

海南省公安厅厅机关 2021 年度信息 系统运行维护项目（第二次）

竞争性谈判文件

项目编号：HNTXGP2021-095R

采购单位：海南省公安厅

采购代理机构：海南天行招投标有限公司

二〇二一年十一月

目 录

第一章	竞争性谈判公告.....	- 2 -
第二章	供应商须知前附表.....	- 4 -
第三章	供应商须知.....	- 10 -
第四章	合同主要条款（参考）.....	- 22 -
第五章	谈判响应文件格式.....	- 25 -
第六章	用户需求书.....	- 40 -
第七章	评审办法和程序.....	- 67 -
附件 1	- 70 -
附件 2	- 71 -

第一章 竞争性谈判公告

项目概况

海南省公安厅厅机关 2021 年度信息系统运行维护项目（第二次）的潜在供应商应在海口市龙华区渡海路 1-31（宝岛花园 C 栋铺面二层）获取采购文件，并于 2021 年 12 月 06 日 09 点 00 分（北京时间）前提交响应文件。

1、项目基本情况

项目编号：HNTXGP2021-095R

项目名称：海南省公安厅厅机关 2021 年度信息系统运行维护项目（第二次）

采购方式：竞争性谈判

预算金额：210 万元

最高限价：210 万元

采购需求：项目分四个包

A 包：厅机关信息系统等保测评（1），预算金额 50 万元；

B 包：厅机关信息系统等保测评（2），预算金额 50 万元；

C 包：厅机关信息系统等保测评（3），预算金额 50 万元；

D 包：厅机关信息系统网络安全整改服务，预算金额 60 万。

超出采购预算金额（最高限价）的报价，按无效报价处理，详见《用户需求书》部分。

合同履行期限（服务期）：**A、B、C 包：**合同签订后 120 日历天完成（其中等保三级系统在 2021 年 12 月 30 日之前完成信息系统安全保护等级测试评估-等级测评工作，并出具《网络安全等级保护等级测评报告》和《安全建设整改设计方案》）；**D 包：**合同签订后的 1 年。

本项目不接受联合体投标。

2、申请人的资格要求（A、B、C、D 包）

1、满足《中华人民共和国政府采购法》第二十二条的规定：

（1）在中华人民共和国注册的、具有独立承担民事责任能力的法人（需提供营业执照副本复印件或三证合一营业执照复印件加盖公章）。

(2) 在人员、设备、资金等方面具有相应的服务能力（提供承诺函加盖公章）。

(3) 具有依法缴纳税金和社会保障资金的良好记录（提供 2021 年任意 3 个月缴纳税金、缴纳社保记录凭证复印件加盖公章。投标供应商是零报税的，应提供由税务部门盖章的纳税申报表。依法免税或不需要缴纳社会保障资金的投标供应商，提供相应文件证明其依法免税或不需要缴纳社会保障资金）。

(4) 具有良好的商业信誉和健全的财务会计制度（提供 2020 年度经会计师事务所审核的财务审计报告或 2021 年任意一个月的财务报表需含资产负债表、利润表和现金流量表复印件加盖公章）。

(5) 具有国家网络安全等级保护工作协调小组办公室颁发的网络安全等级保护测评机构推荐证书或公安部第三研究所颁发的网络安全等级测评与检测评估机构服务认证证书（提供推荐证书复印件）。

(6) 提供参加采购活动前三年内（成立不足三年的从成立之日起计算），在经营活动中没有重大违法记录的声明函（加盖公章）。

(7) 提供供应商在“信用中国”网站（www.creditchina.gov.cn）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和没有被列入“中国政府采购网”（www.ccgp.gov.cn）政府采购严重违法失信行为记录名单（提供 4 张查询截图，显示的查询时间范围须在本项目采购公告发布之后至投标截止日之间）。

2、落实政府采购政策需满足的资格要求： / 。

3、本项目的特定资格要求：

(1) 投标人近三年（2018 年 1 月 1 日起）或企业注册成立之日起无不良行为记录；没有处于被责令停业、投标资格被取消、财产被接管、冻结、破产状态；在最近三年内没有骗取成交和严重违约及重大质量、安全问题（提供声明函加盖公章）；

(2) 单位负责人为同一人或者存在控股、管理关系的不同单位，不得同时参加本项目的投标（提供声明函加盖公章）。

3、获取采购文件

时间：2021 年 11 月 30 日至 2021 年 12 月 03 日，每天上午 08:30 至 12:00，下午 14:30 至 17:30（北京时间，法定节假日除外）。

地点：海口市龙华区渡海路 1-31（宝岛花园 C 栋铺面二层）。

方式：现场、网上同时提交资料；A、B、C、D 包各售价：300.00 元。

现场报名须提交以下资料：（注：递交报名资料时，请注明报的项目包号）

（1）法定代表人携带法定代表人证明书或其授权代表携带法定代表人授权委托书，附营业执照、法定代表人身份证复印件和授权代理人身份证复印件加盖公章；

（2）提供在国家企业信用信息公示系统中查询的企业股东及出资信息（详细到自然人）截图（以上资料复印件均需加盖公章）

网上下载须提交以下资料：海南政府采购网-海南省政府采购电子化交易系统（必须注册系统下载谈判文件）；网上报名时按照系统要求提交资料，并邮寄纸质报名材料到代理机构（纸质资料：1. 法定代表人携带法定代表人证明书或其授权代表携带法定代表人授权委托书，附营业执照、法定代表人身份证复印件和授权代理人身份证复印件加盖公章；2. 国家企业信用信息公示系统中查询的企业股东及出资信息（详细到自然人）截图）。

报名费付款方式：网上支付报名时需公对公转账，现场报名时可缴纳现金。

银行账户：海南天行招投标有限公司

开户银行：中国农业银行海口华信支行

银行账号：21103001040010559

4、响应文件提交

截止时间：2021 年 12 月 06 日 09 点 00 分（北京时间）

地点：海口市龙华区渡海路 1-31（宝岛花园 C 栋铺面二层）。

5、开启

时间：2021 年 12 月 06 日 09 点 00 分（北京时间）

地点：海口市龙华区渡海路 1-31（宝岛花园 C 栋铺面二层）。

6、公告期限

自本公告发布之日起 3 个工作日

7、其他补充事宜

1. 公告发布媒介：中国海南政府采购网。

8、对本次竞争性谈判提出询问，请按以下方式联系

1. 采购人信息

名 称：海南省公安厅

地 址：海口市

联系方式：吴先生；0898-68836887

2. 采购代理机构信息

名 称：海南天行招投标有限公司

地 址：海口市龙华区渡海路 1-31（宝岛花园 C 栋铺面二层）

联系方式：胡工；0898-68597362

3. 项目联系方式

项目联系人：胡工

电话：0898-68597362

第二章 供应商须知前附表

本表关于采购货物的具体要求是对供应商须知的具体补充和修改，如有矛盾，应以本表为准。

序号	内容
1	采购人：海南省公安厅 联系人：吴先生 联系电话：0898-68836887 地址：海口市
2	代理机构：海南天行招投标有限公司 联系人：胡工 电话：0898-68597362 详细地址：海口市龙华区渡海路 1-31（宝岛花园 C 栋铺面二层）
3	供应商资格要求：详见竞争性谈判公告
4	谈判文件的澄清：提交响应文件截止之日 3 个工作日前以书面形式通知
5	谈判文件的修改：提交响应文件截止之日 3 个工作日前以书面形式通知
6	供应商提供的谈判响应文件应由以下内容组成，实际响应中如有必要，供应商可对未涉及的部分予以补充： <ol style="list-style-type: none"> 1. 报价函 2. 报价一览表 3. 法定代表人身份证明 4. 授权委托书 5. 供应商基本情况表 6. 资格证明材料 <ol style="list-style-type: none"> 6.1 营业执照副本复印件加盖公章 6.2 具有依法缴纳税金和社会保障资金的良好记录（提供 2021 年任意 1 个月缴纳税金、缴纳社保记录凭证复印件加盖公章。投标供应商是零报税的，应提供

	<p>由税务部门盖章的纳税申报表。提供的资料须加盖单位公章。依法免税或不需要缴纳社会保障资金的投标供应商，提供相应文件证明其依法免税或不需要缴纳社会保障资金)</p> <p>6.3 具有良好的商业信誉和健全的财务会计制度（提供 2020 年度经会计师事务所审核的财务审计报告或 2021 年任意一个月的财务报表复印件：资产负债表、利润表和现金流量表。材料复印件加盖公章）</p> <p>6.4 谈判保证金缴纳凭证加盖公章</p> <p>6.5 声明函</p> <p>6.6 承诺函</p> <p>7. 技术、商务响应表</p> <p>8. 采购代理服务承诺书</p> <p>9. 中小企业声明函</p> <p>10. 供应商认为需要提供的用于参与评审其他材料</p> <p>注：供应商编制上述文件时，本谈判文件第五章已提供格式的文件须按格式要求填写。</p>
7	<p>合同履行期限（服务期）：A、B、C 包：合同签订后 120 日历天完成（其中等保三级系统在 2021 年 12 月 30 日之前完成信息系统安全保护等级测试评估-等级测评工作，并出具《网络安全等级保护等级测评报告》和《安全建设整改设计方案》）；D 包：合同签订后的 1 年。本项目不接受联合体投标。</p>
8	<p>本项目不接受联合体</p>
9	<p>备选方案：不接受</p>

10	<p>谈判保证金金额： A包缴纳：人民币伍仟元整（¥5000.00）； B包缴纳：人民币伍仟元整（¥5000.00）； C包缴纳：人民币伍仟元整（¥5000.00）； D包缴纳：人民币壹万元整（¥10000.00）。</p> <p>银行账户：海南天行招投标有限公司 开户银行：中国农业银行海口华信支行 银行账号：21103001040010559 用途：（项目编号及包号）谈判保证金 递交截止时间：2021年12月06日09时00分前（以到达指定账户时间为准）</p> <p>缴纳凭证：银行转账凭证 注：1、谈判保证金由供应商账户转出；2、用途须注明简要项目编号。</p>
11	投标有效期：自响应文件递交截止之日起60天
12	谈判响应文件份数：正本一份，副本两份，电子版文件一份。
13	谈判响应文件递交地点：详见竞争性谈判公告
14	供应商在递交谈判响应文件的同时，应将报价函、报价一览表、保证金缴纳凭证密封在一个报价信封内，单独递交。
15	谈判响应文件递交截止时间：2021年12月06日09点00分（北京时间）
16	<p>开标时间：同谈判响应文件递交截止时间。</p> <p>开标地点：同谈判响应文件递交地点。</p>
17	<p>出现以下情况将可导致供应商的投标被拒绝：</p> <ol style="list-style-type: none"> 1. 谈判响应文件的密封、签署、盖章不符合谈判文件的要求； 2. 供应商的资格证明文件不符合谈判文件的要求； 3. 报价函或投标报价不符合谈判文件的要求； 4. 保证金不符合谈判文件递交的要求； 5. 谈判响应文件的响应与谈判文件的实质性要求存在重大偏离； 6. 不符合法律、法规和谈判文件中规定的其他实质性要求。
18	谈判小组由3名专家组成，按规定在海南省综合评标专家库中抽取3名专家。
19	推荐成交候选人3名

20	<p>预算金额（最高限价）：</p> <p>A包：厅机关信息系统等保测评（1），预算金额 50 万元；</p> <p>B包：厅机关信息系统等保测评（2），预算金额 50 万元；</p> <p>C包：厅机关信息系统等保测评（3），预算金额 50 万元；</p> <p>D包：厅机关信息系统网络安全整改服务，预算金额 60 万。</p> <p>【（超出采购预算金额（最高限价）的报价，按无效报价处理）】</p>
21	<p>1、采购代理服务费用由成交人按照预算金额参照国家发展计划委员会文件《采购代理服务收费管理暂行办法》（计价格【2002】1980号）文件中相关规定进行支付。在成交通知书签发前一次性付清。</p> <p>2、供应商应在成交通知书签发后 30 天内与采购人签订合同，并在签订合同后 2 个工作日内将合同送到代理机构进行盖章见证和公示（如需）。</p>

第三章 供应商须知

一、总则

1、资金来源：财政资金。

采购人：见《供应商须知前附表》

采购代理机构：见《供应商须知前附表》

2、合格的供应商

2.1 合格的供应商：见《谈判公告》及《供应商须知前附表》中规定的内容。

2.2 联合体投标：本次采购不接受联合体。

2.3 合格的货物和服务：合同规定的货物和服务指其来源符合谈判文件要求的货物和服务。

2.4 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采购活动。除单一来源采购项目外，为采购项目提供整体设计、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。

2.5 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。

2.6 采购文件中未明确规定允许进口产品参加的，均视为拒绝进口产品参加。（进口产品是指通过中国海关报关验放进入中国境内且产自关境外的产品）。

2.7 现场信用记录查询：

2.7.1 采购代理机构在初步审查环节查询供应商的信用记录。供应商存在不良信用记录的，将被认定为无效响应，并交由谈判小组签字确认。在初步审查结束之后，网站信息发生的任何变更均不再作为评审依据。

2.7.2 不良信用记录指：在“信用中国”网站（www.creditchina.gov.cn）没有被列入重大税收违法案件当事人名单、政府采购严重违法失信名单，没有被列入中国执行信息公开网（<http://zxgk.court.gov.cn/shixin/>）失信被执行人名单和没有被列入“中国政府采购网”（www.ccgp.gov.cn）政府采购严重违法失信行为记录名单投标人。以联合体形式参加投标的，联合体任何成员存在以上不良信用记录的，将被认定为响应无效。

2.7.3 供应商不良信用记录以采购代理机构于开标当天查询结果为准。

3、投标费用

无论投标过程中的作法和结果如何，供应商准备和参加投标活动发生的费用自理。供应商应承担所有与编写和递交谈判响应文件有关费用，采购人和采购机构在任何情况下不负担这些费用。

二、 谈判文件

4、谈判文件的构成

4.1 谈判文件包括：

- 第一章 竞争性谈判公告
- 第二章 供应商须知前附表
- 第三章 供应商须知
- 第四章 合同主要条款（参考）
- 第五章 谈判响应文件格式
- 第六章 用户需求书
- 第七章 评审办法和程序

4.2 供应商应审阅谈判文件中所有须知、格式、条款和规格。供应商未按采购文件要求提供全部资料或提交的谈判响应文件未对谈判文件作出实质性响应，那么供应商将承担其风险并有可能根据第 22 款导致谈判响应文件被拒绝。

5、谈判文件的澄清

任何对谈判文件提出澄清的供应商，应在《供应商须知前附表》中规定的提交响应文件截止之日前 1 日以书面形式通知采购代理机构。采购机构将视情况对提交响应文件截止之日前 1 日收到的澄清要求采用适当方式或以书面形式予以答复，并在其认为必要时，将不标明查询来源的书面答复发给每一已购买谈判文件的潜在供应商。

6、谈判文件的修改

在提交响应文件截止之日前 3 个工作日的任何时候，无论何故，采购人可主动地或在答复供应商提出澄清的问题时对谈判文件进行修改。

谈判文件的修改将以书面形式通知所有购买谈判文件的供应商，并对其具有约束力。供应商在接收后 1 日内应立即以传真的形式确认已收到该修改。

为使供应商在准备谈判文件时有合理的时间考虑谈判文件的修改，采购人可酌情推迟

第 18 款中规定的提交响应文件截止之日。

三、谈判响应文件的编制

7、投标使用的文字

谈判响应文件所有部分均应以中文编制。

8、谈判响应文件的组成

8.1 供应商准备的谈判响应文件应包括以下部分：

- (1) 按第五章谈判响应文件格式填写的报价函及报价一览表。
- (2) 报价一览表与报价函总价不符，以报价一览表为准。
- (3) 按第 12 款出具的，证明供应商有资格投标以及如果成交有能力履行合同的证明

文件。

- (4) 按第 14 款出具的保证金。

8.2 供应商应按第五章《谈判响应文件格式》中规定的结构和顺序编制谈判响应文件。

9、谈判响应文件格式

供应商应按谈判文件第五章提供的谈判响应文件格式编制谈判响应文件。

10、投标报价

10.1、本项目为固定预算采购，任何有选择报价将不予接受，只允许有一个报价。

10.2、响应总报价及分项报价应包括：采购内容的全部费用。

10.3、报价函和报价一览表中所填的价格在合同执行过程中是固定不变的；除非另有规定，非固定的投标价将根据第 22 款规定被采购人拒绝。

10.4、其他要求见《供应商须知前附表》。

11 投标货币

本次采购的货物以人民币进行报价，以其它货币标价的投标将被拒绝。

12 供应商的合格性和资格的声明文件

12.1 根据第 12.2 款规定，供应商须提交证明其有资格进行投标和有能力履行合同的文件，作为谈判响应文件的一部分。

12.2 供应商提供的履行合同的资格声明文件应使采购人满意：

- (1) 供应商具有履行合同所需的财务、技术和生产能力；

(2) 供应商应填写并提交谈判文件第五章上所附的“资格证明文件” 中的所有内容。

13、货物的合格性及符合谈判文件规定的证明文件

13.1 供应商须提交证明其拟供货物和辅助服务的合格性并符合谈判文件规定的证明文件，作为谈判响应文件的一部分。证明文件可以是文字资料、彩页和数据。

13.2 谈判文件规定的其他必要文件。

14、谈判保证金

14.1 根据第 8 款规定，供应商报价时按《供应商须知前附表》中的规定提交谈判保证金。

14.2 谈判保证金是用于保护本次采购免受供应商的行为而引起的风险，根据第 14.6 款规定，发生下述行为予以没收谈判保证金。

14.3 谈判保证金使用投标货币表示，只能采取下列形式：按《供应商须知前附表》执行。

14.4 任何未按第 14.1 款和第 14.3 款规定提交谈判保证金的投标，将被视为非响应性投标而按第 22 款予以拒绝。

14.5 未成交供应商的谈判保证金在成交通知书发出后 5 个工作日退还，成交供应商的谈判保证金在采购合同签订后 5 个工作日退还。

14.6 若发生下列情况，采购人在书面通知后有权没收谈判保证金：

- (1) 供应商在提交响应文件截止时间后撤回响应文件的；
- (2) 供应商在响应文件中提供虚假材料的；
- (3) 除因不可抗力或谈判文件、谈判公告认可的情形以外，成交供应商不与采购人签订合同的；
- (4) 供应商与采购人、其他供应商或者采购代理机构恶意串通的；
- (5) 成交后未按规定缴付采购代理服务费的；
- (6) 谈判文件对履约保证金有要求，而成交供应商未按规定提交履约保证金。

15、投标有效期

15.1 谈判响应文件将在开标日期后《供应商须知前附表》中规定的时间内有效。投标有效期比规定短的可以视为非响应标予以拒绝。

15.2 在特殊情况下，采购人可于投标有效期满之前要求供应商同意延长有效期。要求与答复均应为书面形式往来。供应商可以拒绝上述要求而其保证金不被没收。对于同意该要求的供应商，既不要求也不允许其修改谈判响应文件，但将要求其响应延长保证金的有效期。

16、谈判响应文件的式样和签署

16.1 供应商应按《供应商须知前附表》中规定的数量递交谈判响应文件，**每一份谈判响应文件必须胶装成册**。并要明确注明“正本”和“副本”，如正本和副本或电子文档有差异，以正本为准。

16.2、谈判响应文件正本须打印或用不褪色墨水书写并由法定代表人或授权委托人签字，后者须将“授权委托书”以书面形式附在谈判响应文件中。响应文件的正本须经法定代表人或授权代表人签署和加盖供应商公章，并须加盖骑缝章。谈判响应文件副本可以是正本的复印件。

16.3、除供应商对错处作必要修改外，谈判响应文件中不许有加行、涂抹或改写。若有修改须由签署谈判响应文件的人进行签字，并加盖公章，否则视为无效。

16.4、传真投标、邮寄投标概不接受。

四、谈判响应文件的递交

17、谈判响应文件的密封和标记

17.1、供应商应将谈判响应文件正本和副本分别密封在两个投标专用袋（箱）中，并标明“正本”或“副本”，并在文件专用袋（箱）上标明“正本”“副本”字样。

供应商在递交谈判响应文件的同时，应将报价函、报价一览表、谈判保证金缴纳凭证密封在一个报价信封内，信封上标注“唱标信封”字样，并写明供应商名称、包号、地址、联系人和联系方式，报价信封不密封于正本、副本内，单独密封递交。

供应商务必在开标时提交电子版和纸质版响应文件，电子版响应文件（PDF 格式）的递交，电子版响应文件（PDF）也应密封在小信封内，且标注公司名称，电子文档密封于“正本”内，同时随纸质版响应文件一起递交，否则视为无效响应；供应商提供的电子版响应文件（PDF 格式）必须与纸质版响应文件的正本保持一致。注：电子版 PDF 格式需为纸质文件签字加盖公章扫描件。

17.2、投标专用袋（箱）上须按采购代理机构提供的格式注明：

(1) 按《供应商须知前附表》所示注明开标地点。

(2) 注明项目名称、包号、标段、项目编号、正本、副本，并注明响应文件递交截止时间前“不准启封”的字样。

(3) 写明供应商名称、地址、联系人和联系方式。

17.3、如果未按第 17.1、17.2 款规定密封和标记，采购人将予以拒绝，并退回供应商。

18、递交谈判响应文件的截止日期

18.1 采购人收到谈判响应文件的时间不得迟于《供应商须知前附表》中规定的截止时间。

18.2 采购代理机构可按照第 6 款的规定修改谈判响应文件并酌情延长提交谈判响应文件的截止时间，在此情况下，采购代理机构、采购人和投标人的一切权利和义务将按延期后的谈判响应文件递交截止时间履行。

19、迟交的谈判响应文件

根据第 18 款规定，采购人将拒绝接收任何迟于《供应商须知前附表》中规定的截止时间递交的谈判响应文件。

20、谈判响应文件的修改和撤回

20.1 供应商在提交谈判响应文件后可对其谈判响应文件进行修改或撤回，但采购人须在提交响应文件截止之日前收到该修改或撤回的书面通知。

20.2 供应商对谈判响应文件的修改或撤回的通知应按第 16 款和第 17 款规定进行准备、密封、标注和递送。

20.3 谈判响应文件递交截止时间后不得修改谈判响应文件。

20.4 供应商不得在谈判响应文件递交截止日起至第 15 款规定的谈判响应文件有效期届满前撤销谈判响应文件。否则采购人将按第 14.6 (1) 款规定没收其谈判保证金。

五、开标与评标

21、开标

21.1 采购人在供应商代表自愿出席的情况下，在《供应商须知前附表》规定的地点和时间开标，出席代表需登记以示出席。

21.2 按照第 20 款规定，提交了可接受的“撤回”通知的谈判响应文件将不予开封。

21.3、采购代理机构、公证员（如有）或供应商代表将查验响应文件的密封情况。

22、谈判响应文件的初审

22.1 采购人、谈判小组根据“初步评审表”对谈判响应文件的资格性和符合性进行评审，只有对“初步评审表”所列各项作出实质性响应的谈判响应文件才能通过初步评审。对是否实质性响应谈判响应文件的要求有争议的投标内容，谈判小组将以记名方式表决，得票超过半数的供应商有资格进入下一阶段的评审，否则将被淘汰。具体工作包括：

（1）谈判小组将审查谈判响应文件是否完整、有无提供所需的谈判保证金、是否恰当当地签署、是否大致编排有序等；

（2）根据第 24 款规定对谈判响应文件进行详细评估之前，谈判小组将确定每一谈判响应文件是否对谈判文件的要求作出了实质性的响应。所谓作出实质性响应的投标指的是符合谈判文件要求的全部条款、条件和规格而无任何重大偏离或保留。重大偏离或保留系指实质上影响到合同项下的供货范围、质量和性能，或指与谈判文件有实质不一致，限制了合同项下采购人的权利和供应商的义务，或对该重大偏离的修改对提交实质性响应投标的供应商将不公平。谈判小组决定谈判响应文件的响应性是基于谈判响应文件的内容本身而不靠外部的证据。初步评审表详见附件 1。

22.2 谈判小组将拒绝被定为非响应性的投标，供应商不能通过修正或撤销不符之处而使其投标成为响应性投标。

在采购中，出现下列情形之一的，应予废标：

- （1）符合专业条件的供应商或者对谈判文件作实质响应的供应商不足三家的；
- （2）出现影响采购公正的违法、违规行为的；
- （3）供应商的报价均低于采购最低限价；
- （4）因重大变故，采购任务取消的。

废标后，采购人或采购代理机构应当将废标理由通知所有供应商。

22.3 谈判小组将对确定为实质上响应的投标进行审核，看其是否有计算上和累加上算术错误，修正错误的原则如下：

（1）谈判响应文件中开标一览表（报价表）内容与谈判响应文件中明细表内容不一致的，以开标一览表（报价表）为准；

- （2）谈判响应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；单价金额小数点有明显错位的，应以总价为准，并修改单价；

(4) 对不同文字文本谈判响应文件的解释发生异议的，以中文文本为准。

22.4 谈判小组将按上述修正错误的方法调整谈判响应文件中的投标报价，调整后的价格应对供应商具有约束力。如果供应商不接受修正后的价格，则其投标将被拒绝，其保证金将被没收。

22.5 对供应商报价经过上述修正和调整（包括缺漏项调整）后所得出的价格构成其“评标价”。

22.6 谈判小组将允许修正谈判响应文件中不构成重大偏离的、微小的、非正规的、不一致的或不规则的地方，但这些修正不能影响任何供应商相应的名次排列。

23 谈判响应文件的澄清

对谈判响应文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，谈判小组可以书面形式要求供应商作出必要的澄清、说明或者纠正。供应商的澄清、说明或者补正应当采用书面形式，由其授权的代表签字，并不得超出谈判响应文件的范围或者改变谈判响应文件的实质性内容。

24 谈判响应文件的详细评审：详见第七章《评审办法和程序》。

25 确定成交供应商

谈判小组根据质量和服务均能满足采购文件实质性响应要求且报价最低的原则确定成交供应商。若报价相同的，按技术指标优劣顺序排列。采购人或者采购代理机构应当在成交供应商确定后2个工作日内，在指定的媒体上公告成交结果。

六、授予合同

26 授予合同的准则

26.1 除第29款规定外，合同将授予采购人确定的成交供应商。成交供应商放弃成交或因不可抗力提出不能履行合同，或者谈判文件规定应当提交履约保证金而在规定的期限内未能提交的，采购人可以与排位其后第一位的供应商签订合同，以此类推。

26.2 如采购人发现成交供应商在投标、提供资料时有弄虚作假的行为，经核实，采购人有权拒绝该成交供应商的投标。

26.3 其他规定见《供应商须知前附表》。

27 资格后审

27.1 在没有进行过资格预审的情况下，谈判小组有权进一步审查排名第一的供应商的财务、技术和供货能力及信誉，确定其是否有资格能圆满地履行合同。如果审查通过，则将合同授予该供应商；如果审查没有通过，则拒绝其投标。在此情况下，谈判小组将对排位其后第一位的供应商的能力做类似的审查。

28 在授予合同时变更采购货物数量的权利（适用）

29 接受和拒绝任何投标或所有投标的权利（适用）

29.1、供应商的报价均超过了采购预算（最高限价），且采购人不能支付的，将予以废标；

29.2、因重大变故或为维护国家利益，采购人在授予合同之前仍保留接受或拒绝任何投标或所有投标的权利。

30 成交通知

30.1 谈判响应文件有效期期满前，采购人将以书面形式通知成交供应商其投标被接受。

30.2 采购人向成交供应商发出书面通知的同时，采购人通知落选的供应商其投标未被接受，并按第 14 款规定退还其谈判保证金。

30.3 成交通知书是合同的一个组成部分。

31 签署合同

31.1 采购人通知成交供应商成交时，将提供谈判文件中的合同格式，包括双方之间的有关协议给成交供应商。

31.2 成交供应商在收到成交通知书和合同格式后，在成交通知书上规定的时间内，应派授权代表前往采购人指定地点签订合同。

32 履约保证金（按谈判文件要求执行）

34 采购代理服务费用

采购代理服务费由成交人按照预算金额参照国家发展计划委员会文件《采购代理服务费收费管理暂行办法》（计价格【2002】1980号）文件中相关规定进行支付。在成交通知书签发前一次性付清。

35 质疑和投诉

35.1、质疑、投诉的接收和处理严格按照《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》、《政府采购质疑和投诉办法》、《财政部关于加强政府采购供应商投诉受理审查工作的通知》的规定办理。

35.2、供应商对采购活动事项有疑问的，可以向采购人或采购代理机构提出询问，采购人或采购代理机构应当及时作出答复，但答复的内容不得涉及商业秘密。

35.3、供应商认为采购文件、采购过程和成交、成交结果使自己的权益受到损害的，可以书面形式向采购人或采购代理机构提出质疑。

35.4、采购人或采购代理机构应当在收到供应商的书面质疑后7个工作日内作出答复，并以书面形式通知质疑供应商和其他有关供应商，但答复的内容不得涉及商业秘密。

35.5、质疑供应商对采购人、采购代理机构的答复不满意或者采购人、采购代理机构在规定的时间内作出答复的，可以在答复期满后15个工作日内向采购人监督管理部门投诉。

35.6、供应商提出质疑应当提交质疑函和必要的证明材料。质疑函应当包括下列内容：（一）供应商的姓名或者名称、地址、邮编、联系人及联系电话；（二）质疑项目的名称、编号；（三）具体、明确的质疑事项和与质疑事项相关的请求；（四）事实依据；（五）必要的法律依据；（六）提出质疑的日期。供应商为自然人的，应当由本人签字；供应商为法人或者其他组织的，应当由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。质疑人未按相关法律法规及本谈判文件规定的内容提出质疑的，视为无效质疑，采购人或代理机构将不予受理。

36 政策功能

36.1、本次招标优先选购中华人民共和国财政部公布的《节能环保产品目录》的标的物。

36.2、强制采购节能产品、信息安全产品，优先采购环境标志产品。节能产品是指列入财政部、国家发展和改革委员会制定的《节能产品政府采购清单》，且经过认定的节能产品；信息安全产品是指列入国家质检总局 国家认监委《信息安全产品强制性认证目录》，并获得强制性产品认证证书的产品；环境标志产品是指列入财政部、国家环保总局制定的《环境标志产品政府采购清单》，且经过认证的环境标志产品。

36.3、投标产品属于信息安全产品的，供应商应当选择经国家认证的信息安全产品投

标，并提供由中国信息安全认证中心按国家标准颁发的有效认证证书复印件。

36.4、投标产品属于政府强制采购节能产品的，供应商应当选择《节能产品政府采购清单》中的产品投标，并提供有效的节能产品认证证书复印件。

36.5、谈判文件中提供的参考产品品牌或型号，是采购人根据项目所要实现的功能根据市场情况列出的品牌或型号，并不是限制条件。

36.6、供应商为小型和微型企业（含联合体）的情况：

36.6.1、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）根据财库〔2014〕68号《财政部司法部关于政府采购支持监狱企业发展有关问题的通知》，监狱企业视同小微企业。监狱企业是指由司法部认定的为罪犯、戒毒人员提供生产项目和劳动对象，且全部产权属于司法部监狱管理局、戒毒管理局、直属煤矿管理局，各省、自治区、直辖市监狱管理局、戒毒管理局，各地（设区的市）监狱、强制隔离戒毒所、戒毒康复所，以及新疆生产建设兵团监狱管理局、戒毒管理局的企业。监狱企业投标时，提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件，不再提供《中小微企业声明函》。

（5）根据财库〔2017〕141号《财政部民政部中国残疾人联合会关于促进残疾人就业政府采购政策的通知》，在采购活动中，残疾人福利性单位视同小型、微型企业，享受政府采购支持政策的残疾人福利性单位应当同时满足《财政部民政部中国残疾人联合会关于促进残疾人就业政府采购政策的通知》所列条件。残疾人福利性单位属于小型、微型企业的，不重复享受政策。符合条件的残疾人福利性单位在参加采购活动时，应当提供《残疾人福利性单位声明函》，并对声明的真实性负责。

36.6.2、具体评审价说明：

（1）供应商为小型或微型企业，其评审价=投标报价*（1-6%）；

(2) 供应商为联合体投标，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%)。

(3) 供应商为工信部联企业〔2011〕300 号文规定的小型 and 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〔2020〕46 号），并提供中小企业声明函，否则无效。**如有虚假骗取政策性加分，将依法承担相应责任。**

第四章 合同主要条款（参考）

合同编号：

甲方：

乙方：

甲乙双方根据 2021 年____月____日（项目编号：HNTXGP2021-095R、海南省公安厅机关 2021 年度信息系统运行维护项目（第二次））竞争性谈判采购结果及竞争性谈判文件的要求，经协商一致，达成如下货物购销合同：

一、货物及其数量、金额等

项目名称	
服务内容	
项目包号	
合同总金额：人民币（大写） ¥：	
甲方	联系人： 固定电话：
乙方	联系人： 固定电话：

二、工期/交货期/服务期：

- 1、服务地点：采购人指定地点
- 2、服务期：**A、B、C 包**：合同签订后 120 日历天完成（其中等保三级系统在 2021 年 12 月 30 日之前完成信息系统安全保护等级测试评估-等级测评工作，并出具《网络安全等级保护等级测评报告》和《安全建设整改设计方案》）；**D 包**：合同签订后的 1 年。
- 3、提供技术支持和服务，2 小时内作出实质性响应，对重大问题提供现场技术支持，8 小时内到达指定现场。

4、培训：负责在现场对设备使用维护人员进行设备安装、操作、使用、维护及结构原理方面的培训，乙方承担由此产生的一切费用

5、验收要求：按谈判文件技术参数和国家行业标准进行验收。

三、付款

A、B、C包：

1) 本合同签订后，甲方凭乙方开具的正式有效发票在 20 个工作日内向乙方支付合同金额的 30%；

2) 项目终验通过后，乙方出具的 5%的银行质保函，甲方凭乙方开具的正式有效发票在 20 个工作日内向乙方支付合同金额的 70%。

D包：

1) 本合同签订后，甲方凭乙方开具的正式有效发票在 20 个工作日内向乙方支付合同金额的 40%；

2) 项目服务期限结束后，甲方凭乙方开具的正式有效发票在 20 个工作日内向乙方支付合同金额的 60%；

四、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，按合同金额的 0.5% 计扣违约赔偿费。但违约赔偿费的最高限额为合同金额的 15%。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。

五、合同纠纷处理：本合同执行过程中发生纠纷，作如下处理：

1、由甲乙双方协商处理。

2、申请仲裁。仲裁机构为海南省经济仲裁委员会。

3、提起诉讼。诉讼地点为采购人所在地。

六、合同生效：本合同由甲乙双方签字盖章后生效。

七、合同鉴证：采购代理机构应当在本合同上签章，以证明本合同条款与竞争性谈判文件、响应文件的相关要求相符并且未对采购货物和技术参数进行实质性修改。

八、组成本合同的文件包括：

- (一) 合同通用条款和专用条款；
- (二) 乙方的报价一览表及报价明细表；
- (三) 成交通知书；
- (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。

九、合同备案

本合同一式伍份，中文书写。甲方执叁份、乙方、招标代理机构各执壹份。

甲方：_____（盖章）

地址：

法定（授权）代表人：

二〇二一年__月__日

乙方：_____（盖章）

地址：

法定（授权）代表人：

二〇二一年__月__日

户名：

开户银行：

账号：

代理机构声明：本合同标的经海南天行招投标有限公司依法定程序签订，合同主要条款内容与谈判、响应文件的内容一致。

代理机构：海南天行招投标有限公司（盖章）

经办人：

二〇二一年__月__日

第五章 谈判响应文件格式

封面格式：以下为参考格式，投标供应商可自行排版，但必须包含谈判文件中要求的内容。

项目名称：

项目编号

项目包号： 包

谈判响应文件

【正本/副本】

供应商名称（公章）：

法定代表人或授权代表签字：

联系电话：

日 期： 年 月 日

目 录

1. 报价函
2. 报价一览表
3. 法定代表人身份证明
4. 授权委托书

5. 供应商基本情况表

6. 资格证明材料

6.1 营业执照副本复印件加盖公章

6.2 具有依法缴纳税金和社会保障资金的良好记录（提供 2021 年任意 1 个月缴纳税金、缴纳社保记录凭证复印件加盖公章。投标供应商是零报税的，应提供由税务部门盖章的纳税申报表。提供的资料须加盖单位公章。依法免税或不需要缴纳社会保障资金的投标供应商，提供相应文件证明其依法免税或不需要缴纳社会保障资金）

6.3 具有良好的商业信誉和健全的财务会计制度（提供 2020 年度经会计师事务所审核的财务审计报告或 2021 年任意一个月的财务报表复印件：资产负债表、利润表和现金流量表。材料复印件加盖公章）

6.4 谈判保证金缴纳凭证加盖公章

6.5 声明函

6.6 承诺函

7. 技术、商务响应表

8. 采购代理服务承诺书

9. 中小企业声明函

10. 售后服务方案

11. 供应商认为需要提供的用于参与评审其他材料

注：供应商编制上述文件时，本谈判文件第五章已提供格式的文件须按格式要求填写。

1. 报价函

致：海南天行招投标有限公司

贵公司海南省公安厅厅机关2021年度信息系统运行维护项目（第二次）（项目编号：HNTXGP2021-095R） 包，竞争性谈判文件（包括更正公告，如果有的话）收悉，我们经详细审阅和研究，现决定参加投标报价。

（1）我们郑重承诺：我们是符合《政府采购法》第 22 条规定的供应商，并严格遵守《政府采购法》第 77 条的规定。

（2）我们接受谈判文件的所有的条款和规定。

（3）以转账方式提交谈判保证金，金额为人民币（大写） 元整（小写）¥ 元）。

（4）附报价一览表中规定的应提供服务投标报价为投标总价。

（5）我们同意按照谈判文件第二章“供应商须知前附表”第 11 款的规定，响应文件的有效期为自响应文件递交截止之日起 60 天，在此期间，本谈判文件将始终对我们具有约束力，并可随时被接受。如果我们成交，本谈判响应文件在此期间之后将继续保持有效。

（6）我们同意提供采购人要求的有关本次采购的所有资料。

（7）我们理解，你们无义务必须接受投标价最低的投标，并有权拒绝所有的投标。

同时也理解你们不承担我们本次投标的费用。

（8）如果我们成交，为执行合同，我们将按采购有关要求提供必要的履约保证金。

与本投标有关的一切正式往来信函请寄：

地址： 传真：

电话： 邮箱：

供应商授权代表签字：

供应商名称： （公章）

供应商开户银行：

供应商银行账户：

日期：

2. 报价一览表

项目名称：海南省公安厅厅机关 2021 年度信息系统运行维护项目（第二次）

项目编号：HNTXGP2021-095R

项目包号：_____包

序号	项目	内容
1	供应商名称	
2	投标报价（小写）	
3	投标报价（大写）	
4	合同履行期限（交货期）	
5	交货地点	

供应商名称：（公章）

法定代表人或授权代理人：（签字或盖章）

日期：

注：1、投标报价应包括谈判文件所规定的采购范围的全部内容；

2、为避免供应商为达到成交目的而刻意削价竞争，可能影响项目质量或不能诚信履约。若供应商报价低于预算的 80%（含），签订合同时采购人有权要求供应商提交成交金额的 10%作为履约保证金；如谈判小组认为供应商的报价明显低于其他通过初步审查的供应商报价的，则供应商还须提供相关低价竞标的佐证依据，该佐证将作为响应文件的组成部分并获得谈判小组评审通过，若供应商未提供或提供的佐证文件未能通过谈判小组评审，均视为无效报价。

海南省政府采购交易电子化管理系统

海南省政府采购

海南省政府采购交易电子化管理系统

海南省政府

海南省政府采购交易电子化管理系统

海南省政府

海南省政府采购交易电子化管理系统

海南省政府

海南省政府采购交易电子化管理系统

海南省政府

海南省政府采购交易电子化管理系统

海南省政府

2.1 分项报价表（___）包

（如有需提供分项报价表，格式自拟，但报价内容包括必须《项目服务内容》全部内容）

注：1、所有价格应按谈判文件规定的货币单位填写。

供应商名称：（公章）

法定代表人或授权代理人：（签字或盖章）

日期：

3. 法定代表人身份证明

单位名称：

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_____（供应商名称）_____的法定代表人。

特此证明。

附：法定代表人身份证复印件

投标供应商：_____（盖单位章）

日 期：_____年_____月_____日

法定代表人身份证正反面复印件

4. 法定代表人授权委托书

我_____（姓名）系_____（投标供应商名称）的法定代表人，现授权委托我单位_____（姓名、职务）为我公司代理人。代理人根据授权，以我方名义处理提交、签署、澄清、说明、补正、递交、撤回、修改海南省公安厅厅机关 2021 年度信息系统运行维护项目（第二次）（项目编号：HNTXGP2021-095R）包谈判响应文件、签订合同和处理有关事宜，其法律后果由我方承担。

委托期限：自响应文件递交截止之日起 60 天。

被授权人无转委托权。特此委托。

附：法定代表人和被授权人身份证复印件

投标供应商：_____（盖单位章）

法定代表人：_____（签字或盖章）

被授权人：_____（签字或盖章）

日期：____年____月____日

法定代表人和代理人身份证正反面复印件

5. 供应商基本情况表

公司名称			
注册地址		邮政编码	
联系方式	联系人		电话
	传真		网址
法定代表人	姓名		电话
技术负责人	姓名		电话
成立时间		员工总人数	
企业资质			
营业执照号			
注册资金			
开户银行			
账号			
经营范围			
备注			

6. 资格证明材料

6.1 营业执照副本复印件加盖公章

6.2 具有依法缴纳税金和社会保障资金的良好记录（提供 2021 年任意 1 个月缴纳税金、缴纳社保记录凭证复印件加盖公章。投标供应商是零报税的，应提供由税务部门盖章的纳税申报表。提供的资料须加盖单位公章。依法免税或不需要缴纳社会保障资金的投标供应商，提供相应文件证明其依法免税或不需要缴纳社会保障资金）

6.3 具有良好的商业信誉和健全的财务会计制度（提供 2020 年度经会计师事务所审核的财务审计报告或 2021 年任意一个月的财务报表复印件：资产负债表、利润表和现金流量表。材料复印件加盖公章）

6.4 谈判保证金缴纳凭证加盖公章

6.5 声明函

声明函

致：海南天行招投标有限公司

为响应贵公司组织的海南省公安厅厅机关 2021 年度信息系统运行维护项目（第二次）
（项目编号：HNTXGP2021-095R） 包，相应服务的采购活动，我公司声明：

- 1、满足《中华人民共和国政府采购法》第二十二条的规定。
- 2、在参加本次采购活动前三年内（成立不足三年的从成立之日起计算），在经营活动中没有重大事故、违法记录。
- 3、在近三年（2018 年 01 月 01 日起）或企业注册成立之日起不存在不良行为记录：没有处于被责令停业、投标资格被取消、财产被接管、冻结、破产状态；在最近三年内没有骗取成交和严重违约及重大质量、安全问题。
- 4、本公司与参加本项目的其他供应商不存在以下情形：
 - （1）单位负责人为同一人；
 - （2）存在直接控股或管理关系的。

投标供应商名称（并加盖公章）：_____

法定代表人或授权代理人（签字或盖章）：_____

日期：

6.6 承诺函

承诺函

致：海南天行招投标有限公司

为响应贵公司组织的海南省公安厅厅机关 2021 年度信息系统运行维护项目（第二次）
（项目编号：HNTXGP2021-095R）**包**，服务的采购活动，我公司承诺：

1. 在人员、设备、资金等方面具有相应的设备、专业技术和服务能力，具有履行合同所必需的设备和专业技术和服务能力。

2. 不以联合体方式投标。

3. 不将本项目或部分项目转包。

特此承诺。

投标供应商名称（并加盖公章）：_____

法定代表人或授权代理人（签字或盖章）：_____

日期：_____

7. 技术、商务响应表（包）

说明：供应商必须仔细阅读谈判文件中用户需求书技术、商务条款，逐条应答并按要求填写下表，响应文件有正、负偏离均应在下表中列明。若无偏离，请标明“=”表示完全响应。供应商必须根据所投产品的实际情况（技术资料）如实填写，如发现有虚假描述的，该响应文件无效，并报采购人主管部门严肃处理。

序号	竞争性谈判文件条款描述	供应商响应描述	偏离情况说明 (+/-/=)	备注
1				
2				
3				
4				

供应商名称（盖章）：_____

供应商授权代表（签字）：_____

日期：____年____月____日

注：1、此表为表样，行数可自行添加，但表式不变。

2、供应商根据系统方案添加的设备、材料等也请列出（如有）。

3、是否偏离用符号“+、=、-”分别表示正偏离、完全响应、负偏离，必须逐次对应。

8. 采购代理服务费承诺书

承诺书

致：海南天行招投标有限公司

我们在贵公司组织的海南省公安厅厅机关 2021 年度信息系统运行维护项目（第二次）（项目编号：HNTXGP2021-095R） 包，竞争性谈判采购中若获成交，我们保证在收到付款通知书后按谈判文件的规定，以公司账户转账方式，向贵公司一次性支付应该缴纳的采购代理服务费用。

特此承诺！

供应商代表签字：_____

供应商（全称并加盖公章）：_____

日期：_____

9. 中小企业声明函

中小企业声明函（服务）

本公司（联合体）郑重声明，根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）的规定，本公司（联合体）参加（单位名称）的（项目名称）采购活动，服务全部由符合政策要求的中小企业承接。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

1.（标的名称），属于（采购文件中明确的所属行业）；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于（中型企业、小型企业、微型企业）；

2.（标的名称），属于（采购文件中明确的所属行业）；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于（中型企业、小型企业、微型企业）；

.....

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日期：

从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报。

10. 供应商认为需要提供的用于参与评审其他材料

第六章 用户需求书

一、项目基本情况

1、项目编号：HNTXGP2021-095R

2、项目名称：海南省公安厅厅机关 2021 年度信息系统运行维护项目（第二次）

3、采购方式：竞争性谈判

4、预算金额：210 万元

5、最高限价：210 万元

6、采购需求：项目分四个包

A 包：厅机关信息系统等保测评（1），预算金额 50 万元；

B 包：厅机关信息系统等保测评（2），预算金额 50 万元；

C 包：厅机关信息系统等保测评（3），预算金额 50 万元；

D 包：厅机关信息系统网络安全整改服务，预算金额 60 万。

超出采购预算金额（最高限价）的报价，按无效报价处理。

7、合同履行期限（服务期）：合同履行期限（服务期）：**A、B、C 包：**合同签订后 120 日历天完成（其中等保三级系统在 2021 年 12 月 30 日之前完成信息系统安全保护等级测试评估-等级测评工作，并出具《网络安全等级保护等级测评报告》和《安全建设整改设计方案》）；**D 包：**合同签订后的 1 年。

二、 A 包：用户需求书及要求

(一) 项目服务范围

委托获得公安部认证资质的测评机构，本项目总共对 65 个业务系统进行信息系统安全保护状况进行分等级测试评估——等级测评，并按照要求对测评业务系统出具《网络安全等级保护等级测评报告》和《安全建设整改设计方案》。

A 包等保三级系统 15 个，二级 7 个；合同签订后 120 日历天完成（其中等保三级系统在 2021 年 12 月 30 日之前完成信息系统安全保护等级测试评估——等级测评工作，并出具《网络安全等级保护等级测评报告》和《安全建设整改设计方案》）

(二) 项目服务内容

序号	服务名称	服务期限	服务内容	服务范围
1	网络安全等级保护定级备案指导服务	投标人自合同生效之日起 10 日内	协助招标人对所有信息系统的安全等级确定，并指导编制各系统的《定级报告》及《备案表》。	等保三级系统 15 个，二级 7 个
2	网络安全等级保护测评服务	合同签订后 120 日历天完成（其中等保三级系统在 2021 年 12 月 30 日之前完成信息系统安全保护等级测试评估——等级测评工作，并出具《网络安全等级保护等级测评报告》和《安全建设整改设计方案》）	依据《网络安全等级保护基本要求 2.0》等有关管理规范和技术标准，对等级保护对象的安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等十个层面的安全测评；完成测评工作后，根据招标人的要求出具《网络安全等级保护等级测评报告》，并提出整改建议。针对本次测评，测评结果未通过信息系统，成交供应商协助有关部门对信息系统进行整改指导，提供免费复测，出具《网络安全等级保护等级测评报告》和《安全建设整改设计方案》。	等保三级系统 15 个，二级 7 个

3	安全建设整改方案设计服务	合同签订后120日历天完成（其中等保三级系统在2021年12月30日之前完成信息系统安全保护等级测试评估-等级测评工作，并出具《网络安全等级保护等级测评报告》和《安全建设整改设计方案》）	在完成网络安全等级保护等级测评后，根据本项目相关网络安全等级保护等级测评报告，针对等级测评过程发现的问题，将依据网络安全等级保护政策法规和标准规范，以及《关于开展信息安全等级保护安全建设整改工作的指导意见》（公信安[2009]1429号）的规定，并结合本项目招标人单位的实际情况，出具《安全建设整改设计方案》。		等保三级系统15个，二级7个	
4	售后服务	网络安全培训服务	2	年	自项目验收之日起2年内，对上述信息系统归属的采购单位各部门提供每年不少于1次的培训服务。	海南省公安厅
5		网络安全咨询服务	2	年	自项目验收之日起，提供2年期的网络安全等级保护咨询服务。	海南省公安厅

（三）项目服务要求

3.1 网络安全等级保护定级备案指导服务

投标人自合同生效之日起10日内，根据《信息安全等级保护备案实施细则》（公信安[2007]1360号），根据工作需求，协助采购人编制《定级报告》及《备案表》，并将《定级报告》及《备案表》提交至对应公安部门，通过备案审核并领取《备案证明》。

3.2 网络安全等级保护测评服务

投标人自合同生效且收到招标人开工令之日两个月内，完成网络安全等级

保护测评服务。投标人对本项目 A 包的等保三级系统 15 个，二级 7 个，信息系统完成等级保护对象要素进行确认、分析和梳理，提出详细的等级测评方案。对等级保护对象的整体保护状况和等级保护组件，逐一进行网络安全等级保护等级测评，等级测评的内容包括以下内容：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理十个层面的测评；完成测评工作后，出具《网络安全等级保护等级测评报告》，针对等级保护对象安全建设提出整改建议。

3.2.1 测评实施过程

投标人在测评过程中，按照《信息安全技术 网络安全等级保护测评过程指南》等标准开展测评实施工作，等级测评过程分为四个基本测评活动：测评准备活动、方案编制活动、现场测评活动、报告编制活动。测评双方之间的沟通与洽谈应贯穿整个等级测评过程。测评双方之间的沟通与洽谈应贯穿整个等保测评过程。

3.2.2 测评准备活动

测评准备活动的目标是顺利启动测评项目，收集定级对象相关资料，准备测评所需资料，为编制测评方案打下良好的基础。

测评准备工作应包括工作启动、信息收集和分析、工具和表单准备。

详细要求见下表：

项目内容	工作内容	成果输出
项目启动	1. 组建测评项目组	向测评委托单位提交《项目计划书》、《提供资料清单》
	2. 编制《项目计划书》	
	3. 确定测评委托单位应提供的资料	
信息收集分析	1. 整理调查表单	《等级保护对象调查表》

	2. 发放调查表单给测评委托单位	
	3. 协助测评委托单位填写调查表	
	4. 收回调查结果	
	5. 分析调查结查	
工具和表单准备	1. 调试测评工具	确定测评工具（测评工具清单）
	2. 模拟被测定级对象架构，熟悉被测定级对象	《现场测评授权书》打印各类表单：风险告知书、文档交接单、会议记录表单、会议签到表单
	3. 准备和打印各类表单	

3.2.3 方案编制活动

方案编制活动的目标是整理测评准备活动中获取的定级对象相关资料，为现场测评活动提供最基本的文档和指导方案。

方案编制活动应包括测评对象确定、测评指标确定、测评内容确定、工具测试方法确定、测评指导书开发及测评方案编制等六项主要任务。

详细要求见下表：

工作内容	工作详细任务	输出成果
一、测评对象确认	分析并确定被测定级对象 识别并描述被测定级对象的整体结构 识别并描述被测定级对象的边界 识别并描述被测定级对象的网络区域 识别并描述被测定级对象的主要设备 确定测评对象 描述测评对象	《测评方案》的测评对象部分
二、测评指标确定	确定被测定级对象业务信息和系统服务安全保护等级	《测评方案》的测评指标部分
	根据被测定级对象的 A 类、S 类及 G 类基本安全要求的组合情况，从 GB/T22239、行业规范中选择相应等级的基本安全要求作为基本测评指标	
	根据测评委托单位及被测定级对象业务自身需求，确定特殊测评指标。	
	根据测评委托单位及被测定级对象业务自身需求，确定特殊测评指标。	
	对确定基本测评指标和特殊测评指标进行描述，并分析给出指标不适用的原因	
三、测评内容确定	确定每个测评对象对应的每个测评指标的测评方法	《测评方案》的单项测评实施部分
	确定实施测评的单项测评内容	

四、工具测试点确定	确定工具测试环境 确定工具测试工具 确定工具测试的测评对象 选择测试路径 确定测试工具的接入点 本次项目测评需要使用到如下工具： 漏洞扫描工具； Windows 主机安全配置检查工具； Linux 主机配置检查工具； 网络及安全设备配置检查工具； 病毒检查工具； 木马检查工具； 网站恶意代码检查工具； 在线检查工具(网站安全检查工具)； 终端安全检查工具； 口令破解工具； 渗透测试工具； SQL 注入验证检查工具； 在线数据库安全检查工具。	《测评方案》的工具测试方法及内容部分
五、测评指导书编写	确定单个测评对象，内容包含测评对象的名称、位置信息、用途、管理人员等信息 确定单项测评实施活动，包括测评项、测评方法、操作步骤和预期结果等四部分 确定单项测评、整体测评表述形式 根据测评指导书，形成测评结果记录表格	测评指导书、测评结果记录表格
六、测评方案编制	明确项目整体情况和测评活动依据 根据测评协议书和被测定级对象情况，估算现场测评工作量 根据测评项目组成员安排，编制工作安排情况 根据以往测评经验以及被测定级对象规模，编制具体测评计划，包括现场工作人员的分工和时间安排 汇总上述内容及方案编制活动的其他任务获取的内容形成测评方案文稿 评审和提交测评方案 根据测评方案制定风险规避实施方案	向测评委托单位提交经过评审和确认的《测评方案》、《风险规避实施方案》

3.2.4 现场测评活动

现场测评活动通过与测评委托单位进行沟通和协调，为现场测评的顺利开展打下良好基础，依据测评方案实施现场测评工作，将测评方案和测评方法等内容具体落实到现场测评活动中。现场测评工作主要取得报告编制活动所需的、足

够的证据和资料。

现场测评活动应包括现场测评准备、现场测评和结果记录、结果确认和资料归还三项主要任务。

详细要求见下表：

工作内容	工作详细任务	输出
1. 现场测评准备	测评委托单位对风险告知书签字确认	会议记录，风险告知书，测评方案和现场测评工作计划，现场测评授权书
	测评委托单位协助测评机构签署现场测评授权书	
	召开现场测评首次会	
	双方确认测评计划和测评方案	
2. 现场测评和结果记录	双方确认配合人员、测评环境等各种现场测评需要的资源	《各类测评结果记录/测评证据和证据源记录/文档交接/规划记录单》 访谈结果：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理安全测评的测评结果记录或录音； 文档审查结果：安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理测评的测评结果记录；
	确认测评对象的关键数据已经进行了备份	
	确认具备测评工作开展的条件，测评对象工作正常，系统处于一个相对良好的状况	
	根据测评指导书实施现场测评，获取相关证据和信息	
3. 结果确认和资料归还	测评结束后，双方确认测评工作是否对测评对象造成不良影响，测评对象及系统是否工作正常	配置核查结果：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心测评结果记录表格 工具测试结果：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管
	汇总测评记录，对漏掉和需要进一步验证的内容实施补充测评	
	召开现场测评结束会，测评双方对测评过程中得到的证据源记录进行确认	

	<p>测评人员归还借阅的所有文档资料,并由测评委托单位文档资料提供者签字确认</p>	<p>实地察看结果:安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理测评结果记录</p> <p>测评结果确认:现场核查中发现的问题汇总、测评证据和证据源记录、测评委托单位的书面认可文件</p>
--	--	---

3.2.5 报告编制内容

在现场测评工作结束后,应对现场测评获得的测评结果(或称测评证据)进行汇总分析,形成等级测评结论,并编制测评报告。

测评人员在初步判定单项测评结果后,还需进行单元测评结果判定、整体测评、系统安全保障评估,经过整体测评后,有的单项测评结果可能会有所变化,需进一步修订单项测评结果,而后针对安全问题进行风险评估,形成等级测评结论。报告编制活动应包括单项测评结果判定、单元测评结果判定、整体测评、系统安全保障评估、安全问题风险分析、等级测评结论形成及测评报告编制七项主要任务。

详细要求见下表:

工作内容	工作详细任务	工作依据(模版)
1. 单项测评结果判定	分析测评项所对抗威胁的存在情况	测评报告的等级测评结果记录部分
	分析单项测评项的测评证据,并与要求内容的预期测评结果相比较,给出单项测评结果和符合程度得分	
	综合判定单项测评项的测评结果	
2. 单元测评结果判定	汇总不同测评对象对应测评指标的单项测评结果情况	测评报告的单元测评小结部分
	判定每个测评对象的单元测评结果	
3. 整体测评	分析不符合和部分符合的测评项与其他测评项(包括安全控制点、安全控制点间、区域间)之间的关联关系及对结果的影响情况	测评报告的整体测评部分
	根据整体测评分析情况,修正单项测评结果符合程度得分和问题严重程度值	

4. 系统安全保障评估	根据整体测评结果, 计算修正后的每个测评对象的单项测评结果和符合程度得分	测评报告的系统安全保障评估部分
	根据各对象的单项符合程度得分, 计算安全控制点得分	
	根据安全控制点得分, 计算安全层面得分	
	根据安全控制点得分和安全层面得分, 总体评价被测定级对象已采取的有效保护措施和存在的主要安全问题情况	
5. 安全问题风险分析	针对整体测评后的单项测评结果中部分符合项或不符合项所产生的安全问题, 结合关联测评对象和威胁, 分析可能对定级对象、单位、社会及国家造成的安全危害	测评报告的安全问题风险分析部分
	结合安全问题所影响业务的重要程度、相关系统组件的重要程度、安全问题严重程度以及安全事件影响范围等综合分析可能造成的安全危害中的最大安全危害(损失)结果	
	根据最大安全危害严重程度进一步确定定级对象面临的风险等级, 结果为“高”“中”或“低”	
6. 等级测评结论形成	统计再次汇总后的单项测评结果为部分符合和不符合项的项数	等级测评报告的等级测评结论部分
	计算定级对象综合得分, 形成等级测评结论, 形成等级测评结论	
7. 测评报告编制	概述测评项目情况, 整理前面几项任务的输出/产品	经过评审和确认的被测定级对象等级测评报告
	针对被测定级对象存在的安全隐患, 提出处置建议	
	根据测评协议书、测评委托单位提交的相关文档、测评原始记录和其他辅助信息, 对测评报告进行评审	
	评审通过后, 由项目负责人签字确认并提交给测评委托单位	

3.2.6 测评实施文档

测评机构在上述各阶段活动的测评实施服务过程中, 根据服务规范和测评委托单位要求, 提供系统、完整、清晰的服务日常报告。

提供的服务文档应至少但不限于如下文档:

测评准备阶段:

《项目计划书》;

《等级保护对象调查表》；

《会议记录表》；

方案编制阶段：

《网络安全等级保护测评方案》；

《测评指导书》；

《风险规避实施方案》；

现场测评阶段：

《现场测评授权书》；

《文档交接单》；

《会议记录》；

报告编制阶段：

按系统分别提交《网络安全等级保护等级测评报告》，并针对该信息系统提出安全整改建议。

3.3 安全建设整改方案设计服务

自提交《网络安全等级保护等级测评报告》之日起 30 个工作日内，投标人在完成网络安全等级保护等级测评后，根据本项目相关网络安全等级保护等级测评报告，针对等级测评过程发现的问题，将依据网络安全等级保护政策法规和标准规范，以及《关于开展信息安全等级保护安全建设整改工作的指导意见》（公信安[2009]1429 号）的规定，并结合本项目招标人单位的实际情况，出具《安全建设整改设计方案》。

3.4 网络安全培训服务

自项目验收之日起 2 年内，对本项目范围内的信息系统归属的采购单位各部门提供不少于 1 次的现场培训服务。

培训包含但不限于以下内容：网络安全政策法规培训，解读网络安全法等

相关政策法规的背景、法律条目、深刻含义和应对措施等；有针对性地对关键信息基础设施管理和运维部门技术人员进行相关培训；网络安全意识培训，通过介绍典型的网络安全事件，分析网络安全的重要性；等级保护基础知识培训，介绍等级保护相关法律、法规、标准，以及等级保护工作流程、注意事项和典型案例。

3.5 网络安全咨询服务

3.5.1 网络安全政策/标准咨询

随着国家网络安全等级保护的工作推进，网络安全等级保护政策、法律法规和标准体系也会相应的发布和更新，投标人应针对本项目设立网络安全等级保护咨询平台，自合同验收之日起，提供 2 年咨询服务，咨询内容包括但不限于网络安全等级保护国内外发展动态、等级保护政策、法律法规和标准体系咨询服务。

3.5.2 等级保护对象等级变更咨询

目前海南省公安厅的信息系统部分完成信息系统的定级备案工作。随着信息系统的不断建设和发展，可能会出现信息系统等级变更情况。在信息系统出现等级变更时，投标人需协助海南省公安厅对信息系统进行识别，明确信息系统边界和定级对象，对信息系统的子系统进行划分，确定信息系统以及子系统的安全等级。

定级阶段，投标人需根据等保相关主管部门和国家工信部的要求和指南，协助海南省公安厅完成定级对象确认、系统定级和定级备案工作。

3.5.3 等级保护自查咨询

按照等级保护相关政策要求，信息系统运营使用单位应定期对信息系统进行自查活动，在自查活动期间，投标人应提供海南省公安厅相应的咨询服务。

（四）、项目的实施要求

项目实施过程中，投标方应遵循国家标准、行业标准。

4.1 项目实施要求

1. 在项目实施中投标方必须做到：
2. 提供项目实施组织架构；
3. 提供详细的项目实施方案和计划进度说明书；
4. 投标人应定期向招标人汇报项目的实施进度，包括但不限于项目经理在项目期间每周至少来招标人现场 1 次进行工作汇报，且电话要保持 7*24 小时通畅；
5. 为保障项目服务响应速度，投标人承诺项目实施期间及售后服务期内，提供本地化技术支持服务，对于招标人的电话咨询和常规服务请求在 30 分钟内予以答复，紧急服务请求在 2 小时内到达招标人现场；
6. 严格按照双方确定的计划进度保质保量完成工作；
7. 规范项目实施过程中的文档管理；
8. 项目实施中要引入风险管理、质量管理、成本管理；
9. 实施人员必须签署《保密协议》，按照《保密协议》的要求开展相关工作。

4.2 实施团队要求

本项目实施团队成员名单及职责分工明确，项目期间在项目本地部署不少于 8 人的技术团队，项目经理必须具有 3 年以上的等保测评服务项目管理经验，且每周到项目现场不少于一天；其中，本项目实施成员中，至少有 2 人具备等级保护高级测评师资格和有 5 人具备等级保护中级测评师资格，且属于投标人在册员工(以社保缴纳证明为认定依据)，实施测评工作的技术人员必须具备公安部信息安全等级保护评估中心颁发的《信息安全等级测评师证书》或中关村信息安全测评联盟颁发的《网络安全等级测评师证书》（以下统一简称为“测评师证书”），且在项目现场随身佩戴《测评师证书》备查。实施团队名单中所列人员的社保缴纳证明和《测评师证书》复印件需在投标文件中提供，并加盖公章。

4.3 项目验收

投标方必须书面通知招标方所完成的工作和准备进行验收的项目种类及验收开始时间，此通知书需经招标方认定后方可执行。

4.4 验收组织

成立由招标方、中标方以及其他有关人员组成的验收小组，负责对项目进行全面的验收。

4.5 验收标准

1. 完成了本项目内所有的服务工作；
2. 提交本项目内所有服务工作的服务成果；
3. 提交项目实施阶段所有的过程文档；

4.6 项目工期

第一阶段：投标人自合同生效之日起 30 日内完成网络安全等级保护定级备案指导服务，协助招标人取得备案证明；

第二阶段：投标人自合同生效且收到招标人开工令之日起 60 日内，完成网络安全等级保护测评服务并提交服务成果；

第三阶段：投标人自提交《网络安全等级保护等级测评报告》之日起 30 日内，出具《安全建设整改设计方案》。

三、B包：用户需求书及要求

(一) 项目服务范围

委托获得公安部认证资质的测评机构，本项目总共对 65 个业务系统进行信息安全系统安全保护状况进行分等级测试评估——等级测评，并按照要求对测评业务系统出具《网络安全等级保护等级测评报告》和《安全建设整改设计方案》。

B包等保三级系统 15 个，二级 6 个；合同签订后 120 日历天完成（其中等保三级系统在 2021 年 12 月 30 日之前完成信息安全系统安全保护等级测试评估——等级测评工作，并出具《网络安全等级保护等级测评报告》和《安全建设整改设计方案》）

(二) 项目服务内容

序号	服务名称	服务期限	服务内容	服务范围
1	网络安全等级保护定级备案指导服务	投标人自合同生效之日起 10 日内	协助招标人对所有信息系统的安全等级确定，并指导编制各系统的《定级报告》及《备案表》。	B包等保三级系统 15 个，二级 6 个
2	网络安全等级保护测评服务	合同签订后 120 日历天完成（其中等保三级系统在 2021 年 12 月 30 日之前完成信息安全系统安全保护等级测试评估——等级测评工作，并出具《网络安全等级保护等级测评报告》和《安全建设整改设计方案》）	依据《网络安全等级保护基本要求 2.0》等有关管理规范和技术标准，对等级保护对象的安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等十个层面的安全测评；完成测评工作后，根据招标人的要求出具《网络安全等级保护等级测评报告》，并提出整改建议。针对本次测评，测评结果未通过信息系统，成交供应商协助有关部门对信息系统进行整改指导，提供免费复测，出具《网络安全等级保护等级测评报告》和《安全建设整改设计方案》。	B包等保三级系统 15 个，二级 6 个

3	安全建设整改方案设计服务	合同签订后120日历天完成（其中等保三级系统在2021年12月30日之前完成信息系统安全保护等级测试评估-等级测评工作，并出具《网络安全等级保护等级测评报告》和《安全建设整改设计方案》）	在完成网络安全等级保护等级测评后，根据本项目相关网络安全等级保护等级测评报告，针对等级测评过程发现的问题，将依据网络安全等级保护政策法规和标准规范，以及《关于开展信息安全等级保护安全建设整改工作的指导意见》（公信安[2009]1429号）的规定，并结合本项目招标人单位的实际情况，出具《安全建设整改设计方案》。		B包等保三级系统15个，二级6个	
4	售后服务	网络安全培训服务	2	年	自项目验收之日起2年内，对上述信息系统归属的采购单位各部门提供每年不少于1次的培训服务。	海南省公安厅
5		网络安全咨询服务	2	年	自项目验收之日起，提供2年期的网络安全等级保护咨询服务。	海南省公安厅

（三）项目服务要求

3.1 网络安全等级保护定级备案指导服务

投标人自合同生效之日起10日内，根据《信息安全等级保护备案实施细则》（公信安[2007]1360号），根据工作需求，协助采购人编制《定级报告》及《备案表》，并将《定级报告》及《备案表》提交至对应公安部门，通过备案审核并领取《备案证明》。

3.2 网络安全等级保护测评服务

投标人自合同生效且收到招标人开工令之日两个月内，完成网络安全等级

保护测评服务。投标人对本项目 A 包的等保三级系统 15 个，二级 6 个，信息系统完成等级保护对象要素进行确认、分析和梳理，提出详细的等级测评方案。对等级保护对象的整体保护状况和等级保护组件，逐一进行网络安全等级保护等级测评，等级测评的内容包括以下内容：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理十个层面的测评；完成测评工作后，出具《网络安全等级保护等级测评报告》，针对等级保护对象安全建设提出整改建议。

3.2.1 测评实施过程

投标人在测评过程中，按照《信息安全技术 网络安全等级保护测评过程指南》等标准开展测评实施工作，等级测评过程分为四个基本测评活动：测评准备活动、方案编制活动、现场测评活动、报告编制活动。测评双方之间的沟通与洽谈应贯穿整个等级测评过程。测评双方之间的沟通与洽谈应贯穿整个等保测评过程。

3.2.2 测评准备活动

测评准备活动的目标是顺利启动测评项目，收集定级对象相关资料，准备测评所需资料，为编制测评方案打下良好的基础。

测评准备工作应包括工作启动、信息收集和分析、工具和表单准备。

详细要求见下表：

项目内容	工作内容	成果输出
项目启动	1. 组建测评项目组	向测评委托单位提交《项目计划书》、《提供资料清单》
	2. 编制《项目计划书》	
	3. 确定测评委托单位应提供的资料	
信息收集分析	1. 整理调查表单	《等级保护对象调查表》

	2. 发放调查表单给测评委托单位	
	3. 协助测评委托单位填写调查表	
	4. 收回调查结果	
	5. 分析调查结查	
工具和表单准备	1. 调试测评工具	确定测评工具（测评工具清单） 《现场测评授权书》打印各类 表单：风险告知书、文档交接单、 会议记录表单、会议签到表单
	2. 模拟被测定级对象架构，熟悉被测定级对象	
	3. 准备和打印各类表单	

3.2.3 方案编制活动

方案编制活动的目标是整理测评准备活动中获取的定级对象相关资料，为现场测评活动提供最基本的文档和指导方案。

方案编制活动应包括测评对象确定、测评指标确定、测评内容确定、工具测试方法确定、测评指导书开发及测评方案编制等六项主要任务。

详细要求见下表：

工作内容	工作详细任务	输出成果
一、测评对象确认	分析并确定被测定级对象 识别并描述被测定级对象的整体结构 识别并描述被测定级对象的边界 识别并描述被测定级对象的网络区域 识别并描述被测定级对象的主要设备 确定测评对象 描述测评对象	《测评方案》的测评对象部分
二、测评指标确定	确定被测定级对象业务信息和系统服务安全保护等级	《测评方案》的测评指标部分
	根据被测定级对象的 A 类、S 类及 G 类基本安全要求的组合情况，从 GB/T22239、行业规范中选择相应等级的基本安全要求作为基本测评指标	
	根据测评委托单位及被测定级对象业务自身需求，确定特殊测评指标。	
	根据测评委托单位及被测定级对象业务自身需求，确定特殊测评指标。	
	对确定基本测评指标和特殊测评指标进行描述，并分析给出指标不适用的原因	
三、测评内容确定	确定每个测评对象对应的每个测评指标的测评方法	《测评方案》的单项测评实施部分
	确定实施测评的单项测评内容	

四、工具测试点确定	<p>确定工具测试环境 确定工具测试工具 确定工具测试的测评对象 选择测试路径 确定测试工具的接入点 本次项目测评需要使用到如下工具： 漏洞扫描工具； Windows 主机安全配置检查工具； Linux 主机配置检查工具； 网络及安全设备配置检查工具； 病毒检查工具； 木马检查工具； 网站恶意代码检查工具； 在线检查工具(网站安全检查工具)； 终端安全检查工具； 口令破解工具； 渗透测试工具； SQL 注入验证检查工具； 在线数据库安全检查工具。</p>	《测评方案》的工具测试方法及内容部分
五、测评指导书编写	<p>确定单个测评对象，内容包含测评对象的名称、位置信息、用途、管理人员等信息 确定单项测评实施活动,包括测评项、测评方法、操作步骤和预期结果等四部分 确定单项测评、整体测评表述形式 根据测评指导书,形成测评结果记录表格</p>	测评指导书、测评结果记录表格
六、测评方案编制	<p>明确项目整体情况和测评活动依据 根据测评协议书和被测定级对象情况,估算现场测评工作量 根据测评项目组成员安排,编制工作安排情况 根据以往测评经验以及被测定级对象规模,编制具体测评计划,包括现场工作人员的分工和时间安排 汇总上述内容及方案编制活动的其他任务获取的内容形成测评方案文稿 评审和提交测评方案 根据测评方案制定风险规避实施方案</p>	向测评委托单位提交经过评审和确认的《测评方案》、《风险规避实施方案》

3.2.4 现场测评活动

现场测评活动通过与测评委托单位进行沟通和协调,为现场测评的顺利开展打下良好基础,依据测评方案实施现场测评工作,将测评方案和测评方法等内容具体落实到现场测评活动中。现场测评工作主要取得报告编制活动所需的、足

够的证据和资料。

现场测评活动应包括现场测评准备、现场测评和结果记录、结果确认和资料归还三项主要任务。

详细要求见下表：

工作内容	工作详细任务	输出
1. 现场测评准备	测评委托单位对风险告知书签字确认	会议记录，风险告知书，测评方案和现场测评工作计划，现场测评授权书
	测评委托单位协助测评机构签署现场测评授权书	
	召开现场测评首次会	
	双方确认测评计划和测评方案	
2. 现场测评和结果记录	双方确认配合人员、测评环境等各种现场测评需要的资源	《各类测评结果记录/测评证据和证据源记录/文档交接/规划记录单》 访谈结果：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理安全测评的测评结果记录或录音； 文档审查结果：安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理测评的测评结果记录；
	确认测评对象的关键数据已经进行了备份	
	确认具备测评工作开展的条件，测评对象工作正常，系统处于一个相对良好的状况	
	根据测评指导书实施现场测评，获取相关证据和信息	
3. 结果确认和资料归还	测评结束后，双方确认测评工作是否对测评对象造成不良影响，测评对象及系统是否工作正常	配置核查结果：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心测评结果记录表格 工具测试结果：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管
	汇总测评记录，对漏掉和需要进一步验证的内容实施补充测评	
	召开现场测评结束会，测评双方对测评过程中得到的证据源记录进行确认	

	<p>测评人员归还借阅的所有文档资料,并由测评委托单位文档资料提供者签字确认</p>	<p>实地察看结果:安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理测评结果记录</p> <p>测评结果确认:现场核查中发现的问题汇总、测评证据和证据源记录、测评委托单位的书面认可文件</p>
--	--	---

3.2.5 报告编制内容

在现场测评工作结束后,应对现场测评获得的测评结果(或称测评证据)进行汇总分析,形成等级测评结论,并编制测评报告。

测评人员在初步判定单项测评结果后,还需进行单元测评结果判定、整体测评、系统安全保障评估,经过整体测评后,有的单项测评结果可能会有所变化,需进一步修订单项测评结果,而后针对安全问题进行风险评估,形成等级测评结论。报告编制活动应包括单项测评结果判定、单元测评结果判定、整体测评、系统安全保障评估、安全问题风险分析、等级测评结论形成及测评报告编制七项主要任务。

详细要求见下表:

工作内容	工作详细任务	工作依据(模版)
1. 单项测评结果判定	分析测评项所对抗威胁的存在情况	测评报告的等级测评结果记录部分
	分析单项测评项的测评证据,并与要求内容的预期测评结果相比较,给出单项测评结果和符合程度得分	
	综合判定单项测评项的测评结果	
2. 单元测评结果判定	汇总不同测评对象对应测评指标的单项测评结果情况	测评报告的单元测评小结部分
	判定每个测评对象的单元测评结果	
3. 整体测评	分析不符合和部分符合的测评项与其他测评项(包括安全控制点、安全控制点间、区域间)之间的关联关系及对结果的影响情况	测评报告的整体测评部分
	根据整体测评分析情况,修正单项测评结果符合程度得分和问题严重程度值	

4. 系统安全保障评估	根据整体测评结果, 计算修正后的每个测评对象的单项测评结果和符合程度得分	测评报告的系统安全保障评估部分
	根据各对象的单项符合程度得分, 计算安全控制点得分	
	根据安全控制点得分, 计算安全层面得分	
	根据安全控制点得分和安全层面得分, 总体评价被测定级对象已采取的有效保护措施和存在的主要安全问题情况	
5. 安全问题风险分析	针对整体测评后的单项测评结果中部分符合项或不符合项所产生的安全问题, 结合关联测评对象和威胁, 分析可能对定级对象、单位、社会及国家造成的安全危害	测评报告的安全问题风险分析部分
	结合安全问题所影响业务的重要程度、相关系统组件的重要程度、安全问题严重程度以及安全事件影响范围等综合分析可能造成的安全危害中的最大安全危害(损失)结果	
	根据最大安全危害严重程度进一步确定定级对象面临的风险等级, 结果为“高”“中”或“低”	
6. 等级测评结论形成	统计再次汇总后的单项测评结果为部分符合和不符合项的项数	等级测评报告的等级测评结论部分
	计算定级对象综合得分, 形成等级测评结论, 形成等级测评结论	
7. 测评报告编制	概述测评项目情况, 整理前面几项任务的输出/产品	经过评审和确认的被测定级对象等级测评报告
	针对被测定级对象存在的安全隐患, 提出处置建议	
	根据测评协议书、测评委托单位提交的相关文档、测评原始记录和其他辅助信息, 对测评报告进行评审	
	评审通过后, 由项目负责人签字确认并提交给测评委托单位	

3.2.6 测评实施文档

测评机构在上述各阶段活动的测评实施服务过程中, 根据服务规范和测评委托单位要求, 提供系统、完整、清晰的服务日常报告。

提供的服务文档应至少但不限于如下文档:

测评准备阶段:

《项目计划书》;

《等级保护对象调查表》；

《会议记录表》；

方案编制阶段：

《网络安全等级保护测评方案》；

《测评指导书》；

《风险规避实施方案》；

现场测评阶段：

《现场测评授权书》；

《文档交接单》；

《会议记录》；

报告编制阶段：

按系统分别提交《网络安全等级保护等级测评报告》，并针对该信息系统提出安全整改建议。

3.3 安全建设整改方案设计服务

自提交《网络安全等级保护等级测评报告》之日起 30 个工作日内，投标人在完成网络安全等级保护等级测评后，根据本项目相关网络安全等级保护等级测评报告，针对等级测评过程发现的问题，将依据网络安全等级保护政策法规和标准规范，以及《关于开展信息安全等级保护安全建设整改工作的指导意见》（公信安[2009]1429 号）的规定，并结合本项目招标人单位的实际情况，出具《安全建设整改设计方案》。

3.4 网络安全培训服务

自项目验收之日起 2 年内，对本项目范围内的信息系统归属的采购单位各部门提供不少于 1 次的现场培训服务。

培训包含但不限于以下内容：网络安全政策法规培训，解读网络安全法等

相关政策法规的背景、法律条目、深刻含义和应对措施等；有针对性地对关键信息基础设施管理和运维部门技术人员进行相关培训；网络安全意识培训，通过介绍典型的网络安全事件，分析网络安全的重要性；等级保护基础知识培训，介绍等级保护相关法律、法规、标准，以及等级保护工作流程、注意事项和典型案例。

3.5 网络安全咨询服务

3.5.1 网络安全政策/标准咨询

随着国家网络安全等级保护的工作推进，网络安全等级保护政策、法律法规和标准体系也会相应的发布和更新，投标人应针对本项目设立网络安全等级保护咨询平台，自合同验收之日起，提供 2 年咨询服务，咨询内容包括但不限于网络安全等级保护国内外发展动态、等级保护政策、法律法规和标准体系咨询服务。

3.5.2 等级保护对象等级变更咨询

目前海南省公安厅的信息系统部分完成信息系统的定级备案工作。随着信息系统的不断建设和发展，可能会出现信息系统等级变更情况。在信息系统出现等级变更时，投标人需协助海南省公安厅对信息系统进行识别，明确信息系统边界和定级对象，对信息系统的子系统进行划分，确定信息系统以及子系统的安全等级。

定级阶段，投标人需根据等保相关主管部门和国家工信部的要求和指南，协助海南省公安厅完成定级对象确认、系统定级和定级备案工作。

3.5.3 等级保护自查咨询

按照等级保护相关政策要求，信息系统运营使用单位应定期对信息系统进行自查活动，在自查活动期间，投标人应提供海南省公安厅相应的咨询服务。

(四)、项目的实施要求

项目实施过程中，投标方应遵循国家标准、行业标准。

4.1 项目实施要求

1. 在项目实施中投标方必须做到：
2. 提供项目实施组织架构；
3. 提供详细的项目实施方案和计划进度说明书；
4. 投标人应定期向招标人汇报项目的实施进度，包括但不限于项目经理在项目期间每周至少来招标人现场 1 次进行工作汇报，且电话要保持 7*24 小时通畅；
5. 为保障项目服务响应速度，投标人承诺项目实施期间及售后服务期内，提供本地化技术支持服务，对于招标人的电话咨询和常规服务请求在 30 分钟内予以答复，紧急服务请求在 2 小时内到达招标人现场；
6. 严格按照双方确定的计划进度保质保量完成工作；
7. 规范项目实施过程中的文档管理；
8. 项目实施中要引入风险管理、质量管理、成本管理；
9. 实施人员必须签署《保密协议》，按照《保密协议》的要求开展相关工作。

4.2 实施团队要求

本项目实施团队成员名单及职责分工明确，项目期间在项目本地部署不少于 8 人的技术团队，项目经理必须具有 3 年以上的等保测评服务项目管理经验，且每周到项目现场不少于一天；其中，本项目实施成员中，至少有 2 人具备等级保护高级测评师资格和有 5 人具备等级保护中级测评师资格，且属于投标人在册员工(以社保缴纳证明为认定依据)，实施测评工作的技术人员必须具备公安部信息安全等级保护评估中心颁发的《信息安全等级测评师证书》或中关村信息安全测评联盟颁发的《网络安全等级测评师证书》（以下统一简称为“测评师证书”），且在项目现场随身佩戴《测评师证书》备查。实施团队名单中所列人员的社保缴纳证明和《测评师证书》复印件需在投标文件中提供，并加盖公章。

4.3 项目验收

投标方必须书面通知招标方所完成的工作和准备进行验收的项目种类及验收开始时间，此通知书需经招标方认定后方可执行。

4.4 验收组织

成立由招标方、中标方以及其他有关人员组成的验收小组，负责对项目进行全面的验收。

4.5 验收标准

1. 完成了本项目内所有的服务工作；
2. 提交本项目内所有服务工作的服务成果；
3. 提交项目实施阶段所有的过程文档；

4.6 项目工期

第一阶段：投标人自合同生效之日起 30 日内完成网络安全等级保护定级备案指导服务，协助招标人取得备案证明；

第二阶段：投标人自合同生效且收到招标人开工令之日起 60 日内，完成网络安全等级保护测评服务并提交服务成果；

第三阶段：投标人自提交《网络安全等级保护等级测评报告》之日起 30 日内，出具《安全建设整改设计方案》。

四、C包：用户需求书及要求

（一）项目服务范围

委托获得公安部认证资质的测评机构，本项目总共对 65 个业务系统进行信息系统安全保护状况进行分等级测试评估—等级测评，并按照要求对测评业务系统出具《网络安全等级保护等级测评报告》和《安全建设整改设计方案》。

C包等保三级系统 15 个，二级 7 个；合同签订后 120 日历天完成（其中等保三级系统在 2021 年 12 月 30 日之前完成信息系统安全保护等级测试评估—等级测评工作，并出具《网络安全等级保护等级测评报告》和《安全建设整改设计方案》）

（二）项目服务内容

序号	服务名称	服务期限	服务内容	服务范围
1	网络安全等级保护定级备案指导服务	投标人自合同生效之日起 10 日内	协助招标人对所有信息系统的安全等级确定，并指导编制各系统的《定级报告》及《备案表》。	B包等保三级系统 15 个，二级 7 个
2	网络安全等级保护测评服务	合同签订后 120 日历天完成（其中等保三级系统在 2021 年 12 月 30 日之前完成信息系统安全保护等级测试评估—等级测评工作，并出具《网络安全等级保护等级测评报告》和《安全建设整改设计方案》）	依据《网络安全等级保护基本要求 2.0》等有关管理规范和技术标准，对等级保护对象的安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等十个层面的安全测评；完成测评工作后，根据招标人的要求出具《网络安全等级保护等级测评报告》，并提出整改建议。针对本次测评，测评结果未通过信息系统，成交供应商协助有关部门对信息系统进行整改指导，提供免费复测，出具《网络安全等级保护等级测评报告》和《安全建设整改设计方案》。	B包等保三级系统 15 个，二级 7 个

3	安全建设整改方案设计服务	合同签订后120日历天完成（其中等保三级系统在2021年12月30日之前完成信息系统安全保护等级测试评估-等级测评工作，并出具《网络安全等级保护等级测评报告》和《安全建设整改设计方案》）	在完成网络安全等级保护等级测评后，根据本项目相关网络安全等级保护等级测评报告，针对等级测评过程发现的问题，将依据网络安全等级保护政策法规和标准规范，以及《关于开展信息安全等级保护安全建设整改工作的指导意见》（公信安[2009]1429号）的规定，并结合本项目招标人单位的实际情况，出具《安全建设整改设计方案》。		B包等保三级系统15个，二级7个	
4	售后服务	网络安全培训服务	2	年	自项目验收之日起2年内，对上述信息系统归属的采购单位各部门提供每年不少于1次的培训服务。	海南省公安厅
5		网络安全咨询服务	2	年	自项目验收之日起，提供2年期的网络安全等级保护咨询服务。	海南省公安厅

（三）项目服务要求

3.1 网络安全等级保护定级备案指导服务

投标人自合同生效之日起10日内，根据《信息安全等级保护备案实施细则》（公信安[2007]1360号），根据工作需求，协助采购人编制《定级报告》及《备案表》，并将《定级报告》及《备案表》提交至对应公安部门，通过备案审核并领取《备案证明》。

3.2 网络安全等级保护测评服务

投标人自合同生效且收到招标人开工令之日两个月内，完成网络安全等级

保护测评服务。投标人对本项目 A 包的等保三级系统 15 个，二级 7 个，信息系统完成等级保护对象要素进行确认、分析和梳理，提出详细的等级测评方案。对等级保护对象的整体保护状况和等级保护组件，逐一进行网络安全等级保护等级测评，等级测评的内容包括以下内容：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理十个层面的测评；完成测评工作后，出具《网络安全等级保护等级测评报告》，针对等级保护对象安全建设提出整改建议。

3.2.1 测评实施过程

投标人在测评过程中，按照《信息安全技术 网络安全等级保护测评过程指南》等标准开展测评实施工作，等级测评过程分为四个基本测评活动：测评准备活动、方案编制活动、现场测评活动、报告编制活动。测评双方之间的沟通与洽谈应贯穿整个等级测评过程。测评双方之间的沟通与洽谈应贯穿整个等保测评过程。

3.2.2 测评准备活动

测评准备活动的目标是顺利启动测评项目，收集定级对象相关资料，准备测评所需资料，为编制测评方案打下良好的基础。

测评准备工作应包括工作启动、信息收集和分析、工具和表单准备。

详细要求见下表：

项目内容	工作内容	成果输出
项目启动	1. 组建测评项目组	向测评委托单位提交《项目计划书》、《提供资料清单》
	2. 编制《项目计划书》	
	3. 确定测评委托单位应提供的资料	
信息收集分析	1. 整理调查表单	《等级保护对象调查表》

	2. 发放调查表单给测评委托单位	
	3. 协助测评委托单位填写调查表	
	4. 收回调查结果	
	5. 分析调查结查	
工具和表单准备	1. 调试测评工具	确定测评工具（测评工具清单）
	2. 模拟被测定级对象架构，熟悉被测定级对象	《现场测评授权书》打印各类表单：风险告知书、文档交接单、会议记录表单、会议签到表单
	3. 准备和打印各类表单	

3.2.3 方案编制活动

方案编制活动的目标是整理测评准备活动中获取的定级对象相关资料，为现场测评活动提供最基本的文档和指导方案。

方案编制活动应包括测评对象确定、测评指标确定、测评内容确定、工具测试方法确定、测评指导书开发及测评方案编制等六项主要任务。

详细要求见下表：

工作内容	工作详细任务	输出成果
一、测评对象确认	分析并确定被测定级对象 识别并描述被测定级对象的整体结构 识别并描述被测定级对象的边界 识别并描述被测定级对象的网络区域 识别并描述被测定级对象的主要设备 确定测评对象 描述测评对象	《测评方案》的测评对象部分
二、测评指标确定	确定被测定级对象业务信息和系统服务安全保护等级	《测评方案》的测评指标部分
	根据被测定级对象的 A 类、S 类及 G 类基本安全要求的组合情况，从 GB/T22239、行业规范中选择相应等级的基本安全要求作为基本测评指标	
	根据测评委托单位及被测定级对象业务自身需求，确定特殊测评指标。	
	根据测评委托单位及被测定级对象业务自身需求，确定特殊测评指标。	
	对确定基本测评指标和特殊测评指标进行描述，并分析给出指标不适用的原因	
三、测评内容确定	确定每个测评对象对应的每个测评指标的测评方法	《测评方案》的单项测评实施部分
	确定实施测评的单项测评内容	

四、工具测试点确定	<p>确定工具测试环境 确定工具测试工具 确定工具测试的测评对象 选择测试路径 确定测试工具的接入点 本次项目测评需要使用到如下工具： 漏洞扫描工具； Windows 主机安全配置检查工具； Linux 主机配置检查工具； 网络及安全设备配置检查工具； 病毒检查工具； 木马检查工具； 网站恶意代码检查工具； 在线检查工具(网站安全检查工具)； 终端安全检查工具； 口令破解工具； 渗透测试工具； SQL 注入验证检查工具； 在线数据库安全检查工具。</p>	《测评方案》的工具测试方法及内容部分
五、测评指导书编写	<p>确定单个测评对象，内容包含测评对象的名称、位置信息、用途、管理人员等信息 确定单项测评实施活动,包括测评项、测评方法、操作步骤和预期结果等四部分 确定单项测评、整体测评表述形式 根据测评指导书,形成测评结果记录表格</p>	测评指导书、测评结果记录表格
六、测评方案编制	<p>明确项目整体情况和测评活动依据 根据测评协议书和被测定级对象情况,估算现场测评工作量 根据测评项目组成员安排,编制工作安排情况 根据以往测评经验以及被测定级对象规模,编制具体测评计划,包括现场工作人员的分工和时间安排 汇总上述内容及方案编制活动的其他任务获取的内容形成测评方案文稿 评审和提交测评方案 根据测评方案制定风险规避实施方案</p>	向测评委托单位提交经过评审和确认的《测评方案》、《风险规避实施方案》

3.2.4 现场测评活动

现场测评活动通过与测评委托单位进行沟通和协调,为现场测评的顺利开展打下良好基础,依据测评方案实施现场测评工作,将测评方案和测评方法等内容具体落实到现场测评活动中。现场测评工作主要取得报告编制活动所需的、足

够的证据和资料。

现场测评活动应包括现场测评准备、现场测评和结果记录、结果确认和资料归还三项主要任务。

详细要求见下表：

工作内容	工作详细任务	输出
1. 现场测评准备	测评委托单位对风险告知书签字确认	会议记录，风险告知书，测评方案和现场测评工作计划，现场测评授权书
	测评委托单位协助测评机构签署现场测评授权书	
	召开现场测评首次会	
	双方确认测评计划和测评方案	
2. 现场测评和结果记录	双方确认配合人员、测评环境等各种现场测评需要的资源	《各类测评结果记录/测评证据和证据源记录/文档交接/规划记录单》 访谈结果：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理安全测评的测评结果记录或录音； 文档审查结果：安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理测评的测评结果记录；
	确认测评对象的关键数据已经进行了备份	
	确认具备测评工作开展的条件，测评对象工作正常，系统处于一个相对良好的状况	
	根据测评指导书实施现场测评，获取相关证据和信息	
3. 结果确认和资料归还	测评结束后，双方确认测评工作是否对测评对象造成不良影响，测评对象及系统是否工作正常	配置核查结果：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心测评结果记录表格 工具测试结果：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管
	汇总测评记录，对漏掉和需要进一步验证的内容实施补充测评	
	召开现场测评结束会，测评双方对测评过程中得到的证据源记录进行确认	

	<p>测评人员归还借阅的所有文档资料,并由测评委托单位文档资料提供者签字确认</p>	<p>实地察看结果:安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理测评结果记录</p> <p>测评结果确认:现场核查中发现的问题汇总、测评证据和证据源记录、测评委托单位的书面认可文件</p>
--	--	---

3.2.5 报告编制内容

在现场测评工作结束后,应对现场测评获得的测评结果(或称测评证据)进行汇总分析,形成等级测评结论,并编制测评报告。

测评人员在初步判定单项测评结果后,还需进行单元测评结果判定、整体测评、系统安全保障评估,经过整体测评后,有的单项测评结果可能会有所变化,需进一步修订单项测评结果,而后针对安全问题进行风险评估,形成等级测评结论。报告编制活动应包括单项测评结果判定、单元测评结果判定、整体测评、系统安全保障评估、安全问题风险分析、等级测评结论形成及测评报告编制七项主要任务。

详细要求见下表:

工作内容	工作详细任务	工作依据(模版)
1. 单项测评结果判定	分析测评项所对抗威胁的存在情况	测评报告的等级测评结果记录部分
	分析单项测评项的测评证据,并与要求内容的预期测评结果相比较,给出单项测评结果和符合程度得分	
	综合判定单项测评项的测评结果	
2. 单元测评结果判定	汇总不同测评对象对应测评指标的单项测评结果情况	测评报告的单元测评小结部分
	判定每个测评对象的单元测评结果	
3. 整体测评	分析不符合和部分符合的测评项与其他测评项(包括安全控制点、安全控制点间、区域间)之间的关联关系及对结果的影响情况	测评报告的整体测评部分
	根据整体测评分析情况,修正单项测评结果符合程度得分和问题严重程度值	

4. 系统安全保障评估	根据整体测评结果, 计算修正后的每个测评对象的单项测评结果和符合程度得分	测评报告的系统安全保障评估部分
	根据各对象的单项符合程度得分, 计算安全控制点得分	
	根据安全控制点得分, 计算安全层面得分	
	根据安全控制点得分和安全层面得分, 总体评价被测定级对象已采取的有效保护措施和存在的主要安全问题情况	
5. 安全问题风险分析	针对整体测评后的单项测评结果中部分符合项或不符合项所产生的安全问题, 结合关联测评对象和威胁, 分析可能对定级对象、单位、社会及国家造成的安全危害	测评报告的安全问题风险分析部分
	结合安全问题所影响业务的重要程度、相关系统组件的重要程度、安全问题严重程度以及安全事件影响范围等综合分析可能造成的安全危害中的最大安全危害(损失)结果	
	根据最大安全危害严重程度进一步确定定级对象面临的风险等级, 结果为“高”“中”或“低”	
6. 等级测评结论形成	统计再次汇总后的单项测评结果为部分符合和不符合项的项数	等级测评报告的等级测评结论部分
	计算定级对象综合得分, 形成等级测评结论, 形成等级测评结论	
7. 测评报告编制	概述测评项目情况, 整理前面几项任务的输出/产品	经过评审和确认的被测定级对象等级测评报告
	针对被测定级对象存在的安全隐患, 提出处置建议	
	根据测评协议书、测评委托单位提交的相关文档、测评原始记录和其他辅助信息, 对测评报告进行评审	
	评审通过后, 由项目负责人签字确认并提交给测评委托单位	

3.2.6 测评实施文档

测评机构在上述各阶段活动的测评实施服务过程中, 根据服务规范和测评委托单位要求, 提供系统、完整、清晰的服务日常报告。

提供的服务文档应至少但不限于如下文档:

测评准备阶段:

《项目计划书》;

《等级保护对象调查表》；

《会议记录表》；

方案编制阶段：

《网络安全等级保护测评方案》；

《测评指导书》；

《风险规避实施方案》；

现场测评阶段：

《现场测评授权书》；

《文档交接单》；

《会议记录》；

报告编制阶段：

按系统分别提交《网络安全等级保护等级测评报告》，并针对该信息系统提出安全整改建议。

3.3 安全建设整改方案设计服务

自提交《网络安全等级保护等级测评报告》之日起 30 个工作日内，投标人在完成网络安全等级保护等级测评后，根据本项目相关网络安全等级保护等级测评报告，针对等级测评过程发现的问题，将依据网络安全等级保护政策法规和标准规范，以及《关于开展信息安全等级保护安全建设整改工作的指导意见》（公信安[2009]1429 号）的规定，并结合本项目招标人单位的实际情况，出具《安全建设整改设计方案》。

3.4 网络安全培训服务

自项目验收之日起 2 年内，对本项目范围内的信息系统归属的采购单位各部门提供不少于 1 次的现场培训服务。

培训包含但不限于以下内容：网络安全政策法规培训，解读网络安全法等

相关政策法规的背景、法律条目、深刻含义和应对措施等；有针对性地对关键信息基础设施管理和运维部门技术人员进行相关培训；网络安全意识培训，通过介绍典型的网络安全事件，分析网络安全的重要性；等级保护基础知识培训，介绍等级保护相关法律、法规、标准，以及等级保护工作流程、注意事项和典型案例。

3.5 网络安全咨询服务

3.5.1 网络安全政策/标准咨询

随着国家网络安全等级保护的工作推进，网络安全等级保护政策、法律法规和标准体系也会相应的发布和更新，投标人应针对本项目设立网络安全等级保护咨询平台，自合同验收之日起，提供 2 年咨询服务，咨询内容包括但不限于网络安全等级保护国内外发展动态、等级保护政策、法律法规和标准体系咨询服务。

3.5.2 等级保护对象等级变更咨询

目前海南省公安厅的信息系统部分完成信息系统的定级备案工作。随着信息系统的不断建设和发展，可能会出现信息系统等级变更情况。在信息系统出现等级变更时，投标人需协助海南省公安厅对信息系统进行识别，明确信息系统边界和定级对象，对信息系统的子系统进行划分，确定信息系统以及子系统的安全等级。

定级阶段，投标人需根据等保相关主管部门和国家工信部的要求和指南，协助海南省公安厅完成定级对象确认、系统定级和定级备案工作。

3.5.3 等级保护自查咨询

按照等级保护相关政策要求，信息系统运营使用单位应定期对信息系统进行自查活动，在自查活动期间，投标人应提供海南省公安厅相应的咨询服务。

（四）、项目的实施要求

项目实施过程中，投标方应遵循国家标准、行业标准。

4.1 项目实施要求

1. 在项目实施中投标方必须做到：
2. 提供项目实施组织架构；
3. 提供详细的项目实施方案和计划进度说明书；
4. 投标人应定期向招标人汇报项目的实施进度，包括但不限于项目经理在项目期间每周至少来招标人现场 1 次进行工作汇报，且电话要保持 7*24 小时通畅；
5. 为保障项目服务响应速度，投标人承诺项目实施期间及售后服务期内，提供本地化技术支持服务，对于招标人的电话咨询和常规服务请求在 30 分钟内予以答复，紧急服务请求在 2 小时内到达招标人现场；
6. 严格按照双方确定的计划进度保质保量完成工作；
7. 规范项目实施过程中的文档管理；
8. 项目实施中要引入风险管理、质量管理、成本管理；
9. 实施人员必须签署《保密协议》，按照《保密协议》的要求开展相关工作。

4.2 实施团队要求

本项目实施团队成员名单及职责分工明确，项目期间在项目本地部署不少于 8 人的技术团队，项目经理必须具有 3 年以上的等保测评服务项目管理经验，且每周到项目现场不少于一天；其中，本项目实施成员中，至少有 2 人具备等级保护高级测评师资格和有 5 人具备等级保护中级测评师资格，且属于投标人在册员工(以社保缴纳证明为认定依据)，实施测评工作的技术人员必须具备公安部信息安全等级保护评估中心颁发的《信息安全等级测评师证书》或中关村信息安全测评联盟颁发的《网络安全等级测评师证书》（以下统一简称为“测评师证书”），且在项目现场随身佩戴《测评师证书》备查。实施团队名单中所列人员的社保缴纳证明和《测评师证书》复印件需在投标文件中提供，并加盖公章。

4.3 项目验收

投标方必须书面通知招标方所完成的工作和准备进行验收的项目种类及验收开始时间，此通知书需经招标方认定后方可执行。

4.4 验收组织

成立由招标方、中标方以及其他有关人员组成的验收小组，负责对项目进行全面的验收。

4.5 验收标准

1. 完成了本项目内所有的服务工作；
2. 提交本项目内所有服务工作的服务成果；
3. 提交项目实施阶段所有的过程文档；

4.6 项目工期

第一阶段：投标人自合同生效之日起 30 日内完成网络安全等级保护定级备案指导服务，协助招标人取得备案证明；

第二阶段：投标人自合同生效且收到招标人开工令之日起 60 日内，完成网络安全等级保护测评服务并提交服务成果；

第三阶段：投标人自提交《网络安全等级保护等级测评报告》之日起 30 日内，出具《安全建设整改设计方案》。

五、D包：用户需求书及要求

（一）项目概述

依据等保 2.0 标准及相关规范，对招标人的信息系统进行安全运维服务，通过内网威胁分析服务和安全漏洞扫描评估服务及时发现网络和系统中存在的漏洞、风险和隐患，对网络中的威胁和入侵行为等进行分析和告警；

通过优化、加固网络策略配置服务、边界安全防护服务和运维安全管控服务对网络和系统中的薄弱环节进行安全加固，提升招标人信息系统的网络安全防护能力。

通过网络安全应急响应服务提高招标人网络安全事件响应和处置能力，减少网络安全事件造成的损失和影响。

通过网络安全等级保护安全管理制度完善服务补充和完善招标人网络安全管理制度，加强制度的落实和执行。

(二) 项目服务内容

序号	服务名称	数量	单位	服务内容	服务范围
1	优化、加固网络策略配置服务	1	次	<p>1、结合等保 2.0 标准，对网络架构进行优化；</p> <p>2、结合等保 2.0 标准，提出详细可落地执行的加固优化策略配置调整意见。与设备厂商、维保商沟通，确保调整后的安全策略不影响业务，现场配合设备厂商、维保商实施；</p> <p>3、必要情况下，可直接操作，调整策略配置；</p> <p>4、对实施后的结果进行技术验证。尽可能满足等保的基本要求。</p>	2021 年开展等保测评的信息系统
2	边界安全防护服务	1	年	<p>1. 针对业务系统资产及其安全措施进行调研和梳理；</p> <p>2. 识别并评估业务系统的安全风险及脆弱性，结合等保 2.0 标准，提供技术手段（如硬件工具、软件工具、人工服务等）对特定的网络安全边界进行访问控制、入侵防范、恶意代码防范和 Web 应用安全防护等，保护信息系统免受攻击、入侵和破坏，尽可能满足等保的基本要求。</p> <p>4. 按月输出《边界安全防护报告》。</p>	公安网应用支撑平台域与核心交换机的边界、服务器域与核心交换机的边界
3	内网威胁分析服务	1	年	<p>依据等保标准及相关规范，对公安网核心交换机流量进行检测和分析，对省厅公安网内的入侵、攻击等行为进行监测，提供省厅公安网骨干部分的防火墙和 Web 应用防火墙等设备日志的集中收集、存储和分析服务，尽可能满足等保的基本要求。形成《内网威胁分析报告》和安全通报（内网威胁分析部分）。</p>	省厅公安网骨干部分
4	安全漏洞扫描评估服务	12	次	<p>1、依据等保标准及相关规范，采用多种安全专用评估工具对等级保护对象进行全面深度漏洞探测，及时掌握等级保护对象安全状况，为改善并提高等级保护对象安全性提供依据；并提供详细的安全评估报告和安全通报（漏洞扫描部分），包括扫描的漏洞详细信息、安全加固建议等，对所有漏洞弱点的相关背景提供详细描述、引用，以及相应的修复和改进建议，尽可能满足等保的基本要求。</p>	厅机关公安信息网的网络设备、安全设备、服务器和信息系统等对象（含二级网络设备）

				2、安全通报：每月根据发现的问题，编制一份安全通报，并督促相关单位组织整改。同时通报上期安全整改的督察情况。	
5	运维安全管控服务	1	年	依据等保标准及相关规范，对防火墙和堡垒机进行安全策略设置，规范和限制运维人员的网络接入和访问权限，检查和监督运维人员安装一机两用等安全软件，对运维室的运维环境提供 360 度的视频监控服务，监控记录保存不少于半年，尽可能满足等保的基本要求。	指定运维室，支撑平台域和服务器域涉及的网络设备、安全设备、服务器和信息系统等
6	网络安全应急响应服务	1	年	在等级保护对象安全事件发生时，对安全事件发生的等级保护对象进行安全事故分析，并协助及时解决安全故障、修复系统，最大限度的保护服务器和数据，最快的速度恢复访问和网络畅通，使等级保护对象恢复正常工作，尽可能挽回或减少损失。	海南省公安厅公安信息网出现的网络安全事件
7	网络安全等级保护安全管理制度完善服务	1	次	1. 依据《网络安全等级保护基本要求》中的“安全管理”类安全要求优化现有体系化文件； 2. 包含策略方针、制度、操作手册、记录文档四个层级文件； 3. 指导招标人完善制度，落实制度，建立制度体系，尽可能满足等保的基本要求。	海南省公安厅

2.1 优化、加固网络策略配置服务

2.1.1 服务概述

投标人自合同生效之日起一年内，采取人工咨询指导等形式，依据等保 2.0 标准要求，对各设备供应商、运维服务商等提出详细的合规要求，解答并指导相关技术人员进行网络架构优化、网络及安全设备安全策略配置加固等，并对实施后的结果进行技术验证，尽可能满足等保的基本要求。

主要服务内容如下：

一、网络安全加固指导

调整网络拓扑结构，以提高网络系统的安全性；

划分安全域，并依据相应安全域的安全要求，配置各安全域边界管理设备的安全策略，使得各安全域之间可靠安全隔离；

启用网络设备安全审计，以追踪网络设备运行状况、设备维护、配置修改等各类事件。

二、主机安全加固指导

修改操作系统安全策略，以提高主机操作系统安全性；

启用操作系统安全审计，以追踪操作系统运行状况、登录事件等各类安全事件；

修改数据库安全策略，以提高数据库系统安全性；

启用数据库安全审计，以追踪数据库登录事件、修改事件等各类安全事件。

三、应用安全加固指导

结合应用系统相关业务流程的实际情况，并在不影响系统稳定运行的前提下，指导优化业务应用安全策略，以提高应用系统的安全性；

指导优化及完善应用系统安全审计，以追踪应用系统的登录事件、修改事件等各类安全事件。

序号	服务内容	服务说明	服务对象	主要成果文档	服务频率	服务类型
1	优化、加固网络策略配置服务	1、结合等保 2.0 标准，对网络架构进行优化； 2、结合等保 2.0 标准，提出详细可落地执行的加固优化策略配置调整意见。与设备厂商、维保商沟通，确保调整后的安全策略不影响业务，现场配合设备厂商、维保商实施； 3、必要情况下，可直接操作，调整策略配置； 4、对实施后的结果进行技术验证，尽可能满足等保的基本要求。	2021 年开展等保测评的信息系统	《网络安全加固指导报告》	一年内 1 次	现场服务

2.1.2 服务成果

通过对等级保护对象进行网络安全加固、主机安全加固及应用安全加固指导，以提高等级保护对象的整体技术防护能力，输出《网络安全加固指导报告》。

2.2 边界安全防护服务

2.2.1 服务概述

边界安全防护服务是通过技术手段对特定的网络安全边界进行访问控制、入侵防范、恶意代码防范和 Web 应用安全防护等，保护信息系统免受攻击、入侵和破坏。分析业务访问需求，根据业务访问需求配置安全策略，对入侵行为和恶意代码进行防御，尽可能满足等保的基本要求。

投标人自合同生效之日起一年内，为招标人提供边界安全防护服务，涉及的边界为海南省公安厅公安网应用支撑平台域与核心交换机的边界、服务器域与核心交换机的边界。具体服务要求为：1、公安网应用支撑平台域与核心交换机的边界提供 2 台下一代防火墙和 2 台 Web 应用防火墙作为服务工具，实现访问控制、入侵防范和恶意代码防范，以及 Web 应用系统的安全防护；2、服务器域与核心交换机的边界提供 2 台 Web 应用防火墙作为服务工具，实现 Web 应用系统的安全防护。服务工具应能与现网互联设备的接口兼容，满足性能要求。

序号	服务内容	服务说明	服务对象	主要成果文档	服务频率	服务类型
----	------	------	------	--------	------	------

1	边界安全防护服务	<p>1. 针对业务系统资产及其安全措施进行调研和梳理；</p> <p>2. 识别并评估业务系统的安全风险及脆弱性；</p> <p>3. 通过技术手段对特定的网络安全边界进行访问控制、入侵防范、恶意代码防范和 Web 应用安全防护等，保护信息系统免受攻击、入侵和破坏，尽可能满足等保的基本要求。</p> <p>4. 按月输出《边界安全防护报告》。</p>	<p>公安网应用支撑平台域与核心交换机的边界、服务器域与核心交换机的边界</p>	<p>《边界安全防护报告》（每月一份）</p>	<p>一年</p>	<p>远程服务 现场服务</p>
---	----------	---	--	-------------------------	-----------	----------------------

2.2.2 服务成果

边界安全防护服务的服务成果为《边界安全防护报告》（每月一份）。

2.3 内网威胁分析服务

2.3.1 服务概述

投标人自合同生效之日起一年内，依据等保标准及相关规范，为招标人提供内网威胁分析服务，借助人力和工具对公安网核心交换机流量进行检测和分析，对省厅公安网内的入侵、攻击等行为进行监测，提供省厅公安网骨干部分的防火墙和 Web 应用防火墙等设备日志的集中收集、存储和分析服务，结合流量检测分析、攻击行为和病毒监测，以及安全日志分析等进行公安网内网威胁分析，识别各类安全威胁和入侵行为，形成内网威胁分析报告，尽可能满足等保的基本要求。

服务过程中，投标人需提供流量监测和攻击诱捕技术措施，提供 1 台入侵监测系统和

1 台攻击诱捕设备（含 10 个虚拟 IP）作为服务工具，服务工具应能与现网互联设备的接口兼容，满足性能要求；需提供 1 套日志收集与分析软件（含 20 个日志源）作为服务工具，部署在招标人提供的虚拟机上，进行日志收集分析。需每周到招标人现场开展服务，进行日志查看和分析等工作。

序号	服务内容	服务说明	服务对象	主要成果文档	服务频率	服务类型
1	内网威胁分析服务	依据等保标准及相关规范，对公安网核心交换机流量进行检测和分析，对省厅公安网内的入侵、攻击等行为进行监测，提供省厅公安网骨干部分的防火墙和 Web 应用防火墙等设备日志的集中收集、存储和分析服务，尽可能满足等保的基本要求，形成《内网威胁分析报告》。	省厅公安网骨干部分	《内网威胁分析报告》、《安全通报（内网威胁分析部分）》	一年	现场服务

2.3.2 服务成果

服务成果：每月提交《内网威胁分析报告》、《安全通报（内网威胁分析部分）》各一份，其中，《安全通报（内网威胁分析部分）》和安全漏洞扫描评估服务提交的《安全通报（漏洞扫描部分）》形成一份完整的《安全通报》，每月向相关单位进行通报，并督促和跟进整改情况。

2.4 安全漏洞扫描评估服务

2.4.1 服务概述

投标人自合同生效之日起，为招标人提供一年内 12 次的安全漏洞扫描评估服务，将以等级保护测评标准为基线，利用多种专业漏洞扫描工具对网络、操作系统、数据库、WEB 系统等进行交叉扫描验证，并利用专业安全服务人员经验对扫描结果进行分析，帮助海南省公安厅及时掌握等级保护对象安全状况，发现存在的主要问题和薄弱环节，并对发现的安全隐患提供改善建议，协助指导海南省公安厅堵塞安全漏洞，协助指导海南省公安厅落实和完善安全措施。

通过漏洞安全评估服务，分析海南省公安厅网络和信息系统存在的各种安

全漏洞及问题；帮助海南省公安厅充分了解各个等级保护对象及服务器存在的安全隐患，建立安全可靠的 WEB 应用服务，改善并提升应用系统抗各类 WEB 应用攻击的能力(如：注入攻击、跨站脚本、钓鱼攻击、信息泄漏、恶意编码、表单绕过、缓冲区溢出等)，具体内容详见下表：

序号	服务内容	服务说明	服务对象	主要成果文档	服务频率	服务类型
1	安全漏洞扫描评估服务	<p>1、依据等保标准及相关规范，采用多种安全专用评估工具对等级保护对象进行全面深度漏洞探测，及时掌握等级保护对象安全状况，为改善并提高等级保护对象安全性提供依据；并提供详细的安全评估报告，包括扫描的漏洞详细信息、安全加固建议等，对所有漏洞弱点的相关背景提供详细描述、引用，以及相应的修复和改进建议。</p> <p>2、安全通报：每月根据发现的问题，编制一份安全通报，并督促相关单位组织整改。同时通报上期安全整改的督察情况。</p>	厅机关公安信息网的网络设备、安全设备、服务器和信息系统等对象	《安全漏洞扫描评估报告》、《安全通报（漏洞扫描部分）》	一年 12 次	现场服务

2.4.2 服务成果

通过漏洞安全评估，并在安全可控的前提下对可验证的漏洞进行验证，对数据进行分析，每月输出《安全漏洞扫描评估报告》和《安全通报（漏洞扫描部分）》，为漏洞修复提供技术指导。

2.5 运维安全管控服务

2.5.1 服务概述

投标人自合同生效之日起，依据等保标准及相关规范，为招标人提供一年的运维安全管控服务，针对海南省公安厅指定运维室进行安全管控，对防火墙和堡垒机进行安全策略设置，限制每个运维人员的运维电脑只能通过堡垒机进行设备和系统运维，并且运维人员只能使用运维室接入交换机的特定端口和网线，不能随意接入网络。检查和督促运维人员

在接入公安网的运维电脑安装一机两用、安管平台、杀毒软件和安全助手等安全管理软件。对运维室的运维环境提供 360 度的视频监控服务，确保监控记录保存不少于半年。至少每周提供一次现场服务。

序号	服务内容	服务说明	服务对象	主要成果文档	服务频率	服务类型
1	运维安全管控服务	依据等保标准及相关规范，对防火墙和堡垒机进行安全策略设置，规范和限制运维人员的网络接入和访问权限，检查和监督运维人员安装一机两用等安全软件，对运维室的运维环境提供 360 度的视频监控服务，监控记录保存不少于半年。	指定运维室，支撑平台域和服务器域涉及的网络设备、安全设备、服务器和信息系统等	《运维安全管控报告》	一年	现场服务

2.5.2 服务成果

服务成果为《运维安全管控报告》（每月一份）。

2.6 网络安全应急响应服务

2.6.1 服务概述

投标人自合同生效之日起，为招标人提供一年的网络安全应急响应服务，根据等级保护《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）的“安全事件处置”的要求，当等级保护对象安全事件发生时，为海南省公安厅提供网络安全事件应急响应服务，通过应急响应对安全事件发生的等级保护对象进行安全事故分析，以及时解决安全故障、修复系统，最大限度的保护服务器和数据，最快的速度恢复访问和网络畅通，使等级保护对象恢复正常工作，尽可能挽回或减少损失。

投标人需在招标人本地组建专业的应急响应技术支持团队，在收到招标人应急响应需求后半小时内做出响应，2 小时内到达海南省公安厅现场进行安全事件处置。

网络安全应急响应服务包括但不限于对如下安全事件做出响应：

- 计算机病毒事件

- 蠕虫病毒事件
- 特洛伊木马事件
- 网页内嵌恶意代码事件
- 拒绝服务攻击事件
- 后门攻击事件
- 漏洞攻击事件
- 网络扫描窃听事件
- 信息篡改事件

具体服务内容详见下表：

序号	服务项目	服务说明	服务对象	主要成果文档	服务频率	服务类型
1	网络安全应急响应服务	在等级保护对象安全事件发生时，对安全事件发生的等级保护对象进行安全事故分析，并协助及时解决安全故障、修复系统，最大限度的保护服务器和数据，最快的速度恢复访问和网络畅通，使等级保护对象恢复正常工作，尽可能挽回或减少损失。	海南省公安厅公安信息网出现的网络安全事件	应急响应处理报告（配合部分）	一年不限次数	远程服务现场服务

2.6.2 服务成果

- 针对每次网络安全事件出具《应急响应处理报告》（配合部分）。

2.7 网络安全等级保护安全管理制度完善服务

2.7.1 服务概述

网络安全管理体系是一个系统化、程序化和文件化的管理体系，根据《中华人民共和国网络安全法》第二十一条“国家实行网络安全等级保护制度。网络运营者应当按照网络等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

- （一）制定内部安全管理制度和操作规程，确保网络安全负责人，落实网络安

全保护责任”，将依据我国《管理办法》、《网络安全等级保护基本要求》，参照《信息系统安全管理要求》、《信息系统安全工程管理要求》等标准规范要求，建立健全并落实符合相应等级要求的的安全管理制度。

为了更好的建立完善的的安全管理制度体系，投标人自合同生效之日起，为招标人提供一年 1 次的网络安全等级保护安全管理制度完善服务，依据《网络安全等级保护基本要求》中的“安全管理”类安全要求，并结合国际通用的安全管理体系系列标准，规划安全管理文档体系框架，具体的框架结构如下：



■ 第一级文件【纲领类】

第一级文件为纲领类文件，主要是描述 ISMS（信息安全管理体系-Information security management system）的整体要求、目标和架构的控制性、基础性文件。具体体现为安全管理工作的纲领性文件，指出管理范围、安全目标等。

■ 第二级文件【支持类】

第二级文件为支持类文件，主要描述管理体系各个过程及涉及到的部门活动，明确过程的输入、输出及相互作用；同时也描述各个部门的管理标准，包括信息安全管理体系设计安全域的各项规定。具体体现为规定所要求的管理制度或控制措施等。

■ 第三级文件【规范类】

第三级文件为规范类文件，主要为指南及作业文件，包括编写、操作、管理指南、使用手册和技术规范等，同时工作的标准和技术标准也纳入其中。具体体现为解释特定管理活动的步骤和细节。

■ 第四级文件【记录类】

第四级文件为记录类文件，主要对安全管理各个活动的过程和结果所做的记录。具体体现为记录活动以符合各项管理规定的文件要求的客观证据。

序号	服务内容	服务说明	服务对象	主要成果文档	服务频率	服务类型
1	网络安全等级保护安全管理制度完善服务	1. 依据《网络安全等级保护基本要求》中的“安全管理”类安全要求编制体系化文件； 2. 包含策略方针、制度、操作手册、记录文档四个层级文件； 3. 指导招标人完善制度，落实制度，建立制度体系，尽可能满足等保的基本要求。	海南省公安厅	《网络安全管理制度》	一年1次	远程服务现场服务

2.7.2 服务成果

通过网络安全等级保护管理制度完善服务，输出符合等级保护对象实际管理要求的《网络安全管理制度》。

（三）项目的实施要求

项目实施过程中，投标方应遵循国家标准、行业标准。

3.1 项目实施要求

在项目实施中投标方必须做到：

1. 提供项目实施组织架构；
2. 提供详细的项目实施方案和计划进度说明书；
3. 投标人应定期向招标人汇报项目的实施进度，包括但不限于项目经理在项目期间每周至少来招标人现场 1 次进行工作汇报，且电话要保持 7*24 小时通畅；
4. 为保障项目服务响应速度，投标人承诺提供项目期间本地化技术支持服务，对于招标人的电话咨询和常规服务请求在 30 分钟内予以答复，

紧急服务请求在 2 小时内到达招标人现场；

5. 严格按照双方确定的计划进度保质保量完成工作；
6. 规范项目实施过程中的文档管理；
7. 项目实施中要引入风险管理、质量管理、成本管理；
8. 实施人员必须签署《保密协议》，按照《保密协议》的要求开展相关工作。

3.2 实施团队要求

本项目实施团队成员名单及职责分工明确，项目期间在项目本地部署不少于 10 人的技术团队，项目经理必须具有 2 年以上的安全运维服务项目管理经验，且每周到项目现场不少于一天；其中，本项目实施成员中，至少有 1 人具备高级工程师资格和有 5 人具备中级工程师资格，且属于投标人在册员工(以社保缴纳证明为认定依据)。实施团队名单中所列人员的社保缴纳证明需在投标文件中提供，并加盖公章。

3.3 项目验收

投标方必须书面通知招标方所完成的工作和准备进行验收的项目种类及验收开始时间，此通知书需经招标方认定后方可执行。

3.4 验收组织

成立由招标方、中标方以及其他有关人员组成的验收小组，负责对项目进行全面的验收。

3.5 验收标准

- 完成了本项目内所有的服务工作；
- 提交本项目内所有服务工作的服务成果；

- 提交项目实施阶段所有的过程文档。

（四）项目工期

投标人自合同生效且收到招标人开工令之日起一年内，完成优化、加固网络策略配置服务、边界安全防护服务、内网威胁分析服务、安全漏洞扫描评估服务、运维安全管控服务、网络安全应急响应服务、网络安全等级保护安全管理制度完善服务并提交服务成果。

第七章 评审办法和程序

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、谈判响应文件、谈判承诺文件和最终报价为依据，按公正、科学、客观、平等竞争的要求，推荐技术先进、报价合理、经验丰富、信誉良好、售后服务好及综合实力强的成交供应商。

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。

4、本次采购采用低价优先法，是指以价格为主要因素确定成交候选供应商的评审方法，即在全满足竞争性谈判文件实质性要求前提下，依据统一的价格要素以提出最低报价的供应商作为成交供应商的评审方法。

二、评审程序和评审方法

评审流程如下：

评标准备（谈判响应文件初步评审（符合性审查和资格性审查）（谈判响应文件的比较与评价（从商务、技术两方面进行比较与评价）（专家与通过审查的供应商分别单独进行谈判并做出二次报价（通过审查的供应商按价格由高到低顺序排列，并确定价格最低的供应商为成交供应商）。

1、评标准备

评标委员会成员阅读竞争性谈判文件，了解本次采购的范围和需求，熟悉评标方法；

2、谈判响应文件初步评审

进入评审程序后，谈判小组先对供应商的谈判响应文件进行初步评审。谈判小组将根据评审办法的规定和附表 1 的内容，对谈判响应文件进行初步评审。

若出现以下情况，则谈判响应文件将被认定为不满足采购需求而不能通过初步

审查：

- 1) 谈判响应文件无法定代表人签字，或签字人未经法定代表人授权的；
- 2) 供应商未按谈判文件要求的金额提交谈判保证金的；
- 3) 投标有效期不足的；
- 4) 谈判小组根据谈判文件检查谈判响应文件提供的资格证明材料不齐全、不满足谈判文件的要求，并在谈判小组规定的时间未能补充齐全的；
- 5) 谈判小组根据谈判文件对谈判响应文件的商务和技术部分进行初步审查，检查谈判响应文件提交的内容不齐全、不能证明有能力承担本项目的任务、未按谈判文件的要求作出相应的承诺的；
- 6) 主要技术规格和参数不满足技术参数要求以及商务有重大负偏离的；
- 7) 谈判小组认为报价未实质性响应谈判文件的要求的；
- 8) 没有按时作最终报价或最终报价低于最低限价且采购人无法接受的；
- 9) 违反国家和地方政府采购法律法规的；
- 10) 不满足谈判文件规定的其它条件的。
- 11) 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。

3、谈判

谈判小组只对资格性检查及符合性检查合格的谈判响应文件进行商务及技术评估，综合比较与评价。各供应商做出二次报价。

4、推荐成交供应商

谈判小组根据质量和服务均能满足采购文件实质性响应要求且最后报价最低的原则确定成交供应商。若最终报价相同的，按服务方案、技术人员配备优劣顺序排列。如按服务方案、技术人员配备优劣再无法排列的，就有评审委员会随机抓阄推选中标候选单位的顺序。

三、谈判、评审过程的保密性。

1、接受报价后，直至成交供应商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，任何人均不得向供应商及与谈判评审无关的其他人透露。

2、从谈判响应文件递交截止时间起到确定成交供应商之日止，供应商不得

与参加谈判、评审的有关人员私下接触。在谈判评审过程中，如果供应商试图在谈判响应文件审查、澄清、比较及推荐成交供应商方面向参与谈判评审的有关人员和采购人施加任何影响，其谈判响应文件将被拒绝。

四、接受和拒绝任何或所有报价的权利。

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谈判响应文件的权力，对受影响的供应商不承担任何责任。

附件 1

初步评审表

项目名称：海南省公安厅厅机关 2021 年度信息系统运行维护项目（第二次）

项目编号：HNTXGP2021-095R

序号	审查项目	评议内容 (无效谈判响应文件认定条件)	投标人
1	供应商的资格	是否满足谈判文件供应商资格要求	
2	信用记录查询	是否存在不良信用记录：在“信用中国”网站（ www.creditchina.gov.cn ）没有被列入重大税收违法案件当事人名单、政府采购严重违法失信名单，没有被列入中国执行信息公开网（ http://zxgk.court.gov.cn/shixin/ ）失信被执行人名单和没有被列入“中国政府采购网”（ www.ccgp.gov.cn ）政府采购严重违法失信行为记录名单投标人。以联合体形式参加投标的，联合体任何成员存在以上不良信用记录的，将被认定为响应无效。供应商不良信用记录以采购代理机构于开标当天查询结果为准。	
3	谈判保证金	是否提交足额谈判保证金证明	
4	谈判响应文件递交情况	正本、副本和电子版的提交是否符合谈判文件要求	
5	投标有效期	是否满足谈判文件要求	
6	合同履行期限 (服务期)	是否满足谈判文件要求	
7	其它	无其它无效投标认定条件	
		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”。

保证金退还申请书

致：海南天行招投标有限公司

我司于年月日为 项目（项目编号： ）投标所提交的保证金人民币

¥：元，请贵公司退还时划到以下账户：

开户名称			
开户银行全称		联系人	
银行账户		联系电话	

供应商名称：（公章）

法定代表人或授权代理人：（签字或盖章）

日期：

注：此申请书仅用于退还项目保证金，无须作为响应文件的组成部分装订在响应文件中，请将此保证金退还申请书于开标现场单独递交。