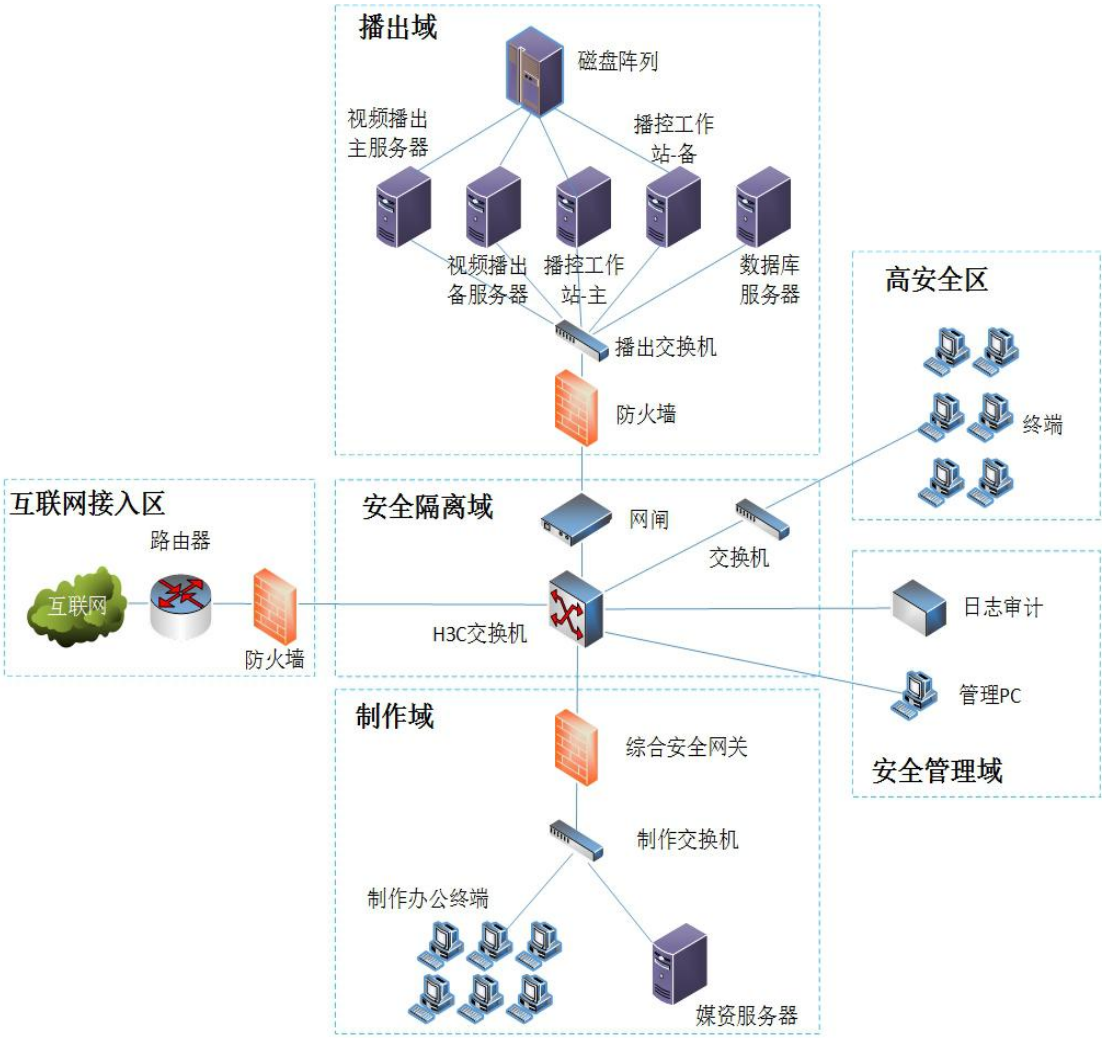
A包 用户需求书

一、现状说明

网络拓扑现状如下：



二、网络安全基础设施建设需求

本项目为网络安全整改和安全服务项目，项目目标为提高县广播电视台相关业务系统的安全防护能力，提升县广播电视台的安全管理能力和风险应对能力。

县广播电视台核心的播控系统为等保第三级的信息系统，因此，本项目需基于最近一次等级保护测评结果和系统现状，参照《网络安全法》和等保第三级的相关要求进行规划和设计。本项目的安全需求分为以下几个方面。

1、安全通信网络

核心交换机配置双机冗余，保证系统的可靠性和容错性。

2、安全区域边界

加强网络边界安全防护，在未部署访问控制设备的边界升级原有的下一代防火墙，配置入侵防御和防病毒功能许可，实现访问控制、入侵防范和恶意代码防范的多重安全防护。

在缺少恶意代码防范措施的网络边界增加恶意代码防范技术措施。

为了及时发现和预警网络环境中的未知威胁，需增加入侵检测系统。

3、安全计算环境

建设统一管理的主机恶意代码防范系统，提高服务器和终端应对恶意代码威胁的能力。

针对数据库系统，增加审计措施和手段。

4、安全管理中心

加强对设备日常维护操作的管控和监测，提供统一的运维管控平台，需增加堡垒机。

三、项目需求清单

序号	产品名称	单位	数量	技术参数及性能配置要求
1	防火墙升级（互联网）	台	1	为互联网接入域的防火墙升级防病毒功能许可，一年升级授权（原防护墙型 V3/TG-22106）
2	防火墙升级（播出域）	台	1	为播出域的防火墙升级防病毒功能许可，一年升级授权（原防护墙型号：V3/TG-22106）
3	核心交换机	台	2	三层以太网交换机，支持≥48 个 10/100/1000BASE-T 端口,支持 4 个 10G/1G BASE-X SFP+端口，包转发率不低于 360Mpps，三年保修
4	接入交换机	台	1	≥48 个 10/100/1000Base-T 接口，4 个千兆 SFP 接口，三年保修

5	堡垒机	台	1	1U，含单交流电源，2*USB 接口，1*RJ45 串口，1*GE 管理口，4*GE 电口，2T SATA 硬盘。图形会话并发 80 个，字符会话并发 180 个。缺省授权管理 25 台设备。包含三年软件更新服务、产品保修服务、远程支持服务。
				要求支持人员半自动登录目标设备，即第一次登录目标设备时运维人员需手工输入目标设备帐号和密码并允许堡垒机保存该帐号密码，之后运维人员就可以自动登录目标设备。请提供截图证明。
				★要求可通过应用发布的方式进行协议扩展，无需定制即可支持其他通用及专有的运维客户端程序。
				★要求支持幽灵账号功能，支持主动对从账号进行关联分析，当发现攻击者植入的异常账号时，对相关管理员采取告警、记录及通知等操作。提供产品功能截图。
				★要求支持孤儿账号功能，能够提供对各从账号的运维使用率的分析功能，当发现使用率异常的从账号，对相关管理员采取告警、记录及通知等操作。提供产品功能截图。
				★支持手机 APP 上进行登录授权审批，金库授权审批，工单审批，方便客户随时随地进行审批工作
				产品须具备公安部颁发的《计算机信息系统安全专用产品销售许可证》（增强级）。提供有效证书复印件。
				产品资质：产品获得中国信息安全测评公司颁发的信息技术产品安全测评证书（EAL3+），提供证书复印件。
6	网络入侵检测系统	台	1	1U 机型，含交流单电源模块，2*USB 接口，1*RJ45 串口，1*RJ45 管理口，6*GE（Bypass）接口，1 个接口扩展槽位。网络吞吐量 8Gbps、HTTP 吞吐

				300Gbps、最大并发连接数 100 万、每秒新建连接数 3 万。包含三年软件更新服务、产品保修服务、远程支持服务。
				系统应提供覆盖广泛的攻击特征库，可针对网络病毒、蠕虫、间谍软件、木马后门、扫描探测、暴力破解等恶意流量进行检测和阻断，攻击特征库数量至少为 8100 种以上。须提供界面截图。
				系统携带的攻击特征库须获得 CVE-Compatible 兼容性认证，CVE 兼容性认证须提供证明文件。
				★系统应提供基于信誉的僵尸网络检测能力，具备可以持续升级的信誉库，IDS 通过信誉库内的恶意网站 IP、C&C 服务器地址的信誉值执行相应的检测动作。须提供信誉库界面截图。
				系统应提供服务器异常告警功能，可以自学习服务器正常工作行为，并以此为基线检测处服务器非法外联行为，须提供界面截图。
				★支持基于 SCADA 等工控协议的相关漏洞攻击检测与防护，提供界面截图。
				★系统应提供敏感数据保护功能，能够识别、阻断通过自身的敏感数据信息（身份证号、银行卡、手机号等），支持正则表达自定义。须提供界面截图。
				设备硬件异常状态监控，可监控设备 CPU 温度，主板温度，风扇的转速。提供设备截图。
				产品要求取得中国信息安全测评中心《信息技术产品安全测评证书（EAL3+）级)》
				★产品须获得国家信息安全测评中心颁发的自主原创产品测评证书，提供证书复印件
7	数据库审计系统	台	1	1U，含单交流电源，2*USB 接口，1*RJ45 串口，1*GE 管理口，6*GE 电口，1 个接口扩展槽位，2T SATA 硬盘。SQL 语句处理能力：15000 条/每秒，入库语

				句量：1500 条/秒，在线日志量 10 亿条以上，归档日志量 100 亿条以上。包含三年软件更新服务、产品保修服务、远程支持服务。
				★支持审计到前端的应用用户、数据库用户、操作系统用户等，需提供截图证明
				支持操作执行的影响范围，如查询、修改或删除的记录行数，执行成功与否的结果以及返回结果集，如查询操作的返回内容。
				★通过模式匹配的方式对 SQL 访问进行监测与告警,判断是否为可疑SQL注入;提供SQL注入特征库，需提供截图证明；
				事件分析：依据安全策略，以时间为基线，统计异常事件的发生数量和趋势，需提供截图证明；
				★告警分析：依据安全策略，以时间为基线，统计严重告警事件的发生数量和趋势,需提供截图证明；
				综合分析：以数据库操作类型为基线统计各类操作状况，需提供截图证明；
				★会话统计：以时间和 IP 为基线统计会话的数量、流量、操作的语句数量，需提供截图证明；
				★支持 MySQL 数据库的 SSL/TSL 加密链路审计，需提供截图证明；
				★对于高风险操作所在的会话,支持旁路阻断功能，避免更大的危害，需提供截图证明；
				产品获得 IPv6 Ready Logo 认证（Phase-2），提供证书复印件。
				产品获得国家信息安全测评信息技术产品安全测评证书 EAL3+级别，提供证书复印件。
8	终端安全系统	套	1	提供 5 个服务器授权，50 个桌面端，抵御病毒、间谍软件、网络钓鱼和其它灰色软件，提供集中的监控界面、系统日志、产品更新、病毒警报等功能，

				含三年防病毒软件升级及病毒特征库升级服务。

四、验收标准和要求：

1、交付时间：合同签订生效之日起 30 天内。

2、交付地点：用户指定地点。

3、付款条件：采购双方签订合同时另行约定。

4、验收要求：按磋商文件技术参数及采购合同进行验收。

B包 用户需求书

一、项目覆盖信息系统

本次项目覆盖信息系统如下：

序号	系统名称	级别	备案编号
1	播控系统	三级（S3A3G3）	46902912001-17001
2	制作系统	二级（S2A2G2）	46902912001-17002

二、项目建设内容

本次项目具体建设内容如下：

序号	服务名称	服务细则	服务频率
1	网络安全测评及安全服务	网络安全等级保护测评服务	一年 1 次
2		漏洞扫描服务	一年 2 次
3		网络安全等级保护加固指导服务	1 次服务
4		网络安全管理制度完善服务	1 次服务

1、网络安全等级保护测评服务

1.1、服务概述

依据《信息安全等级保护管理办法》（公通字[2007]43 号）规定，以及根据公安部和海南省公安厅网络监察职能部门的建议和要求，第二级信息系统应当每两年至少进行一次等级测评，第三级信息系统应当每年至少进行一次等级测评，第四级信息系统应当每半年至少进行一次等级测评，第五级信息系统应当依据特殊安全需求进行等级测评。

将聘请具有公安部认可的网络安全等级保护测评资质的测评机构对县广播电视台相关信息系统开展测评工作，具体工作内容如下：

- **安全技术测评**：包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心等五个方面的安全测评；

- **安全管理测评**：安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等五个方面的安全测评。

序号	服务内容	服务说明	服务对象	服务频率	服务类型
1	网络安全等级保护测评服务	分别对技术类和管理类进行测评，包含：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测评；并提出具有针对性的整改建议。	等级保护对象	1 次	远程服务，现场服务

1.2、服务成果

完成测评工作后，按等级保护对象出具符合公安机关要求的《网络安全等级测评报告》，并提出具有针对性的整改建议。

1.3、服务收益

通过网络安全等级保护测评服务，达到以下收益：

- 通过网络安全等级测评掌握网络安全状况、排查系统安全隐患和薄弱环节；
- 衡量等级保护对象的安全保护管理措施和技术防护措施是否符合相应等级保护基本要求，是否具备了相应等级的安全保护能力；
- 明确等级保护对象安全建设整改需求，避免重复投资、重复建设，避免信息安全事件发生造成的经济损失；
- 落实国家网络安全等级保护相关政策与标准要求，实现等保合规。

2、漏洞扫描服务

2.1、服务概述

安全漏洞扫描评估是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，帮助用户及时掌握信息系统安全状况，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，以及时帮助客户堵塞安全漏洞，协助指导客户落实和完善安全措施，以帮助客户建立信息安全保障机制，减少安全风险，提高应急处置能力，从而促进信息系统持续安全稳定运行。

为了确保我单位两个应用信息系统的正常稳定运行，我单位需聘请具有资质的安全服务商，进行提供一年 2 次（不定期）的信息系统漏洞扫描评估服务。

2.2、服务成果

根据我国网络安全等级保护标准《GB/T 22239—2019 网络安全等级保护基本要求》，聘请第三方的测评机构对网站进行安全漏洞扫描，出具《漏洞扫描安全评估报告》。通过开展不定期安全漏洞扫描评估服务，及时发现存在的安全问题和薄弱环节，分析面临的安全威胁和风险，并对发现的安全隐患提供改善建议。

2.3、服务收益

1.通过主动防御，及时发现网站存在的安全隐患以及可能发生的安全事件，使得客户可以及时快速地应对处理安全事件，制定相应的预防措施，防患于未然。

2.提前消除安全事件带来的影响，降低安全事件给客户带来的损失和风险。

3.周期性的漏洞扫描分析报告，提供专家建议，为客户提供网站安全整体风险状况以及安全发展趋势。

3、网络安全等级保护加固指导服务

3.1、服务概述

随着信息化的不断推进，业务应用持续增加，基础设施的架构越来越复杂，面临的安全威胁越来越多，信息系统是否能够正常运行直接关系到业务或生产是否能够正常运转维系，信息系统的任何安全问题如果没有及时得到妥善处理都将会导致很大的影响，甚至会造成可怕的政治事件。

为了有效促进信息系统的安全稳定运行，将依据国家及行业网络安全等级保护的相关标准及法规的要求，从网络安全、主机安全、应用安全和数据安全的角

度，结合多种技术手段为信息系统提供网络安全等级保护加固服务，逐步构建动态、完整、高效的信息安全技术体系，提高信息系统的整体技术防护能力，从整体上促进信息系统的安全稳定运行。

主要服务内容如下：

①网络安全加固

- 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。

②主机安全加固

- 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。

③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	网络安全等级保护加固指导服务	从网络安全、主机安全、应用安全和数据安全的角度，结合多种技术手段提供网络安全等级保护加固指导，出具《网络安全等级保护安全加固报告》	针对一个重要系统	《网络安全等级保护安全加固报告》	一次性	现场服务

3.2、服务成果

通过对信息系统进行网络安全加固、主机安全加固及应用安全加固指导，以提高信息系统的整体技术防护能力，输出《网络安全等级保护安全加固报告》。

3.3、服务收益

- 满足等级保护制度的各项要求，实现等级保护合规；
- 实现信息系统等级化保护和等级化管理；
- 提高客户信息系统抗攻击的安全防护能力；
- 消除或减少安全隐患和安全事故对信息系统的影响；
- 消除或降低安全风险给信息系统带来的安全隐患；
- 有效促进信息系统业务应用的安全稳定运行。

4、网络安全管理制度完善服务

4.1、服务概述

根据我国网络安全等级保护标准《GB/T 22239—2019 网络安全等级保护基本要求》，结合单位的实际管理需求，调整原有信息安全管理模式和信息安全管理策略，聘请第三方的测评机构协助单位对安全管理制度和规范流程进行梳理、调整和编制，构建满足网络安全等级保护的安全管理体系，完善信息安全管理相关控制措施，控制信息安全风险，确保单位自身的管理要求和相关监管机构要求的符合性，提升安全管理的有效性和持续性。

4.2、服务成果

- **《信息安全管理体系制度》**

信息安全管理体系-制度清单		
序号	**文件名称**	**主要内容**
第一部分 总体方针策略		
1	信息安全工作总体方针	信息安全工作总体方针,为纲领性文件，概要说明机构安全工作的总体目标、范围、原则和安全框架等。
2	安全管理制度制定和发布	本文件规范了体系文件的编制与修订职责、分类、编号、字体字号、编制、审核、批准、发布、保管管理、借阅和复制、修订、

		作废和评审等。
3	信息安全管理体系评审与修订	本文件规范了信息安全管理体系管理评审活动程序，明确管理评审的目的和作用，确认管理评审的输入材料和输出材料；
4	记录表单管理制度	本文件规范了操作过程记录表单，记录各类安全管理活动的过程和操作；规范记录表单的编号、编制、监督与检查、存储保管、查阅与借阅、作废等要求。
第二部分 机构和人员安全管理		
5	信息安全管理体系职责	本文件对信息安全管理机构及人员责任给予定义，通过清晰的责任界定以保证信息安全方针得到有效的贯彻，保障信息安全管理活动的有序进行；包含安全管理机构（信息安全领导小组、安全管理机构职责、机构部门设置）、安全岗位职责（信息安全主管、安全管理负责人、物理安全负责人、网络安全负责人等）、授权与审批、沟通与合作、审核与检查等要求；
6	人员安全管理制度	本文件规范了单位从人员录用、人员离岗、人员岗位调动、人员考核、人员惩戒、人员安全意识教育与技能培训、外部系统运维人员安全管理、运行维护人员安全管理的要求。
7	安全培训与考核管理制度	本文件规范了信息安全培训的要求、培训的内容、培训的管理（发起和实施）等要求。
8	第三方工作人员管理制度	本文件规范了第三方访问的风险管理、第三方物理访问的安全管理、第三方人员安全保密管理、第三方人员安全操作管理等。
第三部分 系统建设管理		
9	信息系统建设管理制度	本文件规范了信息系统建设的整个生命周期，分别从工程实施建设前、建设过程及建设完毕交付等三方面做出规定，具体包括：系统定级、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、系统备案、等级测评和安全服务商选择等方面的管理要求。
第四部分 系统运维管理		
10	机房安全管理制度	本文件规范了机房安全管理要求，包括环境安全管理、设备安全管理、机房出入管理、机房保密管理、机房安全检查等方面要求。
11	办公计算机安全管理制度	本文件规范了办公 PC 信息安全基本要求、使用网络相关规定、监督与检查等。
12	资产管理制度	本文件规定中心信息系统资产管理的责任部门，并规范资产的识别、赋值、管理、以及笔记本管理、存储介质管理、数据资产管理、资产维护与报废等方面要求。
13	介质管理制度	本文件规范了中心各类介质的存放、使用、归还、维护、运输（带出）、报废等方面要求。
14	恶意代码防范管理制度	本文件规范了恶意代码管理的总体要求，包括安全策略、安全管理、安全报告、病毒响应等要求。
15	帐户与密码管理制度	本文件规范了账号密码管理的职责、账号安全、密码安全、权限安全、登记管理、安全检查、以及账号申请与审批等要求。
16	变更管理制度	本文件规范变更的定义、流程、过程职责等要求。
17	网络安全管理制度	本文件规范网络设备维护管理、安全设备维护管理、网络与安全设备运行管理、网络漏洞管理、备份与恢复等方面要求。
18	系统安全管理制度	本文件规范服务器的操作系统基本配置管理、网络服务配置管理、补丁与漏洞扫描管理、日志管理、增强性安全配置管理、业

		务连续性管理等方面要求。
19	数据备份与恢复管理制度	本文件规范数据备份的职责分工、数据备份与恢复管理方面的要求。
20	信息安全事件处置管理制度	本文件规范事件定义、分级、分类、发现、处理、上报与总结等要求。
21	应急响应管理制度	本文件规范应急预案组织与职责、应急预案制定、应急预案启动、应急措施、以及网站方面、黑客攻击、病毒安全、软件系统遭破坏、数据库方面、广域网线路中断、局域网线路中断、设备安全、机房火灾、电力中断、关键人员不在岗、自然灾害等方面紧急处置措施等要求。
22	网站信息发布与安全管理制度	本文件规范网站信息采集、审核、发布和更新等方面要求。

4.3、服务收益

1.落实等级保护制度管理方面的各项要求，实现等保合规。

2.实现信息系统等级化保护和等级化管理。

3.提高本单位内部全员的信息安全意识。

三、验收标准和要求：

1、服务期限：网络安全等级保护测评服务（采购人下达开工指令后 30 个工作日内。

），其他服务期限（1 年）。

2、交付地点：用户指定地点。

3、付款条件：采购双方签订合同时另行约定。

4、验收要求：按磋商文件技术参数及采购合同进行验收。