海南政辉招投标代理有限公司
HAINAN ZHENGHUI TENDER&BID AGCY CO.LTD

竞争性谈判文件

采 购 人：海口市信息中心

项目名称：海口市党政办公网安全保障设备采购

项目编号：HNZH-2018-182

代理机构：海南政辉招投标代理有限公司

2018 年 5 月

目　　录

第一章 谈 判 邀 请 函

受海口市信息中心（“采购人”）的委托，海南政辉招投标代理有限公司（“招标人”或“招标代理机构”）就海口市党政办公网安全保障设备采购（项目编号：HNZH-2018-182）组织竞争性谈判，欢迎合格的国内报价人提交密封报价。有关事项如下：

一、报价项目

1、项目名称：海口市党政办公网安全保障设备采购

2、项目编号：HNZH-2018-182

3、采购内容：见“用户需求书 ”

二、报价人资格要求：（报价人必须具备以下条件并提供相关资格证明材料）

1、在中华人民共和国境内注册，具有独立承担民事责任的能力，注册地非海南省区域的公司需在海南省设立分公司，提供营业执照副本、组织机构代码证副本、税务登记证副本有效证件或者三证合一证；

2、有依法缴纳税收的良好记录（需提供 2018 年 1 月 1 日至今任意一个月的税收记录凭证并加盖公章）；

3、有依法社会保障资金的良好记录（需提供 2018 年 1 月 1 日至今任意一个月的社保记录凭证并加盖公章）；

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（声明函）；

5、本项目不接受联合体参加。

三、谈判文件的获取

1、 时间:2018 年 5 月 21 日至 2018 年 5 月 23 日工作时间(早上 08:30~12:00；下午 14:30~17:30）；

2、 地点：海口市美兰区五指山路 16-3 号康业花园西湖苑 G 栋 2A；

3、方式：现场报名。报名时提交的材料（**现场核查原件，收加盖公章复印件**）：介绍信、营业执照副本、组织代码证副本、税务登记证副本或三证合一的社会信用代码的营业执照、2018 年 1 月 1 日至今任意一个月缴纳社会保障资金及纳税的凭证、法定代表人授权委托书、法定代表人身份证和授权人身份证、报价人资格要求中的证明材料。

4、售 价：人民币 300 元/套（售后不退）

户 名：海南政辉招投标代理有限公司

开户行：中国工商银行股份有限公司海口新华支行

账　户：2201023809200980178

四、报价截止时间、谈判时间及地点

1、递交报价文件时间：2018 年 5 月 24 日 09 时 30 分；

2、报价截止时间：2018 年 5 月 24 日 09 时 30 分；

3、缴纳投标保证金截止时间：2018 年 5 月 24 日 09 时 30 分；

4、谈判时间：2018 年 5 月 24 日 09 时 30 分；

5、谈判地点：海口市美兰区五指山路 16-3 号康业花园西湖苑 G 栋 2A；

6、采购信息发布媒介：中国海南省政府采购网、中国采购与招标网。

五、招标代理机构联系方式

名称：海南政辉招投标代理有限公司

地址：海口市美兰区五指山路 16-3 号康业花园西湖苑 G 栋 2A

电话：0898-66557609

联系人:符工

海南政辉招投标代理有限公司

2018 年 5 月 18 日

第二章 报价人须知

一、 总则

1. 名词解释

1.1 采购人：海口市信息中心

1.2 招标人：海南政辉招投标代理有限公司

1.3 报价人：已从招标人购买谈判文件并向招标人提交报价文件的供应商。

2. 适用范围

2.1 本谈判文件仅适用于招标人组织的本次报价活动。

3. 合格的报价人

3.1 凡有能力按照本谈判文件规定的要求交付货物和服务的投标单位均为合格的报价人。

3.2 报价人参加本次政府采购活动应当符合《中华人民共和国政府采购法》第二十二条的规定，并具备本谈判文件第一章“报价人资格要求”规定的条件。

3.3 报价人应遵守中华人民共和国的有关法律、法规。

4. 报价费用

4.1 无论招标报价过程中的做法和结果如何，报价人均自行承担所有与参加报价有关的全部费用。

5. 谈判文件的约束力

5.1 报价人一旦参加本项目报价，即被认为接受了本谈判文件中的所有条件和规定。

二、 谈判文件

6. 谈判文件的组成

6.1 谈判文件由六部分组成，包括：

第一章 谈判邀请书

第二章 报价人须知

第三章 用户需求书

第四章 合同条款

第五章 报价文件内容和格式

第六章 评审方法

请仔细检查谈判文件是否齐全，如有缺漏，请立即与招标人联系解决。

6.2 报价人被视为充分熟悉本招标项目所在地的与履行合同有关的各种情况，包括自然环境、气候条件、劳动力及公用设施等，本谈判文件不再对上述情况进行描述。

6.3 报价人必须详阅谈判文件的所有条款、文件及表格格式。报价人若未按谈判文件的要求和规范编制、提交报价文件，将有可能导致报价文件被拒绝接受，所造成的负面后果由报价人负责。

7. 谈判文件的澄清

7.1 报价人在收到谈判文件后，若有疑问需要澄清，应于报价截至时间三天前以书面形式（包括书面文字、传真等）向招标人提出，招标人将以书面形式进行答复，同时招标人有权将答复内容（包括所提问题，但不包括问题来源）分发给所有购买了同一谈判文件的报价人。

8. 谈判文件的更正或补充

8.1 在报价截止时间前，招标人可以书面通知的方式修改谈判文件。修改通知作为谈判文件的组成部分，对报价人起同等约束作用。

8.2 当谈判文件与更正公告的内容相互矛盾时，以招标人最后发出的更正公告为准。

8.3 为使报价人有足够的时间按谈判文件的更正要求修正报价文件，招标人有权决定推迟投标截止日期和开标时间，并将此变更书面通知所有购买了同一谈判文件的报价人。

三、 报价文件

9. 报价文件的组成

9.1 报价文件应按“第五章 报价文件内容和格式”要求编制。

10. 报价

10.1 报价人应按开标一览表的要求报价，并且该报价在所有的报价文件中必须是统一的报价。

10.2 报价均须以人民币为计算单位。

11. 报价保证金

11.1 报价保证金是参加本项目投标的必要条件，**投标保证金为：15000 元（人民币壹万伍仟元整）。**

11.2 投标保证金应在2018 年 5 月 24 日 09 时 30 分前划入或存入招标代理机构指定账户并注明汇款单位。

缴纳投标保证金银行账户：

户　名：海南政辉招投标代理有限公司

开户行：中国工商银行股份有限公司海口新华支行

账　户：2201023809200980178

11.3 若报价人不按规定提交报价保证金，其报价文件将被拒绝接受。报价文件必须附上缴纳报价保证金的证明单据，并加盖公司公章及公司财务章并在用途中备注项目编号（如银行回单或收据）。

11.4 报价保证金的退还

11.4.1 中标人的投标保证金按相关规定可直接转为招标服务费（按相关规定收取，多还少补，多出部分在与采购人签订供货合同后 5 个工作日内无息退还）。

11.4.2 落标的报价人的报价保证金将在招标人发出成交通知书 5 个工作日内无息退还。

11.5 发生下列情况之一，报价保证金将不予退还：

（1）报价人在报价有效期内撤回报价书的；

（2）成交人不按本章规定签订合同；

（3）报价人提供虚假材料谋取中标、成交的；

（4）与采购人、其它报价人或者招标人恶意串通的；

（5）向采购人、招标人、评标委员会成员行贿或者提供其他不正当利益的；

12. 报价有效期

12.1 报价有效期为从开标截止之日起计算的六十天，有效期短于此规定的报价文件将被视为无效。

12.2 在特殊情况下，招标人可于报价有效期满之前，征得报价人同意延长报价有效期，要求与答复均应以书面形式进行。报价人可以拒绝接受这一要求而放弃报价，报价保证金将尽快无息退还。同意这一要求的报价人，无需也不允许修改其报价文件，但须相应延长报价保证金的有效期。受报价有效期制约的所有权利和义务均应延长至新的有效期。

13. 报价文件的数量、签署及形式

13.1 报价文件一式叁份，正本一份，副本贰份（报价文件封面需注明正副本，如有分包按包号分别制作投标文件）。

13.2 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。

13.3 投标文件正本中，文字材料需打印或用不褪色墨水书写。投标文件加盖骑缝章。投标文件法人或授权委托人需逐页签字加盖单位公章。

13.4 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、 报价文件的递交

14. 报价文件的密封及标记

14.1 报价人应将报价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。**报价人投多包时要针对每个包单独做投标文件（如项目分包）**。封皮上均应写明：

致：海南政辉招投标代理有限公司

项目名称：海口市党政办公网安全保障设备采购

项目编号：HNZH-2018-182

包号：（如有）

注明：“请勿在开标时间之前启封”

报价单位名称、联系人姓名和电话

14.2 报价文件未按上述规定书写标记和密封者，招标人不对报价文件被错放或先期启封负责。

15. 报价截止时间

15.1 报价人须在报价截止时间前将报价文件送达招标人规定的报价地点。

15.2 若招标人推迟了报价截止时间，应以公告的形式通知所有报价人。在这种情况下，谈判方和报价人的权利和义务均应以新的截止时间为准。

15.3 在报价截止时间后递交的报价文件，招标人将拒绝接受。

五、 谈判及评标

16. 谈判

16.1 招标人按谈判文件第一章规定的时间和地点进行谈判。采购人代表、招标人有关工作人员参加。政府采购主管部门、监督部门、国家公证机关公证员由其视情况决定是否派代表到现场进行监督。

16.2 报价人应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原件签名报到，以证明其出席。未派授权代表或不能证明其授权代表身份的，招标人对报价文件的处理不承担责任。

16.3 谈判时，招标人或报价人代表将查验报价文件密封情况，确认无误后拆封唱标，公布每份报价文件中“报价一览表”的内容，以及招标人认为合适的其他内容，招标人将作开标记录。

16.4 若报价文件未密封，招标人将拒绝接受该报价人的报价文件。

16.5 若未按 13.3 要求提供报价文件的，做无效标处理。

17. 谈判小组

17.1 受采购人的委托，招标人从海南省综合评标专家库中随机抽取相关专家二名和用户代表一名组成谈判小组，其中，技术、经济等方面的专家不少于成员总数的 2/3。该谈判小组独立工作，负责评审所有报价文件并确定成交侯选人。

18. 谈判和评标

18.1 见“第六章 评审方法”。

六、 授标及签约

19. 定标原则

19.1 谈判小组将严格按照谈判文件的要求和条件进行评标,根据评标办法推荐出一至三人为成交候选人，并标明排列顺序。采购人将确定排名第一的成交候选人为成交人并向其授予合同。排名第一的成交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成交候选人。排名第二的成交候选人因前款规定的同样原因不能签订合同的，采购人将把合同授予排名第三的成交候选人。

19.2 在中国海南省政府采购网、中国采购与招标网上公示成交结果。

20. 成交通知

20.1 定标后,招标人应将定标结果通知所有的报价人，并向成交人发出成交通知书。

20.2 成交人收到成交通知书后，须立即以书面形式回复招标人，确认成交通知书已收到，并同意接受。

20.3 成交通知书将是合同的一个组成部分。

21. 签订合同

21.1 成交人应按成交通知书规定的时间、地点与采购人签订成交合同,否则报价保证金将不予退还，给采购人和招标人造成损失的，报价人还应承担赔偿责任。

21.2 谈判文件、成交人的报价文件及评标过程中有关澄清文件均应作为合同附件。

22. 采购代理服务费

22.1 本次采购活动采购代理服务费按相关规定收取，由中标单位向招标代理机构支付。

23. 其它

23.1 本项目不召开答疑会。

第三章 用户需求书

一、项目基本情况

项目名称：海口市党政办公网安全保障设备采购

采购预算：1757440.00元

交付期：合同签订后30天内

付款方式：按合同约定执行

交货地点：采购人指定

二、采购清单及技术参数要求

海口市党政办公网安全保障设备采购清单及参数要求				
序号	设备名称	参数要求	单位	数量
1	机架式服务器	机箱：4U 标准机架式；配套原厂上架滑轨； 处理器：配置 4 颗 Intel Skylake 5118 十二核金牌处理器（2.3GHz 主频, 17M L3 Cache，10.4UPI）； 内存：配置 64GB DDR4 2666MHz ECC 内存； 内存扩展性：内存插槽≥32 个，最大可支持≥4TB 内存扩展； 硬盘：配置 3 块 600GB 10Krpm 12Gb SAS 硬盘； 存储扩展性： 最大可扩展≥8 块 2.5 寸 SSD/SAS/SATA 硬盘； RAID 控制器：配置 2GB 缓存八通道高性能 12Gb SAS RAID 卡，支持 RAID0/1/5/6/10/50/60，支持可选后备超级电容保护模块； 扩展插槽：标配≥4 个 PCI-E3.0 扩展插槽；最大可扩展≥7 个 PCI-E3.0 扩展插槽，支持全高全长 GPU 卡扩展； 网络控制器：配置≥4 个千兆以太网端口，网卡支持虚拟化技术和网络负载均衡等高级特征；支持可选千兆万兆电口或光口网卡； 外存储接口卡：配置 1 块 8Gb 双端口光纤 HBA 卡； 光驱：内置 DVD-RW 光驱； 管理功能：支持 IPMI2.0 和 KVM Over IP 远程管理功能；支持远程监控图形界面，可实现与操作系统无关的远程对服务器的完全控制，允许从远程通过网络访问、安装、配置和控制服务器；硬件级别的访问及控制，提供完全的兼容性；高安全性，所有传输的数据均经过数据加密； 管理记录模块：内置 Micro SD 卡插槽，可实时记录备份主机系统事件信息；支持离线光诊断功能，可在断电环境下诊断主板关键信息故障，更加有助于问题的分析及定位； 电源模块：配置 3 个高效铂金电源，2+1 冗余模式，单个电源功率≤1200W，最大可支持 4 个高效铂金电源，支持 3+1 或 2+2 冗余模式，兼容 220V AC 及 48V/240V/336V DC； 配套软件:配套 1 套服务器原厂商的服务器智能导航软件(含正版 CD 光盘介质)； ▲数据安全服务：由国家信息中心信息安全研究与服务中心提供 3 年硬盘数据恢复服务，提供国家信息中心信息安全研究与服务中心针对本项目的授权书及售后服务承诺函（原件）； ▲设备厂商提供免费现场安装调试服务，提供三年保修，三年免费上门服务，	台	2

		7X24 技术支持，提供设备厂商针对本项目的售后服务承诺函（加盖制造厂商公章原件）。		
2	核心路由器	▲国产品牌； ▲16 个 GE 电接口，2 个 GE 光接口，支持电源冗余配置，主控板冗余配置。配置不超过 230mm 插箱，设备所有线缆前出线，以保证设备可以安放在 300mm 深的机柜，或在 600mm 深机柜前后放置。 ▲业务接口板槽位数>12 个，剩余业务槽位数>4 个，实现三层吞吐转发能力≥60Mpps，主控板内存大于 2G，FLSAH 大于 2G； ▲电源、主控、所有业务接口板卡均支持热插拔； ▲主控路由转发支持冗余备份，电源模块支持冗余备份（非外置冗余电源模块方式）； ▲支持双主控板，主控板不允许有业务接口； 支持的接口类型包括：10GE/GE/FE、cPOS3、POS3、POS12、E1/CE1、V.35/V.24 和国密卡等； ▲支持 WCDMA、TD-SCDMA、FDD-LTE 和 TD-LTE； 开放业务平台：要求支持开放业务服务器平台，客户、厂家和第三方均可在此平台上安装各种应用系统或开发新的增值业务； L2 功能：支持 STP、RSTP、MSTP 协议；支持 L2 交换板、支持跨板 L2 交换、L2 交换和 L3 路由配置要求在同一配置界面实现，支持广播风暴抑制面； IPv4 单播：支持静态路由和 RIPv1/v2, OSPFv2, IS-ISv4 和 BGP-4 动态路由协议； IPv6 单播：支持静态路由和 RIPng, OSPFv3, IS-ISv6 和 BGP4+动态路由协议； IPv4/IPv6 过渡技术：实现标准 IPv4 向 IPv6 的过渡技术，6RD，NAT64，6to4、6 over 4、6in4、4in6、GRE、ISATAP 隧道、6PE 和 6VPE 等 组播：支持静态组播和 PIM-DM, PIM-SM, PIM-SSM 和 MBGP 动态组播，支持 MLDv1/v2； VPN：要求支持 GRE, IPSec 和 L2TP 隧道技术，支持 IPSec 的 NAT 穿越； ▲宽带用户接入：要求支持 PPPoE、IPoE 和 802.1X 接入认证，支持 DHCP 用户开机认证接入和 DHCP+WEB 认证接入； MPLS 及 MPLS VPN：支持 VPWS, VPLS 等 MPLS L2VPN 和 MPLS L3VPN，支持三种跨域方式，支持 L2/L3 MPLS VPN 桥接，支持的 VRF 的数量以及每个 VRF 的路由数，支持 MPLS TE； 电路仿真：支持 PWE3 电路仿真，支持 SAToP 和 CESoPSN 封装； QoS：支持流分类、标记、优先级继承和映射、流量监管（CAR）、流量整形/限速，支持 PQ, CQ, WFQ, CBWFQ 和基于物理端口的拥塞管理，支持基于 WRED 的拥塞避免，支持层次化 QoS 机制 ▲支持二、三层混合 ACL，支持 ACL 统计。支持 32k ACL 规则数，开启 32k 条 ACL，设备性能下降小于 30%； 支持端口镜像、NetFlow V5/V8/V9，要求支持 1:1 采样； 支持防火墙功能，包括包过滤检测和状态检测； ▲支持防火墙单板，提供专业的防火墙功能，包括入侵检测及防御、防病毒、应用程序识别，URL 过滤、恶意网站过滤、内容过滤及用户行为管理等功能； ▲支持 DPI 功能，支持 IM、P2P、Mail 等至少 500 种以上协议的识别，支持 URL 分类过滤，DPI 用户数不小于 5000； 支持 CPU 防护，支持防 DDOS 攻击等； NAT：支持静态 NAT、动态 NAT、PAT、VRF NAT，NAT44，NAT64 等，支持 NAT 双出口，支持 FTP/RSTP/H323/SIP/DNS 等各种 ALG，NAT 并发会话数不少于 512k，NAT 映射条目生成速率不小于 4k/s； 可靠性：支持 VRRP，VRRP Track，VRRP 在二层 VPN 中透传，支持端口捆绑，包括 E1 捆绑、POS 捆绑和 Eth 捆绑，支持 GR，FRR；	台	1

		可管理性：支持 SNMPv1/v2/v3， RMON，SYSLOG 和 MIB，支持 USB 方式升级版本，网管方式批量升级版本； ▲工信部入网证书（IPv4&IPv6）、IPv6 Ready Phase 2、FCC VOC/UL Certification/ CE DOC/ROHS、《商用密码产品生产定点单位证书》、《商用密码产品型号证书》、《商用密码产品销售许可证》、《提供原厂商授权函》（加盖原厂商章）。		
3	一体化安全网关 USG（内网）	国产品牌； 机架式 2U，冗余电源； ▲千兆电口≥6 个；扩展槽≥1；支持扩展千兆光口，万兆光口； ▲整机最大吞吐率≥25Gbps； 最大并发连接数≥550 万； 每秒新建连接数≥18 万； ▲存储空间≥60G SSD； ▲配置 AV 功能模块，含 3 年特征库升级； 支持基于硬件 Hypervisor 技术的底层虚拟化，各个虚拟防火墙之间完全隔离，可运行不同的防火墙版本，拥有完全独立的 CPU、内存、接口等资源。（要求提供功能界面截图进行证明）； 支持基于接口/安全域、地址、用户、服务、应用和时间的防火墙访问控制策略； 支持基于接口/安全域、地址、用户、服务、应用和时间的会话控制策略，包括总连接数控制、每秒总新建连接数控制、每 IP 总连接数控制、每 IP 新建连接数控制（要求提供功能界面截图进行证明）； 支持路由、透明及混合部署模式； 可基于 IP 地址、网段、用户、时间、VLAN、协议类型等条件设定入侵防御模块的检测事件及响应方式； 支持扩展 APT 检测模块，采用沙箱检测技术，对未知木马、病毒、恶意代码具有精确的检测效果，实现对未知威胁、高级持续威胁和 ODAY 攻击的有效防护；可对 exe、rtf、pdf、xls（x）、ppt（x）、doc（x）、pps（x）、swf、rar、zip 等常见的格式进行动态沙箱分析；可对 rtf、pdf、xls（x）、ppt（x）、doc（x）、pps（x）做 PE 内嵌检测，并且能指出文件偏移位置；（要求提供功能界面截图进行证明，并加盖厂家公章）； 支持对文件感染型病毒、蠕虫病毒、脚本病毒、宏病毒、木马、恶意软件等过滤，病毒库数量不少于 1000 万； 支持并开通基于 DPI 和 DFI 技术的应用特征识别及行为控制，应用识别的种类不少于 1000 种； 支持并开通基于线路和多层通道嵌套的带宽管理和流量控制功能，提供至少四层管道嵌套的流控； 支持并开通链路负载均衡，提供轮询、加权轮询、哈希等多种负载均衡算法； 支持并开通 IPSec VPN 和 L2TP VPN，投标产品实配 IPSec VPN 隧道数量不少于 2000 条； 支持通过 ICMP、TCP、DNS 和 HTTP 协议实现对链路可用性的多重健康检查； 支持源 NAT、目的 NAT、静态 NAT，支持一对一、一对多和多对多等形式的 NAT； 支持主-主和主-备模式，主备模式下支持基于设备优先级的主设备抢占功能； 支持基于心跳信号丢失、链路断开等多种方式的 HA 切换条件及逻辑； 支持 HA 设备之间的会话自动同步，包括主主模式和主备模式，确保 HA 切换时业务不发生任何中断； 支持双路 HA 物理心跳线，确保 HA 运行稳定可靠； 支持 HA 设备之间的配置自动同步，确保用户只需在一台设备进行业务配置； 支持防火墙集中管理，包括统一状态监控、配置下发、配置自动备份及回滚、版本统一升级、特征库统一升级等功能； 集中对所有防火墙安全策略进行命中频率分析，辅助用户快速完成策略次序的	台	2

		调整，从而达到优化防火墙处理性能的目的； 支持基于 WEB 和命令行的设备管理模式，WEB 界面和命令行模式下均可实现对设备所有功能的管理配置； 支持 SYSLOG 和 SNMP v3，SYSLOG 日志支持同时发给多个日志服务器； 产品具有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》（要求提供复印件并加盖厂家公章）； ▲产品具有中国国家信息安全测评中心颁发的《信息安全服务资质证书》，为安全工程类三级（要求提供复印件并加盖厂家公章）； ▲设备厂商具有网络安全应急服务支撑单位证书（国家级）（要求提供复印件并加盖厂家公章）； ▲设备厂家具备《中国国家信息安全漏洞库（CNNVD）技术支撑单位一级》资质（要求提供复印件并加盖厂家公章）； ▲提供 3 年设备原厂保修服务； ▲提供原厂商授权函及售后服务承诺函（加盖原厂商章）。		
4	入侵防御安全网关	国产品牌； 机架式 2U，冗余电源； ▲千兆电口≥6 个，具备 BYPASS 功能接口≥4 个，扩展槽≥1 个，USB≥接口≥2 个，RJ45 串口≥1 个； ▲最大吞吐量≥15G； 最大并发连接数≥400 万； 每秒新建连接数≥8 万； ▲含 3 年 IPS 特征库升级； 系统应提供旁路部署及在线、旁路混合部署等部署方式、系统应支持桥组部署方式，并支持 STP 协议； 系统应支持双机热备和双机主备功能，并且主备热备时需支持连接状态和配置同步； 系统入侵防御事件库事件数量不少于 4000 条； 系统应支持无线攻击检测和防护功能扩展，可手工或自动识别和区分内部 AP 和外部 AP，也可以手工或自动识别合法终端，并基于此设定无线准入策略，通过射频信号阻止非法 AP、终端的接入。支持无线扫描、欺骗、DoS、破解等常见无线网络攻击行为的检测、告警、阻断功能，同时支持多种类型流氓 AP 的检测与阻断； 支持可基于 IP 地址、网段、时间、VLAN、协议类型等条件设定 IPS 检测及响应方式； 系统应支持多种事件响应方式，满足客户的安全要求，需包括：重置、临时阻断、丢弃报文、丢弃会话等动作； 系统应支持多种防 web 扫描能力，包括爬虫、CGI 和漏洞扫描等，并支持设置至少 5 个不同级别的扫描容忍度/扫描敏感度； 支持虚拟 IPS 功能，不同的用户可以方便定制满足自身要求的检测模版，至少支持 400 个用户； 支持终端和服务器环境感知能力，通过主动扫描和扫描结果导入获得终端环境情况 系统应提供 SQL 注入攻击、XSS 攻击的检测和防御功能，对 Web 服务系统提供保护 ； 系统应支持自定义事件升级内容。升级界面中至少包含高中低三种级别事件的升级启用选项； 系统应支持对文件感染型病毒、蠕虫病毒、脚本病毒、宏病毒、木马、恶意软件等过滤，病毒库数量不少于 40 万； 系统应支持邮件内容过滤功能，有效防止恶意邮件及信息外泄。可根据邮件 SMTP 命令、发件人、主题、附件、IP 及邮件大小进行过滤；	台	1

		系统应提供定期自定发送报表功能，通过邮件将 html、doc、xls、CSV 和 pdf 格式报表发送给管理员； 系统应支持报表个性化设置，通过自定义报表生成单位、报表生成人、单位 logo 和安全摘要信息等信息，快速生成符合单位特点的报告，减少工作量； 系统应提供 netflow 日志发送功能，满足第三方管理平台对 netflow 日志的审计需求； 系统应支持本地日志及 SYSLOG 日志发送，支持向至少 3 个 syslog 服务器发送日志； 系统应支持声音报警，通过设置事件级别、入侵事件级别和病毒事件进行声音报警； 具备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》；（要求提供复印件并加盖厂家公章）； ▲产品具有中国国家信息安全测评中心颁发的《信息安全服务资质证书》，为安全工程类三级（要求提供复印件并加盖厂家公章）； ▲设备厂商具有网络安全应急服务支撑单位证书（国家级）（要求提供复印件并加盖厂家公章）； ▲设备厂家具备《中国国家信息安全漏洞库（CNNVD）技术支撑单位一级》资质（要求提供复印件并加盖厂家公章）； ▲提供 3 年设备原厂保修服务； ▲提供原厂商授权函及售后服务承诺函（加盖原厂商章）。		
5	漏洞扫描系统	国产品牌； ▲千兆电口≥6 个，RJ45 串口≥1 个，扩展槽≥1 个； ▲硬盘存储容量≥1T，可扫描 IP 数量不限制； ▲含 3 年特征库升级； 漏洞扫描方法应不少于 19000 种，集成系统漏洞扫描、Web 应用扫描、基线核查于一体，（要求提供功能界面截图进行证明）； 漏洞库与 CVE、CNCVE、CNNVD 和 BUGTRAQ 等国际、国内标准兼容； 支持扫描任务优先级设置； 支持对意外中断（网络中断、设备断电）的扫描任务恢复后继续进行扫描； 网站开源架构类扫描：支持 phpmyadmin、WordPress 等的扫描； 支持以系统类型、漏洞类型、危险级别、CVE 等不同视图显示漏洞，支持策略的导入、导出、修改以及合并； 支持对部门和资产的添加、删除、编辑等操作，以及对资产的属性自定义功能； 支持云平台扫描，漏洞覆盖 OpenStack 、KVM、Vmware、Xen 等主流的云计算平台（要求提供功能界面截图进行证明）； 支持给每个任务报表添加自定义安全结论； HTML 离线报表能够通过点击主机 ip 链接，自动跳转至该主机的详细报告； 支持扫描任务预计所需剩余时间显示； 支持每个资产历史扫描的风险趋势图显示，缺省显示最后 24 次扫描结果的趋势显示； 支持对各种网络主机、操作系统、网络设备（如交换机、路由器、防火墙等）、常用软件以及应用系统的识别和漏洞扫描； 应保证至少每周一次的漏洞库更新，并保证紧急的、重要的漏洞做到随时更新。 支持 python 的多个模块的漏洞扫描，如 audioop 模块 、audioop 模块 、rgbimg 模块的漏洞； 支持以 txt、csv、dat 等格式进行资产列表的导入； 报告中的漏洞应具备统一的 CVSS 国际标准评分，以准确衡量漏洞的危险级别，为漏洞修补工作的优先级提供指导； 产品具有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》，（要求提供复印件并加盖厂家公章）	台	1

		▲产品具有中国国家信息安全测评中心颁发的《信息安全服务资质证书》，为安全工程类三级（要求提供复印件并加盖厂家公章）； ▲设备厂家具备《中国国家信息安全漏洞库（CNNVD）技术支撑单位一级》资质（要求提供复印件并加盖厂家公章）； ▲设备厂家具备《国家级网络安全应急服务支撑单位》资质（要求提供复印件并加盖厂家公章）； ▲提供 3 年设备原厂保修服务； ▲提供原厂商授权函及售后服务承诺函（加盖原厂商章）。		
6	一体化安全网关（外网）	配置≥10 个 10/100/1000MBase-T 端口、≥6 个千兆 SFP 光端口、≥2 个万兆光端口； 防火墙吞吐率≥25Gbps、最大并发连接数≥400W； 配置多操作系统引导，多个操作系统均为全功能操作系统; 配置路由、交换、混合、虚拟线工作模式（要求提供截图进行证明）； 支持静态路由、ISP 路由及动态路由协议，支持 802.1q、QinQ 模式； 支持基于源/目的地址、源/目的端口、用户、应用的策略路由，保证关键业务流量通过优质链路转发； 支持手动添加绑定，基于 IP、接口的动态探测绑定，支持三层 IP/MAC 绑定，IP/MAC 绑定表可导入导出； 支持一对一 SNAT、多对一 SNAT、一对一 DNAT、双向 NAT、NoNAT 等多种转换方式； 支持智能 DNS 及 DNS Docting 功能，能够将来自内部网络的域名解析请求定向到真实内网资源，提高访问效率，同时支持通过配置多条 DNS Doctoring，实现内网资源服务器的负载均衡； 支持 IPv6 安全控制策略设置，能针对 IPv6 的目的/源地址、目的/源服务端口、区域、服务、时间、扩展头属性等条件进行安全访问规则的设置； 支持基于 IPv6 的应用层检测（FTP\TFTP）、病毒过滤、IPS 检测； 内置强大应用识别引擎，综合运用端口识别、行为识别、特征识别、关联识别等技术手段，准确识别传统应用如 P2P、web 应用、移动应用、云应用、加密应用等； 支持对单条访问控制策略进行最大并发连接数限制；同时支持对连接数限制策略匹配信息进行分类统计，方便管理员根据统计分析结果进行相应的防护控制； 为保护内部网络资源以及合理分配设备系统资源，需支持对指定的源/目的 IP 地址、MAC 地址、应用制定相应的连接限制策略，策略包含三种限制类型：单个 IP 每秒新建连接限制、单个 IP 连接数限制及连接总数限制； 内置高度集成的一体化智能过滤引擎技术，支持实现在同一条访问控制策略中配置传统的五元组信息、用户、域名、应用、服务、时间、安全引擎（入侵防御、URL 过滤、病毒过滤、内容过滤、文件过滤、审计）的识别与控制； 访问控制策略执行动作支持允许、禁止及认证，对符合条件的流量进行 Web 认证，在策略中可设置用户 Web 认证的门户地址； 提供智能策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查； 支持黑名单功能，可设置多个对象条件，如：五元组信息、地址范围、应用、用户等，实现对特定报文进行快速过滤； 支持扩展攻击检测及防御功能模块，采用协议分析、模式识别、统计阀值和流量异常监视等综合技术手段来判断入侵行为；支持 web 攻击识别和防护，如跨站脚本攻击、SQL 注入攻击； 内置流量检测清洗引擎，支持基于 IP、ICMP、TCP、UDP、DNS、HTTP、NTP 等众多协议类型的防护策略；提供丰富的策略模板，支持策略模板自定义； 支持基于 UDP 协议的检测清洗，包括对源、目的限速，对 UDP 最大及最小报文限制；同时支持 UDP 关联认证，要求所有去往服务器的 UDP 报文，必须首先与该服务器的 TCP 端口建立 TCP 连接，对源地址进行合法性认证；	台	4

		支持基于 DNS 协议的检测清洗，包括但不限于：DNS QUERY FLOOD、DNS REPLY FLOOD、DNS 投毒攻击、DNS 格式检查、DNS NX 异常比率检测等；支持 DNS QUERY 源认证、DNS REPLY 源认证，认证方式可选基本源认证或者 cname 认证； 支持根据 DOS/DDOS 攻击行为自动添加动态黑/白名单功能，可自定义动态黑/白名单超时时间；（要求提供功能界面截图进行证明）； 支持扩展病毒检测功能模块，支持 HTTP/SMTP/POP3/FTP/IM 等协议的病毒防御，对每种协议数据流的检测方向可选双向、上传、下载； 支持多个配置文件并存； 支持分别针对网络层、传输层和应用层提供诊断系统网络连通性的工具，包括 PING、 TRACEROUTE、 TCP、 HTTP 和 DNS； 支持在 WEB 界面进入 CLI 模式，执行系统配置、网络诊断、过滤抓包等命令，提高管理员运维效率； 提供完善的审计数据查询功能，方便管理员对用户的上网行为进行审查和分析。支持对用户上网行为进行完整的审计数据查询，包括访问网站、邮件收发、论坛微博、 FTP、 网盘、 TELNET 等；同时支持对用户上网流量时长进行完整的审计数据查询，包括服务端 IP、用户名、协议、上行流量、下行流量、总流量、时间等； 支持日志本地存储，可对不同类型日志设置存储空间； 支持将日志外发至 SYSLOG 服务器，可将多条日志合并成一条日志传送到日志服务器中，可选择对日志传输是否加密； 所投产品具有公安部颁发的产品销售许可证； 所投产品厂家具备国家级网络安全应急服务支撑单位证书（国家级），提供复印件； 提供三年免费原厂质保，提供原厂商三年售后服务承诺函。		
7	一体化安全网关（高配置-外网）	配置≥6 个 10/100/1000MBase-T 端口、≥4 个千兆 SFP 光端口、≥2 个万兆光端口、≥1 个业务扩展插槽； 防火墙吞吐率≥40Gbps、最大并发连接数≥600W ； 配置多操作系统引导，多个操作系统均为全功能操作系统； 配置路由、交换、混合、虚拟线工作模式（要求提供截图进行证明）； 支持静态路由、ISP 路由及动态路由协议，支持 802.1q、QinQ 模式； 支持基于源/目的地址、源/目的端口、用户、应用的策略路由，保证关键业务流量通过优质链路转发； 支持手动添加绑定，基于 IP、接口的动态探测绑定，支持三层 IP/MAC 绑定，IP/MAC 绑定表可导入导出； 支持一对一 SNAT、多对一 SNAT、一对一 DNAT、双向 NAT、NoNAT 等多种转换方式； 支持智能 DNS 及 DNS Docting 功能，能够将来自内部网络的域名解析请求定向到真实内网资源，提高访问效率，同时支持通过配置多条 DNS Doctoring，实现内网资源服务器的负载均衡； 支持 IPv6 安全控制策略设置，能针对 IPv6 的目的/源地址、目的/源服务端口、区域、服务、时间、扩展头属性等条件进行安全访问规则的设置； 支持基于 IPv6 的应用层检测（FTP\TFTP）、病毒过滤、IPS 检测； 内置强大应用识别引擎，综合运用端口识别、行为识别、特征识别、关联识别等技术手段，准确识别传统应用如 P2P、web 应用、移动应用、云应用、加密应用等； 支持对单条访问控制策略进行最大并发连接数限制；同时支持对连接数限制策略匹配信息进行分类统计，方便管理员根据统计分析结果进行相应的防护控制；为保护内部网络资源以及合理分配设备系统资源，需支持对指定的源/目的 IP 地址、MAC 地址、应用制定相应的连接限制策略，策略包含三种限制类型：单个 IP 每秒新建连接限制、单个 IP 连接数限制及连接总数限制；	台	2

		内置高度集成的一体化智能过滤引擎技术，支持实现在同一条访问控制策略中配置传统的五元组信息、用户、域名、应用、服务、时间、安全引擎（入侵防御、URL 过滤、病毒过滤、内容过滤、文件过滤、审计）的识别与控制； 访问控制策略执行动作支持允许、禁止及认证，对符合条件的流量进行 Web 认证，在策略中可设置用户 Web 认证的门户地址； 提供智能策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查； 支持黑名单功能，可设置多个对象条件，如：五元组信息、地址范围、应用、用户等，实现对特定报文进行快速过滤； 支持扩展攻击检测及防御功能模块，采用协议分析、模式识别、统计阀值和流量异常监视等综合技术手段来判断入侵行为；支持 web 攻击识别和防护，如跨站脚本攻击、SQL 注入攻击； 内置流量检测清洗引擎，支持基于 IP、ICMP、TCP、UDP、DNS、HTTP、NTP 等众多协议类型的防护策略；提供丰富的策略模板，支持策略模板自定义； 支持基于 UDP 协议的检测清洗，包括对源、目的限速，对 UDP 最大及最小报文限制；同时支持 UDP 关联认证，要求所有去往服务器的 UDP 报文，必须首先与该服务器的 TCP 端口建立 TCP 连接，对源地址进行合法性认证； 支持基于 DNS 协议的检测清洗，包括但不限于：DNS QUERY FLOOD、DNS REPLY FLOOD、DNS 投毒攻击、DNS 格式检查、DNS NX 异常比率检测等；支持 DNS QUERY 源认证、DNS REPLY 源认证，认证方式可选基本源认证或者 cname 认证； 支持根据 DOS/DDOS 攻击行为自动添加动态黑/白名单功能，可自定义动态黑/白名单超时时间；（要求提供功能界面截图进行证明）； 支持扩展病毒检测功能模块，支持 HTTP/SMTP/POP3/FTP/IM 等协议的病毒防御，对每种协议数据流的检测方向可选双向、上传、下载 ； 支持多个配置文件并存； 支持分别针对网络层、传输层和应用层提供诊断系统网络连通性的工具，包括 PING、 TRACEROUTE、 TCP、 HTTP 和 DNS； 支持在 WEB 界面进入 CLI 模式，执行系统配置、网络诊断、过滤抓包等命令，提高管理员运维效率； 提供完善的审计数据查询功能，方便管理员对用户的上网行为进行审查和分析。支持对用户上网行为进行完整的审计数据查询，包括访问网站、邮件收发、论坛微博、 FTP、 网盘、 TELNET 等；同时支持对用户上网流量时长进行完整的审计数据查询，包括服务端 IP、用户名、协议、上行流量、下行流量、总流量、时间等； 支持日志本地存储，可对不同类型日志设置存储空间； 支持将日志外发至 SYSLOG 服务器，可将多条日志合并成一条日志传送到日志服务器中，可选择对日志传输是否加密； 所投产品具有公安部颁发的产品销售许可证； 所投产品厂家具备国家级网络安全应急服务支撑单位证书（国家级），提供复印件； 提供三年免费原厂质保，提供原厂商三年售后服务承诺函。		
8	万兆入侵检测系统	配置≥6 个 10/100/1000BASE-T 接口、≥2 个万兆光接口、≥1 个可插拔的扩展槽； 整机吞吐率≥14Gbps、最大并发连接数≥320W、含三年攻击规则库升级服务； 要求内置 SSD 固态硬盘存储日志； 配置多操作系统引导； 配置独立的攻击检测规则库，能够针对 4000 种以上攻击行为进行检测，涵盖网络攻击、异常事件、网络资源滥用流量等； 配置独立的应用识别规则库，能够根据数据内容而非端口智能识别包括 P2P、即时通讯、电子商务、股票交易、网络游戏、网络电视、移动应用等在内的 23 大类超过 1000 种应用；	台	1

		支持扩展独立的病毒检测特征库，内置 400 万以上病毒检测规则； 融合模式匹配、协议分析、异常检测、会话关联分析，逃逸等多种技术，准确识别入侵攻击行为，为用户提供 2~7 层深度入侵检测； 支持 VLAN、MPLS、PPPoE 网络，能够在该网络环境中检测出攻击事件； 支持 IPv6、IPv6overIPv4、IPv6 和 IPv4 混合网络，能够在该网络环境中检测出攻击事件； 可检测的攻击类型包括：溢出攻击类、RPC 攻击类、WEBCGI 攻击类、拒绝服务类、木马类、蠕虫类、扫描类、网络访问类、HTTP 攻击类、系统漏洞类等； 支持检测包括 land、Smurf、Pingofdeath、winnuke、tcp_sscan、ip_opTSon、teardrop、targa3、IDSpoof、Synflood、Icmpflood、Udpflood、Portscan、IDSweep 等在内的 DOS/DDOS 攻击； 系统支持 DNS 异常包及 DNS Flood 攻击检测；支持 DHCP 异常包及 DHCP Flood 攻击检测； 支持 ARP 异常包及 ARP Flood 攻击检测；支持 CC 攻击检测；支持 DDOS 机器人自学习功能，学习时间可设置； 配置攻击报文取证功能，检测到攻击事件后将原始报文完整记录下来，作为电子证据； 系统支持扩展无线入侵防御功能； 支持 WEB 站点漏洞扫描功能，内置爬虫、支持关键字自学习和 HTML 分析； 系统支持网页防篡改功能； 应支持设备温度监视以及报警，可以自定义温度阀值。（提供功能界面截图证明）； 系统应支持多种形式的日志存储,本地存储、发送至日志服务器、本地+日志服务器双存储、自动方式判断日志服务器状态自动决定日志的记录方式。（需提供界面截图）； 所投产品具备计算机信息系统安全专用产品销售许可证，要求提供复印件并加盖厂家章； 所投产品具备涉密信息系统产品检测证书，要求提供复印件并加盖厂家章； 所投产品厂家具备国家级网络安全应急服务支撑单位证书（国家级），要求提供复印件并加盖厂家章； 提供三年免费原厂质保，提供原厂商三年售后服务承诺函。		

注明：投标文件需逐条响应是否满足，标有▲的指标及承诺函为重大指标项。

第四章 合同条款（参考）

甲方：_____

乙方：_____

甲乙双方根据_____年____月____日(项目名称)项目(项目编号:HNZH-2018-182)竞争性谈判招标结果及招标文件的要求,经协商一致,达成以下意见。

（具体条款由甲、乙双方依据本项目招标文件、乙方投标文件进行协商。）

一、 合同纠纷处理

本合同执行过程中发生纠纷，作如下处理：

1、申请仲裁。仲裁机构为海南仲裁委员会。

2、提起诉讼。诉讼地点为采购人所在地。

二、 合同生效

本合同由甲乙双方签字盖章后生效。

付款方式：项目验收合格后一次性付清全部合同款。

三、 合同鉴证

招标人应当在本合同上签章，以证明本合同条款与采购文件、投标文件的相关要求相符并且未对采购货物（或服务）和技术参数进行实质性修改。

四、 组成本合同的文件包括：

（一）本项目招标文件；

（二）乙方的投标文件和询标时乙方的书面承诺（如有）；

（三）中标通知书；

（四）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。

五、 合同备案

本合同一式**肆**份，中文书写。甲方、乙方、招标人和主管财政部门各执一份。

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：_____

_____年___月____日 _____年___月____日

招标人：海南政辉招投标代理有限公司（盖章）

经办人：_____

_____年___月____日

第五章 报价文件内容和格式

请报价人按照以下文件要求的格式、内容制作报价文件，并按以下顺序编制目录及页码，否则可能将影响对报价文件的评价。

1、开标一览表（表 1）；

2、报价函（表 2）；

3、报价明细表(表 3）；

4、 授权委托书（表 4）；

5、供应商资格证明文件（表 5）；

6、用户需求响应表（表 6）；

7、无重大违法记录声明函（表 7）；

8、其他报价人认为需提供的材料（表 8）。

由供应商根据自身实际情况并结合采购文件相关要求据实编写，格式由投标人自定。

※投标证明文件没有注明提供原件的，所提供的复印件须加盖供应商的公章。

表 1、开标一览表

项目名称：海口市党政办公网安全保障设备采购

项目编号：HNZH-2018-182

单位：人民币 元

海口市党政办公网安全保障设备采购	
本项目投标报价（大小写一致）	（小写）：
	（大写）：
交付时间	

注：供应商的报价应包含服务、税费等所有费用。

投标单位公章 ：_____

法定代表人（授权代表）签名_____

日期： 年 月 日

表 2、报价函

致：海南政辉招投标代理有限公司：

根据贵单位项目编号为_____的报价邀请函，正式授权下述签字人_____（姓名和职务）代表报价人_____（报价单位名称），提交报价书正本一式壹份，副本一式贰份。

根据此函，我们宣布同意如下：

1、我方接受谈判文件的所有的条款和规定。

2、我方同意按照谈判文件第一章“报价人须知”的规定，本报价文件的有效期为从报价截止日期起计算的_____，在此期间，本报价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报价的所有资料或证据。

4、我方完全理解贵方不一定要接受最低报价的报价，即最低报价不是成交的保证。

5、如果我方成交，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、如果我方成交，我方将支付本次谈判的服务费。

报价人名称：_____（公章）

地址：_____邮编：_____

电话：_____传真：_____

授权代表签字：_____ 职务：_____

日期：_____

表 3、报价明细表

项目名称：海口市党政办公网安全保障设备采购

项目编号：HNZH-2018-182

序号	名称	型号/规格	单位	数量	单价	总价	交货期
1							
2							
3							
…							

注：

(1)此表为表样，行数可自行添加，但表式不变；

(2)总价=单价*数量，数量由投标人自行计算并填列；

(3)本表中“报价总计”数应当等于“报价一览表”中“投标总计”数。

报价人全称：（盖章） 授权代表签字

表 4、授权委托书

致：海南政辉招投标代理有限公司：

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_____代表我方参加海南政辉招投标代理有限公司组织的海口市党政办公网安全保障设备采购（项目编号为：）的政府采购活动，并授权其全权办理以下事宜：

1、参加报价活动；

2、出席谈判会议；

3、签订与成交事宜有关的合同；

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）

受托人　（签名）

年　　月　　日

表 5：报价人资格要求证明材料：（详见第一章供应商资格要求）

表 6、用户需求响应表

项目名称：海口市党政办公网安全保障设备采购

项目编号：HNZH-2018-182

序号	货物名称	采购性能指标及技术参数	投标性能指标及技术参数	偏离情况说明（＋/-/=）
1				
2				
3				
4				
5				
	…			

报价人全称（公章）： **授权代表（签字）：**

注：1、此表为表样，行数可自行添加，但表式不变。

2、请在“投标人技术参数/功能描述” 中列出所投设备/项目的详细技术参数和功能描述情况，要求将技术参数和功能分别描述，否则将视为不响应或负偏离。

3、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。

表 7、 无重大违法记录声明函

海南政辉招投标代理有限公司：

我单位在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。

特此声明！

投标单位盖章：
年 月 日

表 8、其他报价人认为需提供的材料

第六章 评审办法

一、 评审原则

1、本次采购采用竞争性谈判方式进行，评审由依法组成的谈判小组负责完成。评审基本原则：评审工作应依据《中华人民共和国政府采购法》以及国家和地方政府采购的有关规定，遵循“公开、公平、公正、择优、诚实信用”的原则。

2、本次评审是以谈判文件，报价文件和谈判承诺文件和最终报价（即二次报价）为依据，按公正、科学、客观、平等竞争的要求，谈判小组从质量和服务均能满足采购文件实质性响应要求的供应商中，按照最后报价由低到高的顺序提出 3 名（含）以上成交候选人。

3、参加谈判工作的所有人员应遵守《中华人民共和国政府采购法》以及国家和地方政府采购的有关规定，严格保密，确保竞争性谈判工作公平、公正，任何单位和个人不得无理干预谈判小组的正常工作。

二、 评审程序和评审方法

评审程序分初步评审和谈判。

1、 初步评审

进入评审程序后，谈判小组先对报价人的报价文件进行初步评审。谈判小组将根据评审办法的规定和**初步审查表**的内容，对报价文件进行初步评审。

出现下列情况的报价文件将被认定为不满足采购需求而不能通过初步审查：

（1）报价人未提交报价保证金或金额不足、出具的证明不按谈判文件要求的；

（2）资格证明文件不全的。

（3）报价文件无法定代表人签字，或签字人无有效的法定代表人授权书的；

（4）报价文件有效期不足的；

（5）非固定价格投标的；

（6）不满足谈判文件规定的其它条件的。

初步评审采用“一项否决”的原则，只有全部符合要求的才能通过初步评审。

2、 谈判（二次报价）

按照评审程序的规定，谈判小组阅读通过初步评审的报价人的报价文件，据此与报价人进行技术、商务、服务和价格内容的澄清、修正和谈判，谈判中发现报价人的报价文件资料不清晰或造成理解有歧义时,谈判小组准许其在规定时间内做出解释说明，如

不及时做出合理的说明，该报价则将会由于不符合谈判的基本要求而被拒绝。

3、推荐成交候选人

1 有效报价是指通过文件初审的报价人最终报价经价格核对后的评审价格，且不超过采购人的预算。

2 如果有效报价达到 3 家或以上，谈判小组从质量和服务均能满足采购文件实质性响应要求的供应商中，按照最后报价由低到高的顺序提出 3 名（含）以上成交候选人。

三、 报价的核对

3 谈判小组详细分析、核对价格表，看其是否有计算上或累加上的算术错误，修正错误的原则如下：

1.1 若用数字表示的金额和用文字表示的金额不一致，以文字表示的金额为准；

1.2 当单价与数量的乘积与总价不一致时，以单价为准，并修正总价；（小数点明显标示错误的除外）

4 谈判小组将按上述修正错误的方法调整报价文件中的报价，调整后的价格对报价人具有约束力。如果报价人不接受修正后的价格，则其报价将被拒绝。

四、 谈判、评审过程的保密性。

1、接受报价后，直至成交报价人与买方签订合同后止，凡与谈判、审查、澄清、评价、比较、确定成交人意见有关的内容，任何人均不得向报价人及与谈判评审无关的其他人透露。

2、从报价递交截止时间起到确定成交报价人日止，报价人不得与参加谈判、评审的有关人员私下接触。在谈判评审过程中，如果报价人试图在报价文件审查、澄清、比较及推荐成交报价人方面向参与谈判评审的有关人员和采购人施加任何影响，其报价将被拒绝。

五、 接受和拒绝任何或所有报价的权利。

招标人和采购人保留在成交之前任何时候接受或拒绝任何报价，以及宣布竞争性谈判无效或拒绝所有报价的权力，对受影响的报价人不承担任何责任。

六、 变更技术方案的权利。

在竞争性谈判过程中，采购人有权变更技术方案或采购数量，如果报价人根据采购人提出的变更要求调整方案或价格后未能获得合同，采购人和招标人不承担任何责任。

附表 1、初步审查表

项目名称：海口市党政办公网安全保障设备采购

项目编号：HNZH-2018-182 日期：2018 年 5 月 24 日

序号	审查项目	评议内容（无效投标认定条件）	投标人		
			1#	2#	3#
1	投标人的资格	符合第一章报价人资格要求			
2	投标文件的有效性	是否符合招标文件的式样和签署要求且内容完整无缺漏			
3	保证金	投标保证金是否按要求提交			
4	投标有效期	从投标截止日期起计算的 60 天			
5	实质性响应	所投产品是否完全满足招标文件要求，无其他重大指标负偏离，能满足采购需求			
6	交货期	是否满足采购要求			
7	投标报价	报价有效、不漏项、不超出采购预算			
8	其它	是否有其它无效投标认定条件			
结论（通过/不通过）					

1、在表中的各项只需填写“√/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

[末页]