用户需求书

一、项目基本情况

1、项目编号：HNTXGP2021-095

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

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：项目分两个包，其中A包：厅机关信息系统等保测评，预算金额150万【超出采购预算金额（最高限价）的报价，按无效报价处理】，B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

7、合同履行期限（服务期）：A包：合同签订后120日历天完成（其中45个等保三级系统在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》）；B包：合同签订后的1年。本项目不接受联合体投标。

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，对65个业务系统（其中三级45个，二级20个）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》。

（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》。	65个业务系统

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45个等保三级系统在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》。	65个业务系统
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45个等保三级系统在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》。	65个业务系统
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。投标人对招标人的 65 个业务系统（其中三级 45 个，二级 20 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	《测评方案》的测评对象部分

	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	
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	测评指导书、测评结果记录表格
	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	
六、测评方案编制	明确项目整体情况和测评活动依据	向测评委托单位提交经过评审和确认的《测评方案》、
	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	《风险规避实施方案》
	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	

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	
	双方确认配合人员、测评环境等各种现场测评需要的资源	
2.现场测评和结果记录	确认测评对象的关键数据已经进行了备份	《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
	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	
	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	

3.结果确认和资料归还	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	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; 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、安全管理中心测评结果记录，工具测试完成后的电子输出记录，备份的测试结果文件 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 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
	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	
	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	

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	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
2	边界安全防护服务	1	年	1.针对业务系统资产及其安全措施进行调研和梳理； 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。 4.按月输出《边界安全防护报告》。	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	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）。	省厅公安网骨干部分
4	安全漏洞扫描评估服务	12	次	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。 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	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）

				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	1.针对业务系统资产及其安全措施进行调研和梳理； 2.识别并评估业务系统的安全风险及脆弱性； 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。 4.按月输出《边界安全防护报告》。	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	《边界安全防护报告》（每月一份）	一年	远程服务 现场服务

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	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。 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。	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。

投保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

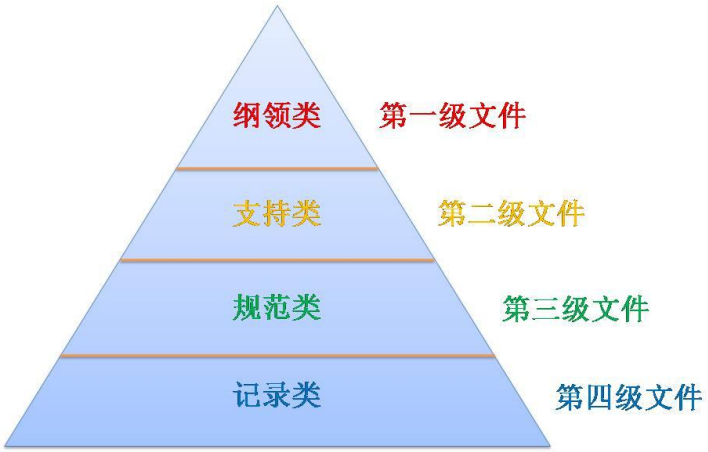
- 针对每次网络安全事件出具《应急响应处理报告》（配合部分）。

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安全管理制度。

为了更好的建立完善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。