开标

15.1 海南海政招标有限公司按投标文件第一章规定的时间和地点进行开标，采购人代表、招标代理机构有关工作人员参加。投标人可以委派授权代表参加开标活动，参

加开标的代表须持本人身份证件签名报到以证明其出席，评标委员会成员（包括采购人委派的用户评委）不能参加开标活动。

投标人未参加开标的，视同认可开标结果。

15.2 开标时，投标人代表将查验投标文件密封情况，确认无误后拆封唱标，公布每份投标文件中“开标一览表”的内容，以及海南海政招标有限公司认为合适的其他内容，海南海政招标有限公司将作开标记录。

15.3 若投标文件未密封，海南海政招标有限公司将拒绝接受该投标人的投标文件。

16. 评标委员会

16.1 评标委员会由技术、经济等方面的专家和用户代表组成，其中技术、经济等方面的专家随机抽取，且人数不得少于总数的 2/3。专家人数见投标人须知前附表 16.1 款。该评标委员会独立工作，负责评审所有投标文件并确定中标侯选人。

17.关于政策性加分

17.1 所投分包(如不分包则指本项目)的所有投标产品进入当期节能清单的，其评标价=投标报价*（1-2%）；投标人所投产品满足此规定的，必须提供声明函并提供相关证明文件。

17.2 所投分包(如不分包则指本项目)的所有投标产品进入当期环保清单的，其评标价=投标报价*（1-1%）；投标人所投产品满足此规定的，必须提供声明函并提供相关证明文件。

17.3 投标人为小型和微型企业（含联合体）的情况：

17.3.1 中小企业的认定标准：

1）提供本企业制造的货物、承担的工程或者服务，或者提供其他中小企业制造的货物，不包括提供或使用大型企业注册商标的货物；

2）本规定所称中小企业划分标准，是指国务院有关部门根据企业从业人员、营业收入、资产总额等指标制定的中小企业划型标准（工信部联企业〔2011〕300 号）；

3）小型、微型企业提供有中型企业制造的货物的，视同为中型企业；小型、微型、中型企业提供有大型企业制造的货物的，视同为大型企业。

4）监狱企业视同为小型、微型企业。

（投标人为小型、微型企业，同时所投产品为小型、微型企业生产的才能享受政策性优惠）

17.3.2 具体评审价说明：

1）投标人为小型或微型企业，其评审价=投标报价*（1-6%）；

2）投标人为联合体投标，联合体中有小型或微型企业且联合协议中约定小型、微型企业的协议合同金额占到联合体协议合同总金额 30％以上的，其评审价=投标报价*（1-2%）。

17.3.3 投标人为工信部联企业〔2011〕300 号文规定的小型和微型企业（含联合体）的，必须如实填写“中小企业声明函”（内容、格式见财库〔2011〕181 号），并提供营业收入、人员等相关证明材料，否则无效。**如有虚假骗取政策性加分，将依法承担相应责任。**

18. 评标

18.1 除采购人代表、评标现场组织人员外，采购人的其他工作人员以及与评标工作无关的人员不得进入评标现场。

18.2 见“第六章 评审方法和程序”。

六、授标及签约

19. 定标原则

19.1 评标委员会将严格按照投标文件的要求和条件进行评标,根据评标办法推荐排名前三的投标人为中标候选人，其中排名第一的投标人为第一中标候选人。采购人将确定排名第一的中标候选人为中标人并向其授予合同。排名第一的中标候选人因不可抗力或者自身原因不能履行合同，或者本文件规定应当提交履约保证金而在规定期限未能提交的，或者是评标委员会出现评标错误，被他人质疑后证实确有其事的，采购人将把合同授予排名第二的中标候选人或重新组织招标。如此类推。

19.2 海南海政招标有限公司将在指定的网站上公告投标结果。

20. 质疑处理

20.1 投标人如认为招标文件、招标过程和中标结果使自己的权益受到损害的，应在知道或应知道其权益受到损害之日起七个工作日内以书面形式向海南海政招标有限公司提出质疑，并附相关证明材料。匿名、非书面形式、七个工作日之外的质疑均不予受理。

21. 中标通知

21.1 定标后,海南海政招标有限公司应将定标结果通知所有的投标人。

21.2 中标人收到中标通知后，应在规定时间内到海南海政招标有限公司处领取中标通知书，并办理相关手续。

21.3 中标通知书将是合同的一个组成部分。

22. 签订合同

22.1 中标人应按中标通知书规定的时间、地点与采购人签订中标合同,否则投标保证金将不予退还，给采购人和招标代理机构造成损失的，投标人还应承担赔偿责任。

22.2 投标文件、中标人的投标文件及评标过程中有关澄清文件均应作为合同附件。

23. 招标代理服务费

23.1 根据投标人须知前附表 23.1 款收取。

24.其它

24.1 本项目不召开答疑会。

第三章 用户需求书

一、项目名称

信息管理系统等级保护整改

二、项目概述

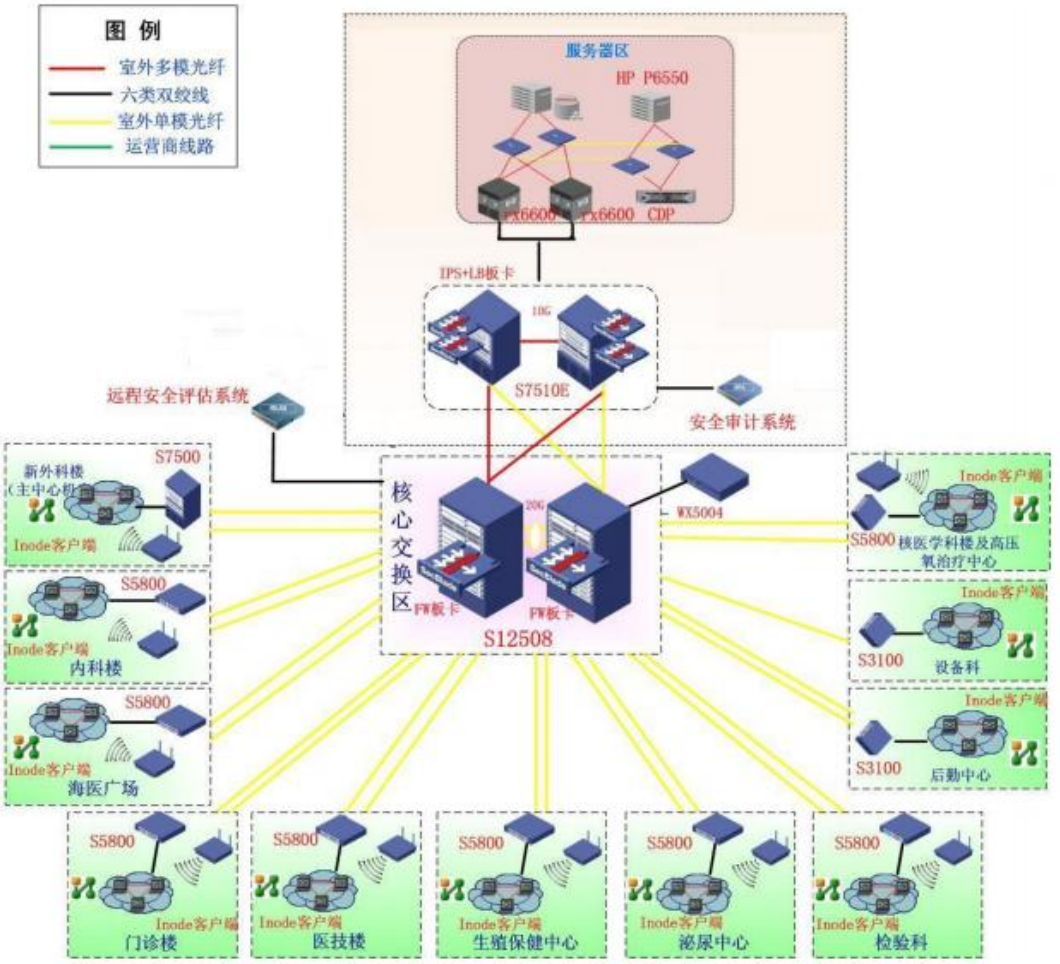
随着信息化应用水平的不断深入和提高，国家和海南医学院第一附属医院自身对信息安全的重视程度和相关要求也越来越高，在此背景下，受海南医学院第一附属医院的委托以《信息技术信息系统安全等级保护基本要求》和《信息技术信息系统安全等级保护测评要求》为基础，依据《信息安全技术信息系统安全等级保护测评过程指南》分别从安全技术类物理安全、网络安全、主机安全、应用安全、数据安全及备份恢复五个层面和安全管理类安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理等五个方面，对海南医学院第一附属医院信息管理系统的安全保护现状进行了客观的访谈和检查。

为达到国家 GB/T 22239-2008《信息技术信息系统安全等级保护基本要求》相应的等级保护能力要求，需对海南医学院第一附属医院信息管理系统启动等级保护安全整改工作的建议与规划方案，以增强系统的安全防护能力，有效抵御内部和外部威胁，切实达到国家及行业信息安全等级保护相应要求，使海南医学院第一附属医院信息管理系统在现有运行环境下风险可控，能够为海南医学院第一附属医院客户及内部各部门提供安全、稳定的业务服务。保证海南医学院第一附属医院相关业务系统达到系统定级相应的等级保护能力要求。

三、项目需求

（以下参数中标注有“★”号的条款必须实质性响应，负偏离（不满足要求）将导致投标无效；“▲”号的条款为重要技术要求，响应程度将影响技术得分。）

（一）海南医学院第一附属医院目前网络结构



信息系统服务器部署在内网服务器区，在网络边界处部署 H3C 板卡防火墙实现基本的安全防护，配备绿盟审计系统实现网络审计，配备绿盟远程安全评估系统进行漏洞扫描，H3C S7510E 交换机上配备 LB 板卡但未启用；各业务科室的无线路由均隐藏 SSID 且绑定 MAC 地址。

（二）系统情况

医院信息管理系统由海南医学院第一附属医院负责建设，目前部署在外科楼十六层的信息中心主机房，由海南医学院第一附属医院信息中心负责技术支撑及运维。海南医学院第一附属医院是该系统的主管单位，同时也是定级的责任单位。该系统实现入院管理、院长查询、住院发药、综合维护、药房管理、药库管理、护士工作站管理、出院管理、门诊发药、门诊收费、手术管理等方面。该系统的保护等级为三级（S3A3G3）。

（三）安全责任制落实情况

单位配置有信息安全领导小组、信息系统负责部门及人员，明确了相关责任部门及人员的信息安全职责，但未制定信息系统建设发展规划文件，存在没有授权审批方面的制度等问题。不利于建立信息安全长效机制，落实信息安全措施，切实履行好信息安全保障责任。

（四）安全管理制度体系建设情况

单位安全管理制度体系建设仍有待进一步完善，当前制定了涵盖物理、网络、主机、应用、数据等方面的安全管理制度。但未制定信息安全总体方针文件，且部分制度存在结构与内容不全面，缺少各岗位操作规程文件（如安全管理员、网络管理员、系统管理员、主机审计员、数据库管理员、机房管理员以及安全审计员等），未定期对安全管理制度体系的合理性和适用性进行审定，不利于保障信息系统的有效运转和信息安全管理工作的开展。

（五）基础设施与网络环境

单位现已建有专用的信息中心主机房，位于外科楼十六层，采取了防雷、防盗、防火、防静电等措施，并配备了电子门禁系统和视频监控，对出入机房的人员进行严格的访问控制；机房配备了 UPS 设备、备用供电系统以及冗余电路，能够保证系统电力供应安全要求；相关申请审批单及运行维护记录保存完整，机房安全措施落实到位。

网络环境方面，单位在网络边界部署了防火墙作为基础防护，主要网络设备提供硬件冗余有效保障系统的高可用性；数据中心部署了 IPS。但重要服务器设备缺乏防毒墙的防护设备，存在一定的安全隐患。

（六）安全控制措施实施情况

在主机安全层面，管理员对服务器和数据库设置了较强的口令，但未定期更换口令；策略上存在的问题主要有未启用登录失败处理功能、未启用登录操作超时锁定功能、以及安全审计功能未开启或开启后未定期对日志记录进行分析、未采用双因子认证进行身份鉴别等；

在应用安全层面，系统具有身份鉴别功能和安全审计功能，在系统访问上做了严格的访问控制，起到了基本的安全防护作用，但系统缺乏口令复杂度设置和登录失败处理功能。另系统在通信完整性、保密性、抗抵赖上的功能也存在不足。另外，通过扫描发现服务器存在高危漏洞，存在较大的安全风险。

（七）系统建设管理情况

当前信息系统已经建成投入使用，本系统明确了安全保护等级并到相关部门进行备案，建设阶段的重要过程文档有工程实施方案、验收报告及交付清单等；但系统建设方面的管理制度仍有缺失，主要体现在缺少工程实施、测试验收以及系统交付等方面的管理制度，不利于对信息系统的建设情况进行统一管理及整体把控。

（八）系统运维管理情况

本信息系统有专人负责日常运维管理，与本信息系统相关联的服务器、数据库、应用系统等均有指定专人或运维商进行统一管理。

在日常运维过程中，缺少相关岗位操作规程及部分记录文档等内容，对系统日常补丁升级、漏洞检查、安全审计记录、恶意代码防范等缺乏统一有效的监管，在系统变更、安全事件处置等方面的管理制度不够完善，制定了应急预案但未进行定期演练。

在数据保护方面，缺乏成文的备份恢复策略指导文件，不利于出现紧急事件时有序的进行应急处理。

综合上述评价结果，本信息系统的总体安全保护状况相对等级保护基本要求有一定的差距，需进一步完善。

（九）主要安全问题

（1）网络层面

1、未部署防毒墙等安全防护设备保护信息系统安全，可能增加被攻击者入侵的风险。

2、未采用两种或两种以上的组合鉴别技术对网络设备用户进行身份鉴别。

3、网络设备未启用登录失败处理功能。

4、部分设备采用明文传输协议 telnet 进行远程管理。

（2）主机层面

1、登录系统用户未采用两种或两种以上的身份鉴别技术对用户身份进行鉴别，采用单一认证方式时，如口令被窃取、监听或暴力破解，则可能被攻击者冒用身份。

2、操作系统和数据库未启用口令复杂度功能，未启用登录失败处理功能，攻击者在网络中任何可达位置对设备用户名、口令进行暴力猜解，造成身份冒用。

3、未对系统日志记录以及定期保存及分析，无法及时发现异常情况。

4、对服务器进行远程管理时，未采取加密措施。

5、系统管理、安全管理以及安全审计等特权用户权限未进行分离。

6、服务器及运维终端未支持恶意代码防范的统一管理，可能会受到木马、蠕虫等病毒的攻击。

（3）应用层面

1、登录系统用户未采用两种或两种以上的身份鉴别技术对用户身份进行鉴别，采用单一认证方式时，如口令被窃取、监听或暴力破解，则可能被攻击者冒用身份。

2、应用系统未提供登录失败处理功能，攻击者在网络中任何可达位置对应用系统用户名、口令进行暴力猜解，造成身份冒用。

（4）安全管理部分

安全管理制度，安全管理机构，人员安全管理，系统建设管理，系统运维管理五大层面建设不够全面和完善，必需的相关制度及其贯彻执行记录部分缺乏，存在一定的管理疏漏，易导致越权滥用、无作为及误操作等安全管理隐患。

1. 设备清单

序号	产品名称	技术要求	数量	单位
1	防毒墙	详见“2.1、防毒墙”中产品技术要求	2	台
2	入侵检测系统	详见“2.2、入侵检测系统”中产品技术要求	1	台
3	安全管理平台	详见“2.3、安全管理平台”中产品技术要求	1	台
4	账号集中管理与审计系统	详见“2.4、账号集中管理与审计系统”中产品技术要求	2	台
5	移动办公接入网关(SSL VPN)	详见“2.5、移动办公接入网关”中产品技术要求	1	台
6	安全服务	详见“2.6、安全服务”中技术要求	1	项

2. 设备技术参数

2.1 防毒墙

序号	指标项	指标要求
1.	性能指标	★标准 2U 机架式设备，支持多核，提供端口不少于 4 个电口、4 个千兆光口，4 个万兆光口，具有 2 对 Bypass 功能，支持双机热备； 网络吞吐量不少于 3Gbps,Http 吞吐量不少于 10Gbps,SMTP 吞吐量不少于 1500 万邮件/小时。
2.	基础网络适应性	支持桥接、路由、NAT、虚拟线等网络部署模式
		支持 PPPOE 拨号设备接入，具备断线重连技术

		支持静态路由；ECMP 路由；OSPF、RIP、BGP 动态路由功能；支持 VLAN 间路由；支持 ISP 路由，并内置 ISP 地址列表；IGMP V1、V2、V3 组播路由协议
		支持基于源、目的 IP 的策略路由；支持基于协议、端口或应用的策略路由 ；支持主备路由，支持配置路由优先级
		支持端口镜像，将设备任一接口数据镜像到观察口，供用户分析
		支持端口聚合功能，实现带宽扩展
		支持 DNS 代理、DHCP client、DHCP server 代理
		支持双向 NAT 技术、静态 NAT 技术、动态 NAT 技术；支持多对一、一对多和一对一等多种方式的地址转换
		▲支持 IPV6 地址/地址组配置，且支持基于 IPV6 地址/地址组配置防火墙安全策略、防病毒策略、文件过滤策略、流量控制策略（提供界面截图）
		支持 IPV6 GRE 隧道技术，支持 IPv6 over 、IPv4 6to4、IPv6 over IPv4 ISATAP 技术；支持 NAT64、DNS64 翻译技术
		支持 IPV6 包过滤、策略路由、静态路由、HTTP 应用协议、自动获取 IPV6 地址
		支持多出口负载均衡，支持轮流、加权最少、权重轮流、最少连接等算法，支持多运营商智能选路
3.	防火墙	支持自定义安全策略，可基于 MAC 地址、IP 地址、端口、服务、应用、时间计划定义安全策略；能识别 2000+种应用
		支持检测 IP 地址盗用，并拦截盗用 IP 地址的主机经过设备的各种访问
		支持基于源 IP/目的 IP 配置并发连接数上限
		支持对 ARP FLOOD 攻击、ICMP FLOOD 攻击、UDP FLOOD 攻击、SYN FLLOD 攻击、DNS FLOOD 攻击、TearDrop 攻击、Smurf 攻击、LAND 攻击、WinNuk 攻击、ICMP 大包攻击进行防护
		支持会话超时时间自定义， 包括：TCP 连接建立、TCP 超时等待、UDP 超时等待
		支持根据源 IP 地址/目的 IP 地址查看会话连接排行； 支持多个维度监控当前所有会话，包括协议、源/目的地址、源/目的端口、状态；
		支持 IP-MAC 绑定，可自动扫描内网设备的 IP-MAC 地址；支持管理员手动配置；支持从外部文件导入 IP-MAC 地址列表；支持配置例外 IP 和例外端口；
4.	病毒木马防护	▲支持特征查杀引擎、机器学习引擎两种防病毒引擎，支持双引擎同时工作；（提供界面截图） 支持快速扫描和文件扫描两种工作模式切换（提供界面截图）
		支持多种文件类型的扫描及多重压缩文件扫描，最高支持 20 层解压
		支持本地库和云端扫描结合的方式；支持病毒库在线和离线更新
		支持基于 IP/IP 组、协议（HTTP、FTP、SMTP、POP3）配置防病毒策略；支持检测并报警、阻断、隔离三种响应处理方式；支持下载/删除隔离区恶意文件
		支持僵尸网络及恶意代码检测，如蠕虫病毒、后门木马、间谍软件等
		支持检测并拦截 HTTP、FTP 电子邮件等协议所携带的恶意代码，并记录拦截日志
		支持 400 万条以上的病毒库，并且可以自动或者手动升级
		提供长达 3 年的病毒特征库升级服务，云端机器学习病毒检测模型升级服务；支持定时升级、离线升级、在线升级；
		支持木马类型报告，提供超过 200 种木马的分析，包括木马文件名、类型、主要特征、分析步骤及结果、验证方法，措施建议和 Snort 规则
5.	网中网管控	▲支持对 WiFi 分享网络中移动终端进行检测，能检测到移动终端的系统类型包括安卓、苹果等，并对 WiFi 分享行为进行管控（提供界面截图）
6.	流量控制	支持基于用户/用户组、IP/IP 组、应用、时间计划的带宽控制策略

		▲支持配置保障通道和限制通道；支持限制同一用户组内单 IP 上下行带宽（提供界面截图）
		支持高、中、低三级通道优先级，支持动态调整带宽、利用空闲带宽
7.	反垃圾邮件	支持基于关键字的内容过滤，对 HTTP 上传，邮件主题、正文、附件名、发件人、收件人进行过滤
8.	信息泄露防护	支持基于文件类型的下载过滤，对 HTTP 上传、FTP 上传、邮件附件进行过滤，
		支持 web 内容过滤，支持自定义正则表达式过滤 web 请求内容/响应内容
9.	URL 过滤	▲支持基于源 IP/IP 组配置 URL 访问控制策略；内置成人类、赌博类、娱乐类等 63 类常见 URL 类型组，用户可快速完成配置；支持配置 URL 过滤策略优先级（提供界面截图）
		▲支持 URL 黑白名单，支持配置黑白名单优先级（提供界面截图）
		支持自定义恶意网站，具备恶意网站过滤功能
10.	系统管理	支持管理员角色三权分立，支持管理员用户名+密码/UKEY 双因子认证；支持按模块为管理员角色配置权限
		支持配置管理员密码安全策略，密码更换时间、密码最小长度等详细要求
		支持配置 IPV4/IPV6 可信管理主机
		支持 SNMP 协议；支持 NTP 协议
		支持图形化系统调试工具；内置抓包工具
		支持按系统备份历史记录回滚
		支持对规则库手动升级，支持配置定时升级，支持自动升级；
		支持为不同 IP/IP 组定制用户认证页面
		支持配置向导，为用户提供常用功能配置指导；支持配置检查功能
		支持集中管理功能，监控所有设备状态；支持统一下发配置，统一更新规则库，日志上报功能
11.	日志审计	支持本地存储日志、syslog 多发日志；支持覆盖、暂停、报警三种日志满响应方式；支持配置日志入库归档周期
		▲支持系统登录日志、恢复与备份日志、重启关机日志、管理员操作日志、资源告警日志、防火墙日志、防病毒日志、信息泄露防护日志、DDOS 攻击防护日志、应用管控日志、URL 访问日志、用户认证日志、网中网检测日志（提供界面截图）
		支持用户自定义日志任务，支持分模块、基于时间、响应方式、协议、源地址/目的地址等维度导出 Excel 格式日志
		支持配置日志审计平台或者第三方日志服务器，提供强大的日志管理和日志审计功能（存储、审计、报表）
		支持导出流量统计报表，支持基于应用、协议、IP/用户等维度统计流量并排行
12.	报警	支持对入侵事件、攻击事件等进行报警，并记录报警数据
		支持对系统运行状态进行报警，如 CPU、内存、带宽超过阈值
		支持邮件、短信、SNMP Trap、声音报警等报警方式
13.	高可用性	支持主-主模式、主-备模式的双机热备
		支持物理设备状态监测，即主防毒墙出现断电或其他故障时，备防毒墙能及时发现并接管主防毒墙的工作
		支持会话状态、配置同步
		支持冗余心条线机制
		支持 VRRP 协议和 STP 协议
		支持链路状态检测的双机热备
		支持基于集群工作模式的负载均衡功能，使多台防毒墙能够协同工作均衡网络

		流量
		支持电源冗余电源；支持电源热插拔；支持业务接口卡热插拔
14.	产品资质（出具加盖厂商公章的复印件）	具备公安部颁发的《计算机信息系统安全专用产品销售许可证》
		▲具备中国人民解放军信息安全测评认证中心颁发的《军用信息安全产品认证证书》
15.	厂商资质（出具加盖厂商公章的复印件）	▲厂商具备 ISO20000、ISO27001 和 CMMI 5 级证书
		厂商具备中国信息安全认证中心（ISCCC）颁发的应急处理服务资质
		具备中国信息安全认证中心（ISCCC）颁发的信息系统安全集成一级资质
		具备中国信息安全评测中心颁发的信息安全服务资质证书
		为省级或省级以上计算机信息网络安全协会指定服务单位

2.2 入侵检测系统

序号	指标项	技术规格参数要求
1.	★性能指标	网络接口：1管理口，7检测口（4光4电）
		最大并发连接数：≥3800000
		最大吞吐量：≥5.4Gbps
2.	产品架构	机架式硬件，专业 IDS 入侵检测设备
		支持多网段、跨网段的多路混合部署
3.	入侵检测	内置攻击规则特征库，规则库规则列表≥8000种
		支持用户自定义特征规则
		支持入侵规避发现，能发现躲避或欺骗检测的行为，如 IP 碎片重组，TCP 流重组、协议端口重定位等等
		支持内置事件调整，可对事件种类、事件说明、事件级别重新编辑
		支持 SYN flood、TCP flood、UDP flood、ICMPflood 攻击检测
		支持多种告警方式，至少包含声音告警、邮件告警、短信告警、snmp trap 等
		▲系统携带的攻击特征库须获得 CVE-Compatible 兼容性认证，CVE 兼容性认证须提供证明文件。
4.	高级威胁检测	▲系统应提供基于信誉的僵尸网络检测能力，具备可以持续升级的信誉库，IDS 通过信誉库内的恶意网站 IP、C&C 服务器地址的信誉值执行相应的检测动作。须提供信誉库界面截图。
		系统应提供服务器异常告警功能，可以自学习服务器正常工作行为，并以此为基线检测处服务器非法外联行为，须提供界面截图。
		▲系统应提供敏感数据外发的检测功能，能够识别通过自身的敏感数据信息（身份证号、银行卡、手机号等），须提供界面截图。
5.	部署能力	系统应提供系统规则和用户规则模板，减少配置工作量，提高部署效率，需提供界面截图。
6.	产品资质	具备公安部颁发的《计算机信息系统安全专用产品销售许可证》

	（出具加盖厂商公章的复印件）	具备国家保密科技测评中心颁发的《涉密信息系统产品检测证书》
		产品要求取得中国信息安全测评中心《信息技术产品安全测评证书（EAL3+）级）》
		投标 IDS 产品应具有 IPv6 Ready Logo 证书，提供有效证书的复印件
7.	厂商资质（出具加盖厂商公章的复印件）	▲厂商具备 ISO20000 和 ISO27001 证书
		厂商具备中国信息安全认证中心（ISCCC）颁发的应急处理服务资质
		具备中国信息安全认证中心（ISCCC）颁发的信息系统安全集成一级资质
		具备中国信息安全评测中心颁发的信息安全服务资质证书
		厂商须获得中国信息安全测评中心颁发的：信息安全服务资质证书-风险评估类（二级），提供证书复印件；
		产品厂商获得互联网安全研究中心颁发的应用安全联盟会员认证，提供会员证书复印件。
		▲产品厂商获得网络安全应急服务支撑单位证书（国家级），提供证书的复印件。
		厂商须获得中国信息安全测评中心颁发的：信息安全服务资质证书（安全工程类二级）、信息安全服务资质证书（安全开发类一级），须提供以上两个证书的复印件。

2.3 安全管理平台

序号	指标项	技术规格参数要求
1.	系统架构	开放式设计：平台化设计，功能模块插件化，用户可以自主选择需要的功能模块，或在现有平台上进行客户化定制
		分布组件：各功能组件之间采用网络方式进行通讯，各组件可以分布安装在不同的机器上，以支持大规模和灵活的部署
		采用业界主流的 B/S 方式，通过 SSL 加密通信
2.	性能参数	管理资产数量≥100 标准资产
		日志保存时间：3 个月
		最大日志记录条数为：1 亿条
		日志分析结果保存天数：365 天
		事件处理能力：3000 条/秒
3.	部署方式	单机部署：各组件集中式部署
		分布式部署：采集器和分析引擎支持分布式部署，可根据实际需要灵活扩容
		级联部署：下级 SOC 可将告警信息，日志信息汇报给上级 SOC
4.	资产管理	支持对资产属性的定义，资产属性包括：资产名称、资产类别、IP 地址、资产价值、厂商信息、资产版本、所属部门、所属区域、地理位置、责任人等信息

		支持对资产的新增，删除，修改，导出，导入等操作
		支持资产设备自动发现
		支持对资产进行多条件组合的检索查询
		支持资产漏洞导入，查看和漏洞统计
		支持资产风险值计算模型，可用风险值量化单设备风险和整个网络的风险情况
		▲支持资产健康度计算模型、可信度计算模型，可用健康值和可信值量化表示
5.	设备管控	支持对网络设备、安全设备、主机、服务器等设备的监控
		支持 CPU 使用率、内存使用率、磁盘使用率、进程信息、软件信息、网口流量信息等设备状态的监控，并可图形化展示
		支持 ssh，snmp，bdsec 接口进行设备管理，设备管理包括：重启、关机、时间同步、关闭服务、启动服务、策略备份、策略下发等。
6.	拓扑管理	▲可自动发现网络设备及其网络连接情况，获取最初的网络拓扑信息，并通过拓扑图展示(提供界面截图)
		★可在拓扑图上查看某个网元的基础信息（设备名称、设备类型、设备厂商、操作系统等），运行状况（cpu、硬盘、内存使用率等），事件情况（上报事件、发起事件、受影响事件等），告警情况
		可查看网元间网络连通情况，流量信息等
		可在拓扑图上对设备进行管控操作，包括关机、重启、时间同步等
		用户可手工编辑拓扑，包括节点属性编辑，网元连接线编辑，拓扑背景图更换，拓扑区域划分
		支持选择不同的地理域、设备类型、组织架构等维度信息，从不同维度查看拓扑图
		可通过拓扑图运维工具集中进行运维，运维工具包括 ping，traceroute 等
7.	业务管理	支持业务建模，录入业务系统信息，包括系统名称、责任人、相关设备、相关支撑服务等
		可定期对业务系统关键 URL 的可访问情况进行检查,可检测 URL 是否可达，访问延时等
		可根据业务建模自动生成三层业务拓扑图，用户可修改编辑业务拓扑图
		支持通过拓扑图直观展示故障业务系统的支撑服务告警情况，主机设备基本信息、事件信息、告警信息、漏洞信息等情况，帮助用户分析判断业务故障的原因
		支持业务异常数统计，内置业务健康度计算模型，可通过业务健康值和业务异常数图示化标识可能存在故障的系统
8.	IT 资源监控	▲可监控多种中间件,数据库的运行指标情况,包括 weblogic,tomcat,apache,iis 等中间件，包括 mysql，oracle，sqlserver，db2，sysbase 等数据库（提供界面截图）
		内置监控对象，对象模型，对象指标等一系列完整的指标体系，用户可选择监控对象后简单录入配置信息即可实现监控
		可通过扩展适配器的方式，与不同网管系统，运维平台对接，获取监控数据

9.	蜜罐管理	▲支持模拟开放服务端口，引诱攻击者入侵，并记录入侵行为数据（提供界面截图）
10.	自动巡检	▲支持用户按周或者按月制定周期巡检任务，系统可自动执行巡检脚本，完成设备连通性、运行状态、运行进程等项目的自动巡检，支持巡检报告导出（提供界面截图）
11.	应急管理	▲支持应急资源的录入与查询（提供界面截图）
		支持应急预案的制定
		支持应急事件录入与查询
		支持应急演练计划制定与查询
12.	等保测评	▲支持根据待评级的等保级别，列出对应等保级别所需满足的测评项目（提供界面截图）
		支持根据各测评项目检查情况录入或者选择对应的检查结果，支持根据结果生成测评整改分析报告，并可产生统计报表
13.	流量分析	支持通过动态推移图的方式直观展示实时流量情况
		支持按照不同维度对流量进行统计
		▲支持异常流量分析，内置基线学习引擎，学习多种维度的流量基线，用户可配置基线策略，通过基线策略和流量基线分析异常流量（提供界面截图）
14.	漏洞管理	▲支持对多个厂家多种型号的漏扫设备漏扫报告的导入，导入数据包括漏洞端口、漏洞级别、漏洞名称、ip 地址、漏洞类型、漏洞 CVE 号、漏洞 SID 号（提供界面截图）
		可根据漏洞生成漏洞报表，可利用漏洞数据产生预警和进行关联分析
15.	事件管理	支持 syslog、snmp trap、文件、wmi、opsec 协议的日志采集，支持网络设备、安全设备、服务器、数据库、中间件、应用系统等多种软硬件设备的日志采集
		日志采集策略设置，可过滤指定来源的日志
16.	关联分析	支持多维度多场景的关联分析，支持通过统一配置方式增加或者修改关联模型
		支持事件规则关联、情报关联、资产关联、流量关联、指标关联等多种组合关联
17.	风险分析	提供符合 bs7799/iso17799 标准的资产风险分析和风险计算方法，风险按照国际标准划分为 5 级
		用户可以从资产风险追踪到相关的高风险事件，有效判断资产风险的来源，并进行正确的处理
18.	行为及信息监控	▲支持通过部署行为监测探针，可获取终端的违规行为信息，包括违规终端 IP，违规行为类型，违规时间（提供界面截图）
		▲支持通过部署信息监测探针，可监测内网的敏感信息内容，当出现敏感信息后，系统将触发告警，告警信息包括，告警主机 IP，告警时间，敏感内容详情（提供界面截图）
19.	异常事件分析	▲支持按照事件数量、事件类型、事件目标、事件协议等维度，依照某一学习周期学习并生成基线（提供界面截图）
		支持设置基线偏离阈值，设置事件正常发生时间范围等条件，系统可根据条件检测异常事件

20.	报表管理	系统预置丰富的系统报表，充分满足用户的需求。报表支持多种格式的显示
		报表的生成方式分为手工报表和自动报表两种，手工报表可以直接支持生成，自动报表可以按照每小时、每天、每月、每年等周期的方式生成
		提供多种展现仪表盘，包括柱状图、折线图、饼状图、视网膜图、雷达图、热力图提供用户可定制 Top N 展示图表
21.	可视化分析	网络态势：支持展示基于 GIS 地图的攻击路径、攻击事件统计、威胁类型分布、设备产生日志总量趋势统计、整体安全风险系数、攻击事件列表等
		流量态势：支持展示基于 GIS 地图的流量热力图、外部源流量统计、协议类型统计、源和目的流量关系统计、资产总流量趋势统计、基于流量发现攻击事件列表等
		脆弱性态势：支持展示漏洞数量统计、漏洞类型统计、漏洞与资产关联关系统计、脆弱性利用分析等
22.	分布式采集器管理	▲支持分布式采集，通过传感器实现不同协议不同类型数据的统一传输，通过插件的方式实现采集方式的扩展（提供界面截图）
		支持传感器管理，实现对所有传感器运行状态的查看，和对传感器的启停控制
		支持插件管理，包括对各种采集插件的启停控制，状态查看，以及插件运行策略的设置
23.	合规检查	支持系统弱口令检查：检查系统或者应用是否存在弱口令，定期进行检查，并产生告警
		支持防病毒软件检查：定期检查系统是否有安装基线配置的防病毒软件，如果未安装，则产生告警
		支持软件安装记录检查：定期检查系统是否有私自安装非法软件，如果未安装，则产生告警
		支持软件卸载记录检查：定期检查系统是否私自卸载必须软件，如果检查到卸载记录，则产生告警
		支持系统进程与服务黑白名单检查：定期检查系统是否有启动非法进程，如果有启动，则产生告警
		支持网络连接异常监控：定期检查系统是否网络连接异常，如果连接异常，则产生告警
24.	黑客行为分析	反向拍照：可对攻击源进行反向拍照，获取攻击源的地域、操作系统等详细信息，以供后续取证
		攻击处理知识库：提供攻击事件的防范处理知识，帮助管理员快速解决问题
25.	联动功能	▲为了建立统一安全管理联动平台，与防毒墙必须同一品牌，提供原厂商联动证明原件
26.	产品要求（出具加盖厂商公章的复印件）	产品具备国家版权局颁发的软件著作权登记证书
		获得公安部颁发的《计算机信息系统安全专用产品销售许可证》
		产品具备国家保密局涉密信息系统安全保密测评中心颁发的涉密信息系统产品检测证书
		产品具备 IPV6 认证
27.	厂商资质（出具加盖厂商公章的复印	▲厂商具备 ISO20000、ISO27001 和 CMMI 5 级证书
		厂商必须具备中国信息安全认证中心（ISCCC）颁发的应急处理服务资质

	件）	具备中国信息安全认证中心（ISCCC）颁发的信息系统安全集成一级资质
		具备中国信息安全评测中心颁发的信息安全服务资质证书
		为省级或省级以上计算机信息网络安全协会指定服务单位

2.4 账号集中管理与审计系统

序号	指标项	技术规格要求
1.	产品架构	支持双机热备
		支持冗余网卡，允许将两张网卡绑定在一起使用，两张网卡同时使用一个 IP，当一张网卡有问题的时候另一张可以继续使用
		支持 VMware、KVM、XEN 等主流虚拟化平台以及第三方虚拟化平台部署
		支持 Docker 部署
2.	★性能指标	支持100许可；
		接口：4个百兆/千兆自适应电口；1个 Console 接口，2个 USB 接口
		审计日志存储空间≥1.5T；
		到目标设备的连接时间不大于2秒；
		MTBF 不少于6万小时；
3.	支持操作协议	终端命令操作：Telnet、SSH；
		远程桌面： RDP、VNC；
		文件上传和下载： FTP、SFTP；
4.	用户管理	用户帐号实名制：根据具体的维护人员添加唯一与其身份对应的用户，实现维护人员身份的唯一性管理
		可以设定活动、禁用两种用户帐号状态，当用户在一定时间内连续输错密码时，可以自动禁用该用户帐号
		▲支持静态密码、USBKEY 形式双因子认证；支持 AD 域、LDAP 域、Radius 网络认证方式；支持短信验证码、手机 APP 验证码、数字证书等动态口令认证；支持根据不同用户采用不同静态认证与动态认证的任意组合（提供界面截图）
		支持忘记密码后通过邮箱找回密码
		支持三权分立的原则和要求，审计员、管理员、运维人员职、权分离
		▲支持批量定时修改设备密码，支持随机生成不同密码、随机生成相同密码以及手工指定相同密码的密码策略，并严格遵守密码强度设置，修改后的设备密码可以以邮件的方式发送给密码管理员（提供界面截图）
		用户帐号支持导入导出功能
5.	多级部门管理	▲支持多级部门管理功能，增加部门管理员和部门审计员，不同的用户和设备归属于不同的部门（子部门），不同部门的配置管理员只能针对自己部门及自己直属子部门设备进行访问权限设置，上级管理员可以对下级的管理员授权管理（提供界面截图）
6.	智能发现	▲能对 IP 地址段进行扫描，识别出该 IP 地址段内开放的应用类型、服务、端口等信息，支持一键添加管理功能（提供界面截图）
7.	审计内容	SSH、Telnet 字符命令界面操作审计
		FTP、SFTP 文件上传、下载、删除、改名等操作的审计
		VNC、RDP 远程桌面操作审计

		HTTP、HTTPS 操作审计
		支持 FTP/SFTP 方式文件上传的副本备份，可供审计员审计查看
		支持磁盘映射方式文件上传的副本备份，可供审计员审计查看
8.	数据库运维操作审计	审计包括访问起始和终止时间、用户名、用户 IP 地址、目标设备 IP、设备名称、数据库类型、操作内容等；支持操作内容录像回放
9.	安全策略	IP 策略：可以允许或拒绝指定的 IP 登录管理界面，还可以按照用户的需要指定用户或设备在一个指定 IP 或 IP 段下才可以对设备进行访问管理
		密码策略：可以指定密码有效期、密码复杂度设置
		防绕策略：可以指定 IP 或 IP 段进行防绕是否阻断与是否产生告警记录的选择
		时间策略：可以指定用户或设备在一个指定的时间段内有效。可以按照用户的需要定制时间白名单
10.	文件传输检测控制	▲支持文件上传下载（ftp/sftp)方式下对文件/文件夹标题及内容检测，及时发现敏感信息，对违规的下载或上传操作进行拦截或者产生后台告警，避免重要数据泄露（提供界面截图）
11.	图形用户行为审计	▲实现对远程桌面中的客户端操作动作进行识别分类等，能够识别文件的打开、删除、重命名，活动窗口的检测、菜单点击，键盘输入检测等动作。审计人员能够通过关键信息快速过滤和定位到目标位置，查看关键操作，提升审计效率（提供界面截图）
12.	工单管理	▲支持工单申请和下发，授权运维人员根据授权在指定时间内访问指定资源，申请内容包括设备 IP、设备账户、运维有效期、备注事由等，运维工单可以邮件方式通知管理员（提供界面截图）
13.	无感知应用发布	▲可通过无感知应用发布的方式进行协议扩展，支持 B/S 和 C/S 方式的通用及专有的运维客户端程序，支持远程应用本地化展示、支持应用的单点登陆功能（提供界面截图）
14.	管理向导	▲通过设备管理向导完成设备从添加到授权的步骤；通过应用管理向导可以完成应用从录制配置文件到授权的步骤（提供界面截图）
15.	图形展示	▲首页访问关系图形展示，根据用户、设备、应用的不同颜色区分，通过连接图形直观展示用户对设备或应用的访问关系（提供界面截图）
16.	自动化运维	▲管理员可以根据设备/设备组、系统账号、时间、脚本内容（自定义）， 创建自动脚本任务；该任务到期自动执行，执行的结果自动发送给相关管理员（提供界面截图）
17.	报表管理	支持通过时间、用户、账号、源 IP、目标 IP、完成状态进行会话浏览排名统计
		支持应用浏览的排名统计和播放、下载
		提供拦截日志和防绕日志的查询和报表导出
		提供系统登陆日志、系统操作日志等自身审计日志和多种报表，给企业考核提供依据
18.	联动功能	为了建立统一安全管理联动平台，与安全管理平台必须同一品牌，提供原厂商联动证明原件
19.	产品资质（出具加盖厂商公章的	具备国家版权局颁发的《软件著作权登记证书》
		具备公安部颁发的《计算机信息系统安全专用产品销售许可证》
		具备国家保密科技测评中心颁发的《涉密信息系统产品检测证书》

	复印件）	具备中国信息安全认证中心颁发的《IT 产品信息安全认证证书》（ISCCC）
		具备中国人民解放军信息安全测评认证中心颁发的《军用信息安全产品认证证书》
		具备中国质量认证中心颁发的《中国国家强制性产品认证证书》（CCC）
		具备中国质量认证中心颁发的《中国节能产品认证证书》
		产品具备 IPV6 金牌认证
20.	厂商资质（出具加盖厂商公章的复印件）	▲厂商具备 ISO20000、ISO27001 和 CMMI 5 级证书
		厂商必须具备中国信息安全认证中心（ISCCC）颁发的应急处理服务资质
		具备中国信息安全认证中心（ISCCC）颁发的信息系统安全集成一级资质
		具备中国信息安全评测中心颁发的信息安全服务资质证书
		为省级或省级以上计算机信息网络安全协会指定服务单位

2.5 移动办公接入网关

序号	指标项	技术规格
1	**部署方式参数**	支持网关模式、单臂模式部署两种方式；SSLVPN 加密速度≥480Mbps SSLVPN 每秒新建用户数≥400 防火墙吞吐量≥2.2Gbps 最大并发会话数目≥1600,000 网络接口≥6 个千兆电口、4 个≥千兆光口 尺寸≥2U;冗余电源
2	**安全性**	支持终端使用包括 IE6、7、8、10、11 或其他 IE 内核的浏览器，以及最新版本的非 IE 内核浏览器，如 Windows EDGE，Google Chrome，Firefox，Safari，Opera 最新版登录 SSLVPN 系统，登录后可完整支持各种 IP 层以上的 B/S 和 C/S 应用。（提供截图证明并加盖原厂公章）
3	**高性能**	支持启用多线路时，自动检测故障线路，并自动踢出故障线路；一旦线路恢复，可在一定时间内自动恢复。支持启用多线路时，自定义用户访问选路策略，包括按上/下行带宽，轮询，按优先级等方式。（提供截图证明并加盖原厂公章）
		▲支持利用网页进行动态寻址的方法，客户端无需安装插件、不依靠 IP 地址库、不依赖于第三方动态 IP 寻址、直接根据速度探测实现用户端接入线路的自动优选,用户通过访问寻址代理页面（简称 Webagent 页面），通过 Webagent 页面自动寻找 VPN 设备 IP(非 DDNS),该方法不必单独注册域名或占用 IP 地址，大大降低了系统部署难度。（提供截图证明并加盖原厂公章）
		支持针对不同的 web 页面进行数据优化，支持动态压缩技术，基于数据流进行压缩，减少不必要的数据传输。（提供截图证明并加盖原厂公章）
		▲针对 B/S 资源支持 WebCache 技术，动态缓存页面元素，提高 Web 页面响应速度。支持流缓存技术，实现网关与网关、网关与移动客户端之间进行多磁盘、双向、基于分片数据包的字节流缓存加速，削减冗余数据，降低带宽压力的同时提高访问速度；支持共享流缓存功能，实现多分支网关在总部共享流缓存数据，提高流缓存效果（提供截图证明并加盖原厂公章）

4	**厂商资质**	提供中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》（提供证书复印件并加盖厂家公章） 提供产品 IPV6 Ready 认证证书(提供证书复印件并加盖厂家公章） ▲要求厂商具有 CMMI 5 级认证。（提供证书复印件并加盖厂家公章） ▲设备生产厂商需为国家密码管理局发布的《SSL VPN 技术规范》起草单位之一（提供相关证明并加盖厂家公章） ▲要求厂商是微软安全响应中心（Microsoft Security Response Center）发起的 MAPP（Microsoft Active Protection Program）计划成员，可在微软发布每月安全公告之前获得微软产品的详细漏洞信息，为用户提供更及时的安全防护。（提供相关证明并加盖厂家公章） 提供公安部信息安全产品检测中心颁发的《GA/T 686-2007 信息安全技术 虚拟专用网安全技术要求》三级或三级以上检测报告（三级以上为四级、五级）（提供证书复印件并加盖厂家公章）

2.6 安全服务

2.6.1 安全加固服务：针对安全扫描过程中发现的安全漏洞，在可控的范围下，对操作系统、数据库、中间件发现的安全漏洞进行加固。

2.6.2 应急体系建设和应急演练：根据国家和卫计委有关信息安全应急体系建设要求，结合医院实际情况，制定应急预案，并定期组织应急模拟演练，并做好应急演练总结。

2.6.3 应急响应服务：当用户单位遭受网络病毒/木马、黑客入侵、DOS 攻击等安全事件时，服务商在第一时间派出安全专家进行现场排查处理，保障业务系统的连续性，阻止和减小安全事件带来的负面影响。

2.6.4 安全培训服务：以实际业务运作为立足点，注重理论和实操结合，通过理论讲授、实验操作、问题讨论等方面，普及安全教育，提高安全意识，提高安全防范能力。主要内容包括网络安全的相关法律法规培训、各种网络攻击技术原理及防御培训、网络安全策略及安全管理培训、常用网络安全产品原理及应用培训等服务。

2.6.5 原厂服务：设备提供 3 年售后服务（软件升级、硬件质保）。必须提供 7×24 小时电话支持；应急服务紧急攻击事件 2 小时内响应，最大限度减少损失。提供两个名额的原厂培训（含参加认证考试）。

四、项目相关要求

1、工期或交货期

合同签订后 30 天内。

2、投标人必须提供详细的保修期内技术支持和服务方案，技术支持和服务方案包括（但不限于）：

1）整体工程提供不少于 3 年的免费维护，设备按原厂商标准提供维护。质保期内免费提供保证系统正常运行的全部备件及维护，免费提供系统运行所需软件的维护服务及最新版本。

2）提供不少于 3 年 5×8 小时上门保修，免费更换全部配件；提供 7×24 小时技术支持和服务，1 小时内作出实质性响应，对重大问题提供现场技术支持，4 小时内到达指定现场。

3、培训要求：

在项目建设过程中需对相关人员进行技术培训，在以后系统运行过程中亦需根据具体情况进行相应内容的培训，以保证系统的管理人员、技术人员和应用人员能够及时、准确地了解和熟练地运行系统。

4、投标人必须根据所投产品的技术参数、资质资料编写投标文件。在中标结果公示期间，采购人有权对中标候选人所投产品的资质证书等进行核查，如发现与其投标文件中的描述不一，代理机构将报政府采购主管部门严肃处理。

5、投标人必须如实地对招标文件中各项技术要求作出明确的逐项响应承诺，并对其真实性负责。

投标货物（含软件部分）的技术响应情况必须在《技术及资质响应表》中完整体现。

6、投标人的报价应包括本项目建设所有货物、运输、安装、集成、调试、试运行、服务、税等费用。

第四章 合同条款

甲方：_____

乙方：_____

甲乙双方根据____年____月____日信息管理系统等级保护整改（项目编号:HZ2018-370）公开招标结果及招标文件的要求,经协商一致,同意以下专用条款作为本项目合同条款的补充。当合同条款与专用条款不一致时，以专用条款为准。

一、合同标的及金额等(详见附件清单)

序号	项目名称	项目内容	单价（元）	数量	单位	合计（元）	备注
1							
2							
合同总额		（小写）：￥ 元					
		（大写）： 元整					

二、合同通用条款

（双方友好协商）

三、付款方式

与采购人协商决定

三、违约赔偿

1. 除下一条规定的不可抗力外，如果乙方没有按照合同规定的时间交货和提供服务，甲方可从合同款中扣除违约赔偿费，每延迟一个工作日迟交货物（含软件及相关服务）或未提供服务或提供产品及服务不满足项目需求，按合同金额的 1%/天计扣违约赔

偿费。但违约赔偿费的最高限额为合同金额的 10%。如果乙方延迟交货时间超过一个月，甲方有权终止合同，并按合同约定及法律规定追究乙方的违约责任。

2. 如果双方中任何一方由于战争、严重火灾、水灾、台风和地震以及其它经双方同意属于不可抗力的事故，致使合同履行受阻时，履行合同的期限应予以延长，延长的期限应相当于事故所影响的时间。

四、合同纠纷处理

本合同履行过程中发生纠纷，应协商解决，协商不成，可向人民法院提起诉讼解决。

五、合同生效

本合同由甲乙双方签字盖章后生效。

六、合同鉴证

招标代理机构应当在本合同上签章，以证明本合同条款与招标文件、投标文件的相关要求相符并且未对采购内容和技术参数进行实质性修改。

七、本合同的组成文件

1. 合同通用条款和专用条款；

2. 招标文件、乙方的投标文件和评标时的澄清函（如有）；

3. 中标通知书；

4. 甲乙双方商定的其他必要文件。

上述合同文件内容互为补充，如有不明确，由甲方负责解释。

八、合同备案

本合同一式陆份，中文书写。甲方执叁份，乙方、招标代理机构各执一份，另外一份由招标代理机构报政府采购主管部门备案。（如果甲方或乙方需要，则可在此增加合同份数。如果不是财政性资金或没有报财政部门审批的项目，则无需提供备案合同）。

甲方： _____ **（盖章）**　　**乙方：** _____ **（盖章）**

地址：_____　　地址：_____

法定（或授权）代表人：_____　　法定（或授权）代表人：_____

开户行：_____　　开户行：_____

户名：_____ 户名：_____

帐号：_____ 帐号：_____

_____年___月____日 _____年___月____日

招标代理机构声明：本合同标的经海南海政招标有限公司依法定程序采购，合同主要条款内容与招投标文件的内容一致。

招标代理机构：海南海政招标有限公司（盖章）

经办人：_____

_____年___月____日

第五章 投标文件内容和格式

请投标人根据本招标文件要求，按以下格式、内容制作投标文件，并按以下顺序编制目录及页码：

1、投标函（表 1）

2、开标一览表（表 2）

3、技术及资质要求响应表（表 3）

4、投标人简介（包含且不限于从业人员人数、上年度营业收入等）

5、企业提供营业执照副本、税务登记证、组织机构代码证（或三证合一）复印件，事业单位提供事业单位法人证书，以及投标人资格要求中的所有材料复印件

6、保证金缴纳证明复印件

7、企业纳税证明或者会计师事务所出具的财务审计报告

8、社会保障缴费记录复印件

9、授权委托书（表 4，报价文件正本原件，副本复印件）

10、法人代表、授权代表身份证复印件

11、参加政府采购活动前三年内，在经营活动中没有重大违法记录的声明函（表 5，同时提供信用中国或中国政府采购网信用查询页面截图）

12、同类项目业绩表（表 6）

13、生产厂商授权书（表 7）

14、技术部分（包括设计方案、实施方案、所投产品彩页、技术资料、售后服务、培训等）

15、投标人认为需要的其它材料

为了便于评委对报价文件内容的审核，投标人可针对招标文件第六章中“技术、商务评分表”编写响应页码索引表，即投标文件中关于该评分项目内容的页码。

注：以上复印件均需要加盖公章或投标专用章

表 1、投标函

致：海南海政招标有限公司

根据贵单位项目编号为_____的投标邀请函，正式授权下述签字人____（姓名和职务）代表投标人_____（投标单位名称）提交投标文件。

根据此函，我们宣布同意如下：

1、我方接受招标文件的所有的条款和规定。

2、我方同意按照招标文件第二章“投标人须知”的规定，本投标文件的有效期为从投标截止日期起计算的 60 天，在此期间，本投标文件将始终对我方具有约束力，并可随时被接受。

3、我们同意提供贵单位要求的有关本次投标的所有资料或证据，并保证资料、证据的真实有效性。

4、我方完全理解贵方不一定要接受最低投标价的投标，即**最低投标价不是中标的保证**。

5、如果我方中标，我们将根据招标文件的规定严格履行自己的责任和义务。

6、如果我方中标，我方将按规定支付本次招标的服务费。

投标人名称：_____（公章）

地址：_____邮编：_____

电话：_____传真：_____

授权代表：_____（签字或私章）_____ 职务：_____

日期：_____

表 2、开标一览表

项目名称：信息管理系统等级保护整改

项目编号： HZ2018-370

工期/服务期：_____

序号	项目名称	项目内容	单位	数量	单价	小计
1						
2						
3						
4						
5						
…						
投标总额		（小写）				
		（大写）				

投标人全称：（盖章） 授权代表：（签名或私章）

注：1、投标总金额包括本包招标书中要求的所有货物、运输、安装、集成、调试、试运行、服务、税等费用；

2、开标一览表格式不得自行改动。

表 3、技术及资质响应表

说明：投标人必须仔细阅读招标文件中所有技术规范条款和相关功能要求，并对所有技术规范、功能条目及资质要求列入下表，未列入下表的视作投标人不响应。带▲或★的指标列入下表时，必须在指标前面保留▲或★。**投标人必须根据所投产品的实际情况（技术资料）如实填写，评标委员会如发现有虚假描述的，该投标文件无效，该投标人列入黑名单，并报政府采购主管部门严肃处理。**

序号	设备/项目	招标文件技术参数/功能要求	投标人技术参数/功能响应描述	偏离情况	页码索引
1					
2					
3					
4					
5					
	…				

投标人全称：（公章） 授权代表：（签字或私章）

注：1、此表为表样，行数可自行添加，但表式不变。

2、**此表后面按响应顺序附上第三章中要求的各产品资质文件、检测报告等复印件（如有），否则视为不满足**。

3、投标人在“投标人技术参数/功能描述” 中填写所投设备/项目的详细技术参数或功能描述情况，投标人必须如实填写，**不得拷贝“招标文件技术参数/功能描述”要求，否则视为不满足**。

4、偏离情况说明分正偏离、完全响应、负偏离，分别表示优于要求、满足要求、不满足要求。**评委评标时不能只根据投标人填写的偏离情况说明来判断是否响应**，而应认真查阅“投标文件技术参数/功能响应”内容以及相关的技术资料判断是否满足要求。

5、“页码索引”指“投标人技术参数/功能描述”所对应证明材料在投标人投标文件中的页码。

表 4、授权委托书

致 海南海政招标有限公司：

本授权书声明：

委托人：_____

地　址：_____ 法定代表人：_____

受托人：姓名_____ 性别：____ 出生日期：____年__月__日

所在单位：_____职务：_____

身 份 证：_____联系方式:_____

兹委托受托人_____代表我方参加海南海政招标有限公司组织的信息管理系统等级保护整改（项目编号为：HZ2018-370 ）的招标活动，并授权其全权办理以下事宜：

1、参加投标活动；

2、出席开标评标会议；

3、签订与中标事宜有关的合同；

4、负责合同的履行、服务以及在合同履行过程中有关事宜的洽谈和处理。

受托人在办理上述事宜过程中以其自己的名义所签署的所有文件我方均予以承认。受托人无转委托权。

委托期限：至上述事宜处理完毕止。

委托单位 （公章）

法定代表人 （签名或私章）

受托人 （签名或私章）

_____年_____月_____日

表 5、参加政府采购活动前三年内，在经营活动中没有重大违法记录的声明函

致：海南海政招标有限公司

为响应贵公司组织的信息管理系统等级保护整改（项目编号为：HZ2018-370 ）货物及服务的招标采购活动，我司声明如下：

本项目招标公告前三年内，我司在经营活动中没有被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单等重大违法记录。

如有虚假，我司愿意接受相关处罚。

特此声明。

投标人名称：_____（公章）

地址：_____邮编：_____

电话：_____传真：_____

授权代表：_____（签字或私章）_____ 职务：_____

日期：_____

注：提供信用中国或中国政府采购网信用查询页面截图

表 6、投标人项目业绩表

项目名称：信息管理系统等级保护整改

项目编号： HZ2018-370

序号	项目名称	项目内容	合同金额	签约时间	业主联系人电话	备注

投标人全称（公章）： 授权代表（签名或私章）：

注：1、在此表后面按顺序附上各项目的合同复印件。

表 7、生产厂商授权书

海南海政招标有限公司：

作为设在_____（制造厂家地址）的制造/生产_____（货物名称）的_____（制造厂家名称）在此以制造厂的名义授权_____（投标人名称和地址）用我厂制造的上述货物参加海南海政招标有限公司组织的采购项目编号为 HZ2018-370 的信息管理系统等级保护整改的投标活动及后续的合同谈判和签署合同。

我们在此保证以合作人来约束自己，并为上述投标人就此次招标而提交的货物承担全部质量保证责任及按招标文件要求提供售后服务。

（可增加其它服务承诺内容）

我方于_____年____月____日签署本文，以此为证。

投标人名称：_____

出具授权书的制造厂家名称：_____

姓　　名：_____（制造厂授权代表签名或私章）

职　　务：_____　　联系电话：_____

公　　章：_____　　日　　期：_____

注：1、如投标人所投产品为国外品牌产品，生产厂家在国内有注册分支机构的由注册分支机构出具授权，否则由国内的总代理出具授权（总代理需附上代理证明）。所投产品为国内品牌产品的，由生产厂家或负责该区域的分公司或注册机构出具授权。

2、授权出具单位如有内部格式授权书，可以按其格式出具，但必须包含上述格式文件的意思表达。

3、制造厂盖章可以为公章或授权专用章。

4、制造厂商参与投标则无需提供此授权书。

第六章　评审办法和程序

一、评审办法和步骤

1、评标办法采用综合评分法。

2、评标步骤：先进行资格审查，然后由评标委员会进行符合性审查以及技术、商务的详细评审。只有通过资格审查、符合性审查的投标人才能进入详细评审。

二、资格审查

1. 根据财政部第 87 号令第四十四条的规定，采购人、招标代理机构对投标人的资格进行审查。

2. 采购人、海南海政招标有限公司根据“资格审查表”（附表 1）对投标人的资格性进行评审，只有对“资格评审表”（附表 1）所列各项作出实质性响应的投标文件才能通过资格评审。有以下情况的将不能通过初步评审：

- 投标人未能满足投标人资格要求的；
- 投标人未按招标文件要求的金额提交投标保证金的；
- 投标有效期不足的；
- 不符合招标文件规定的其它条件。

3. 判断投标文件的响应与否只根据投标文件本身，而不寻求外部证据。

4. 通过资格审查的投标人不足三家，则本次招标失败。

三、符合性审查

1. 评标委员会根据“符合性审查表”（附表 2）对通过资格审查的投标文件的符合性进行评审，只有对“符合性审查表”所列各项作出实质性响应的投标文件才能通过符合性审查。对是否实质性响应招标文件的要求有争议的投标内容，评标委员会将以记名方式表决，得票超过半数的投标人有资格进入下一阶段的评审，否则将被淘汰。

2. 判断投标文件的响应与否只根据投标文件本身，而不寻求外部证据。

3. 评标委员会在符合性审查中，对算术错误的修正原则如下：

（1）开标一览表内容与投标文件中明细表内容不一致的，以开标一览表为准

（2）投标文件的大写金额和小写金额不一致的，以大写金额为准；

（3）总价金额与按单价汇总金额不一致的，以单价金额计算结果为准；

（4）单价金额小数点有明显错位的，以总价为准并修改单价。

（5）若投标人不同意以上修正，投标文件将视为无效。

4.评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，将要求其在评标现场接到通知后 20 分钟内提供书面说明，必要时提交相关证明材料。投标人不能证明其报价合理性的，评标委员会将其作为无效投标处理。

5.通过符合性审查的投标人不足三家，则本次招标失败。

四、详细评审

1. 评标委员会根据评审办法对通过初步评审的投标文件进行详细评审，并进行技术和商务的评审打分。

2. 技术、商务评分：具体评审的内容详见（附表 2）；

3. 价格分统一采用低价优先法计算，将通过初步评审的所有投标人最低的投标价格，即满足招标文件要求且价格最低的投标价为基准价，其价格分为满分。其他投标人的价格分统一按照下列公式计算：

价格分=(基准价 / 投标报价)×价格权值×100

4. 如投标人满足第二章第 17 条“关于政策性加分”规定的，应按该条规定对投标人的评标价进行调整。

5. 综合评分及其统计：按照评标程序、评分标准以及分值分配的规定，评标委员会成员分别就各个投标人的技术、商务状况，其对招标文件要求的响应情况进行评议和比较，评出各投标人的得分，得分与投标报价分相加得出综合得分。综合得分最高的投标人为第一中标候选投标人，综合得分次高的投标人为第二中标候选投标人，以此类推。综合得分相同的，按投标报价由低到高顺序排列。综合得分和投标报价均相同的，按技术指标由优至劣顺序排列。

附表 1

资格审查表

项目名称：信息管理系统等级保护整改

项目编号： HZ2018-370

序号	审查项目	评议内容（无效投标认定条件）	投标人 1	投标人 2	投标人 3
1	投标人的资格	是否符合投标人资格要求			
2	保证金	是否提交保证金的			
3	投标有效期	是否满足招标文件要求			
4	投标报价	是否超过最高限价或预算金额			
结　　论					

1、表中只需填写“√/通过”或“×/不通过”。

2、在结论中按“一项否决”的原则，只有全部是√/通过的，填写“合格”；只要其中有一项是×/不通过的，填写“不合格”。

3、结论是合格的，才能进入下一轮；不合格的被淘汰。

采购人代表：　　海南海政招标有限公司代表：

海南海政招标有限公司

年　月　日

附表 2

符合性审查表

项目名称：信息管理系统等级保护整改

项目编号： HZ2018-370

序号	审查项目	评议内容（无效投标认定条件）	投标人 1	投标人 2	投标人 3
1	投标文件符合性	是否满足招标文件的实质性要求，带★号关键性指标（如有）是否全部满足招标文件要求			
2	投标文件的有效性、完整性	是否符合招标文件的式样和签署要求			
3	报价项目完整性	是否对本项目内所有的内容进行投标，漏报其投标将被拒绝			
4	投标报价	投标价是否固定价且投标价是唯一的			
5	工期或交货期	是否满足招标文件要求			
6	其它	无其它无效投标认定条件			
7	结　　论				

1、表中只需填写“√/通过”或“×/不通过”。

2、在结论中按“一项否决”的原则，只有全部是√/通过的，填写“合格”；只要其中有一项是×/不通过的，填写“不合格”。

3、结论是合格的，才能进入下一轮；不合格的被淘汰。

评　委：

海南海政招标有限公司

年　　月　　日

附表 3

技术、商务评分表

项目名称：信息管理系统等级保护整改

项目编号：HZ2018-370

序号	评审内容	评分细则	满分	投标人
1	技术指标参数响应情况	技术指标参数全部满足或优于得 35 分，“▲”号指标项一项不满足扣 2 分，其它指标项一条不满足扣 1 分，扣完为止（以供应商提供加盖所投产品原厂商公司的技术参数证明函或产品彩页为准）	35	
2	厂商支持情况	提供主要设备（防毒墙、入侵检测系统、安全综合管理系统、账号集中管理与审计系统、移动办公接入网关）的原厂授权书及原厂售后服务承诺函（指同时具有原厂针对本项目授权书及原厂售后服务承诺函），评分等次按照：全部有得 2 分；缺 1 个扣 1 分；扣完为止。	2	
3	项目管理和工期计划的合理性	对比各投标人人员安排、质量保障等措施的规范性、合理性，优：2 分；良：1 分；差：0 分	2	
4	人员安排、质量保障等措施的规范性、合理性	对比各投标人售后服务响应情况，优：2 分；良：1 分；差：0 分	2	
5	售后服务响应情况	对比各投标人售后服务响应情况，优：2 分；良：1 分；差：0 分	2	
6	调试及验收方案	对比各投标人调试及验收方案，优：2 分；良：1 分；差：0 分	2	
7	本项目项目经理的资质，提供证书复印件	项目经理同时具有： 1.工信部颁发的高级项目经理资质； 2.信息系统项目管理师证书； 3.IT 服务项目经理证书； 4.ITIL 认证证书； 5.CISP 证书； 6.网络工程师证书； 每项 0.5 分，最高得 3 分 （提供资质证书复印件和在本公司任职的外部证明材料（加盖政府有关部门印章的打印日期在本项目投标截止日之前六个月以内的《投保单》或《社会保险参保人员证明》））	3	
8	投标人资质	1.投标人资质（信息安全等级保护安全建设服务机构能力评估合格证书。	8	

		2.中国信息安全认证中心（ISCCC）颁发的信息安全应急响应服务资质认证。 3.中国信息安全认证中心（ISCCC）颁发的信息安全风险评估服务资质认证。 4.ITSS 信息技术服务运行维护标准符合性证书。 5.中国信息安全认证中心（ISCCC）颁发的信息系统安全集成服务资质认证。 6.中国信息安全测评中心颁发的信息安全服务资质证书。 7.通信网络安全服务能力评定证书（风险评估类）。 8.计算机信息系统安全服务备案证书） 每个 1 分，最高不超过 8 分。		
9	投标人荣誉、信用	（1）连续 3 年或以上获得工商部门颁发的“守合同重信用企业证书”； （2）连续 3 年或以上获得银行颁发的 AAA 级或以上级别认证证书； （3）连续 3 年或以上获得第三方信用评价机构颁发的 AAA 级信用等级认证证书； （4）连续 3 年或以上获得纳税信用 A 级证书； （5）连续 3 年或以上获得省级或以上诚信示范企业证书。 具有全部证书得 3 分，一项不满足扣 1 分，最低 0 分。	3	
10	本项目主要技术及管理人员资质情况	主要技术及管理人员： （1）具有 IT 服务项目经理证书； （2）具有信息网络安全专业人员（信息安全等保类）认证证书； （3）具有信息安全等级保护安全建设专业技术人员证书； （4）具有注册信息安全专业人员 CISP 证书； （5）具有信息网络安全专业人员认证 INSPC 证书； （6）具有信息安全保障人员（风险管理类）认证证书。 满足以上每个条件得 1 分；最高得 6 分。 （提供资质证书复印件和在本公司任职的外部证明材料（加盖政府有关部门印章的打印日期在本项目投标截止日之前六个月以内的《投保单》或《社会保险参保人员证明》）	6	
11	投标人所获国际认证情况	1.ISO 20000 IT 服务管理体系认证； 2.ISO 27001 信息安全管理体系认证； 3.ISO 14001 环境管理体系认证； 4.ISO 9001 质量管理体系认证； 5.OHSAS 18001 职业健康安全管理体系认证； 具有每个证书得 1 分，最高得 5 分。	5	
12	投标人经营状况	考查各投标人近三年经营情况，均盈利：1 分；其他情况或未提供审计报告复印件的为 0 分	1	
13	投标人 2014 以来具有等级保护评估服务	具有等级保护评估服务项目经验合同，每个 1 分，最高得 4 分。（以合同复印件为准。）	4	

	类项目经验			
14	价格分	满足招标文件要求且价格最低的投标价为基准价，价格分计算公式：价格分=(基准价／投标报价)×价格权值×100%	25	
15	合计		100	

评委：