第三章 用户需求书

一、项目名称

1、项目名称：高清电视播控系统等级保护设备购置（四次招标）

2、交付期：合同签订之日起 60 天内

3、预算金额：1330000.00 元

4、（投标人的报价不得超过其预算金额，否则将导致废标）

5、交货地点：海口市龙华区中沙路 15 号

6、付款方式：合同签订后支付合同总价的 30%，设备到场后支付合同总价的 40%，项目验收完成后支付合同总价 25%，扣除 5%质保金一年后支付。

二、概述

随着广播电视数字化、网络化的快速推进，IT 技术在广播电视台得到了广泛应用，计算机网络渗透到了广播电视制作、播出、传输、发射等各个环节，广播电视的数字化程度得到了大幅提升。先进的技术手段深刻的影响着广播电视的转型发展，但对广播电视的安全工作也提出了更高的要求。网络信息安全是新技术的产物，也是广播电视系统安全工作近年来面临的一个重要问题。尤其是随着广播电视台的业务网规模的不断扩大，系统功能和业务内容的不断扩宽，网络信息安全工作的重要性日益凸显，上升到了与安全播出同等重要的层面。

基于此，广电总局于 2011 年发布了《广播电视安全播出管理规定》（总局令第 62 号），明确提出要开展信息系统等级保护工作。并且为进一步贯彻落实相关要求，广电总局先后制定了《广播电视相关信息系统安全等级保护定级指南》（GD/J 037-2011）和《广播电视相关信息系统安全等级保护基本要求》（GD/J 038-2011）等相关标准与规范，作为规范全行业信息安全防护工作，提升安全播出保障能力的基础性标准。

由此可见，信息安全事关国家安全、社会稳定，广播电视系统虽然对信息安全给与了高度重视，尤其是信息安全与广播电视行业技术特性差异性，迫切

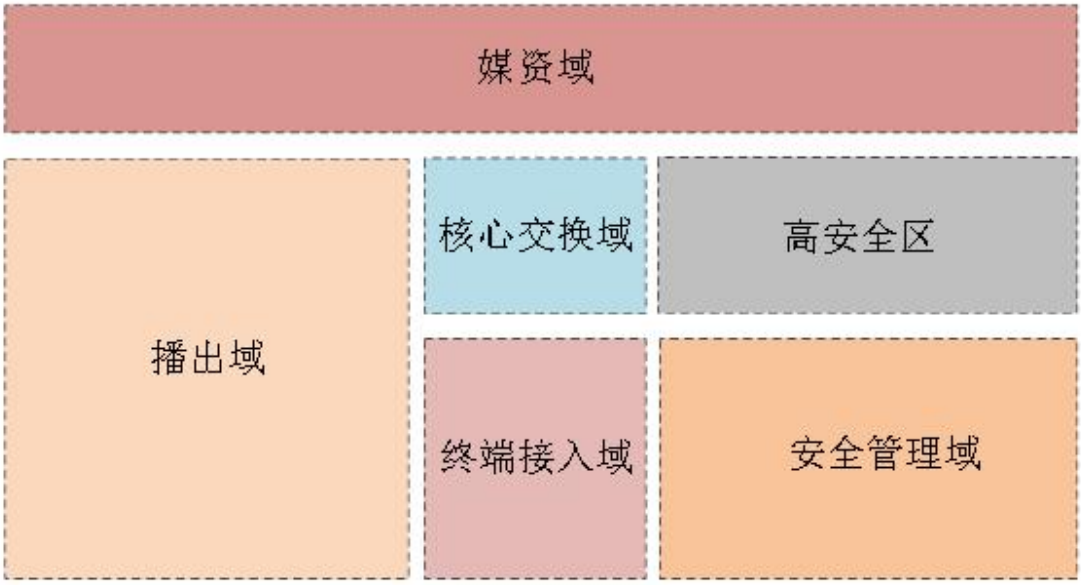
需要广播电视系统进一步加大对信息安全工作研究力度，加大新技术手段的应用，建立可管可控可信可行的信息安全保障体系是一项迫在眉睫的工作。

海口广播电视台作为海口市重要宣传机构，承担着向市民传播当地社会政治、经济、文化和群众生活的重大任务。因此，应积极响应国家号召，进行信息安全建设，保障安全播出。本方案依据广电总局已发布的相关技术标准、技术规范、实施指南、实施细则等要求，为海口广播电视台高清播控系统制定符合标准要求的信息安全网络安全防护体系建设方案。安全播出是海口广播电视台运营与发展的基础与核心，保障播出安全，是本次建设的最终目的。

三、需求分析

海口广播电视台高清播控系统为我单位现有业务系统，现要对高清播控系统进行等级保护合规建设。根据《广播电视相关信息系统安全等级保护定级指南》（GD/J 037-2011）中 4.5.2 广播电视相关信息系统安全保护等级要求，高清播控系统等级保护应按照第三级进行建设。根据《广播电视相关信息系统安全等级保护基本要求》（GD/J 038-2011）中基础网络安全、边界安全、终端系统安全、服务端系统安全、应用安全、数据安全与备份恢复、安全管理中心、通用物理安全和通用管理安全等相关要求，本项目是对海口广播电视台高清播控系统进行第三级等级保护建设。

本次投标人应严格按照等级保护基本要求对海口广播电视台进行等级保护方案设计，按照如下安全域进行划分：



四、技术规范

投标人所提供的方案和设备应至少满足所列标准和规范性文件，对于未列出的标准和规范性文件，若国内已有相应标准的首先应遵循国内标准，若国内暂无标准的可以参照厂家标准，但必须提供厂家标准的详细资料，并作详细说明。

- 信息安全等级保护管理办法（公通字[2007]43 号）
- 关于开展全国重要信息系统安全等级保护定级工作的通知（公信安[2007]861 号）
- 信息安全等级保护整改工作的指导意见（公信安[2009]1429 号）
- 广播电视安全播出管理规定（总局令 62 号）
- 广播电视相关信息系统安全等级保护定级指南（GD/J 037-2011）
- 广播电视相关信息系统安全等级保护基本要求（GD/J 038-2011）
- 广播电视相关信息系统安全等级保护测评指南（GD/J 044-2012）
- 《中华人民共和国网络安全法》
- 《建筑内部装修设计防火规范》GB 50222

- 《采暖通风与空气调节设计规范》GB 50019
- 《供配电系统设计规范》GB50052-1995
- 《建筑照明设计规范》GB50034-1995
- 《安全防范工程技术规范》GB50348-2004
- 《建筑物电子信息系统防雷技术规范》GB50343-2004
- 《计算机机房用活动地板技术条件》GB 50343-2004
- 《气体灭火系统设计规范》GB50370
- 《电子信息系统机房设计规范》（GB50174-2008）

五、设备清单及配置

序号	产品名称	配置	单位	数量	备注
一、安全部分					
1	综合安全网关	机箱：标准 2U 机箱；整机吞吐率≥10Gbps；端口规格：千兆电口≥12， SFP 光口≥12，SFP+光口≥12； ；冗余电源：双电源；详细配置：IPS 吞吐量≥6Gbps,防病毒吞吐量≥3.5Gbps,每秒新建连接数≥20 万,最大并发连接数≥400 万；IPSec VPN 隧道数≥1024，SSL VPN 接入数≥1500；保修情况：含三年硬件维修服务，含三年 AV 和 IPS 特征库升级服务	台	2	
2	网闸	标准 2U 机箱，双冗余电源；内网：不少于 4 个 SFP 插槽，≥4 个 SFP+插槽，4 个 10/100/1000M Base-TX 网络接口，1 个 10/100/1000M Base-TX 管理接口，1 个 10/100/1000M Base-TX HA 接口（双机热备口）；外网：不少于 4 个 SFP 插槽，≥4 个 SFP+插槽，≥4 个 USB 口;4 个 10/100/1000M Base-TX 网络接口,1 个 10/100/1000M Base-TX 管理接口，1 个 10/100/1000M Base-TX HA 接口（双机热备口）；系统	台	2	

		吞吐量≥9Gbps,并发连接数>60 万；系统延时 <1ms，硬件延时 <1ns；整机配液晶屏，提供工作状态，当设备处于异常状态下，声或光报警、设备提供 HA 工作状态监控灯，可通过 HA 灯可查看设备 HA 工作状态，方便设备维护；支持文件交换、FTP 访问、数据库传输、邮件传输、安全浏览、安全通道、消息模块等功能；含三年硬件保修和技术支持服务。			
3	数据库审计系统	系统：审计产品采用专用工控机硬件架构，非普通 PC 服务器， MTBF(平均故障间隔时间)≥65000 小时；网口类别:≥6 千兆电口；≥4 千兆光口 硬盘: ≥1T*2（支持 RAID1） 内存≥8G*2；电源:双电源；系统启动采用 CF 卡加硬盘方式，保证稳定可靠不可篡改。 审计性能：能够稳定、流畅地同时支持 12 个数据库数审计能力，不会产生漏审；含三年硬件维修和技术支持服务。	台	1	
4	堡垒机	1U 机架式软硬一体设备,专用硬件平台和安全操作系统，不少于 6 个千兆电口，硬盘容量≥1TB，单电源。实现对运维操作（telnet/ssh/ftp/sftp/RDP/VNC/X11)的集中管理、访问控制、单点登录以及操作审计等功能，含应用发布模块。支持不少于 700 路字符会话或 200 路图形会话并发。最少支持两种以上不同的组合鉴别技术实现被管资源双因素认证，被管资源数≥100 个点，含三年的硬件维保服务。	台	1	
5	入侵检测系统	电源:冗余电源;≥1T 可用磁盘空间,≥6 个 10/100/1000M 以太网端口；网络层≥1Gbps，应用层≥500Mbps；文件检测≥3 万/24 小时；含三年硬件维修服务，含三年事件库和病毒库升级服务。	套	1	
6	日志审计系统	2U 标准机架式，冗余电源；端口规格：≥6 个千兆电口，1 个 console 口，内存≥8GB，磁盘≥4T； 平均处理能力（每秒日志解析能力 EPS)：≥4000EPS;峰值处理能力(每	套	1	

		秒日志解析能力 EPS）：≥5000EPS。含三年硬件维修和技术支持服务。			
7	主机安全及管理系统	包含管理中心软件 1 套，10 台服务器防护软件授权、40 台桌面系统防护授权。支持检测 WEB 攻击、异常访问、远程控制、WEB 后门访问、发件人欺骗、邮件头欺骗、邮件钓鱼、邮件恶意链接、恶意文件攻击、DGA 域名请求、SMB 远程溢出攻击、WEB 行为分析、隐蔽信道通信、暴力破解、挖矿等风险主机安全及管理系统由管理控制中心和客户端组成，功能包含传统病毒查杀、漏洞管理、性能监控功能，在系统防护方面还可做到主动防御、系统登录防护、系统进程防护、文件监控，还支持网络防护、Web 应用防护、勒索挖矿防御、外设管理等；售后服务情况：一年 7*24 小时电话服务；服务使用期限：含三年升级服务。	套	1	
8	漏洞扫描服务	漏洞扫描服务可以对不同操作系统下的计算机、网络设备、安全设备等进行漏洞检测。对用户网络进行漏洞扫描，用于分析和指出网络设备的安全漏洞及被测系统的薄弱环节，给出详细的《漏洞扫描报告》，并针对检测到的网络安全隐患给出相应的修补措施和安全建议。	项	1	
9	安全加固	依据国家及行业信息安全等级保护的相关标准及法规的要求，结合我单位业务系统的实际情况和测评结果，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信息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，最终出具《信息安全加固报告》。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，并根据响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，	项	1	

		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）应用安全加固知道：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；对 WEB 应用系统的代码规范安全加固进行指导。			
10	安全管理制度	依据国家广电行业信息安全等级保护基本要求，针对我单位信息管理工作实际需求，开展信息安全管理体系建设，对组织的管理体系方面进行安全管理，明确主管领导、落实责任部门、落实安全岗位和人员、确定安全管理策略、制定安全管理制度、落实安全管理措施、落实《基本要求》管理制度各项指标和要求，提高信息系统的管理和运维水平。提交由安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系：一级文件为纲领性文件，是信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、安全框架和安全职责，包括《信息安全工作总体仿真》、《信息安全管理机构职责》、《安全管理制度制定和发布》和《信息安全管理体系评审与修订》。二级文件为安全管理制度，是安全管理活动中的各类安全管理制度，包括《人员安全管理制度》、《安全培训与考核管理制度》、《信息系统建设管理制度》、《机房安全管理制度》、《办公计算机安全管理制度》、《资产管理制度》、《介质管理制度》、《恶意代码防范管理制度》、《网络安全管理制度》、《系统安全管理制度》、《数据	项	1	

		备份与恢复管理制度》、《信息安全事件处置管理制度》、《账户与密码管理制度》、《变更管理制度》和《应急预案管理制度》。三级文件为安全操作规程，是管理人员或操作人员执行的日常管理操作规程，包括《设备操作规程》、《操作系统操作规程》、《数据库操作规程》等。四级文件为操作过程记录表单，记录各类安全管理活动的过程和操作。			
11	管理交换机	二层百兆盒式交换机；可支持双绞线、光纤传输介质；；支持 IPV4、IPV6 等网络标准协议；配置 24 个 10/100Base-TX 以太网端口,4 个千兆 SFP,2 个复用的 10/100/1000Base-T 以太网端口 Combo,PoE+,交流供电；支持 WEB 管理、SNMP 管理 ；交换容量 64Gbps、包转发率 14.1Mpps；保修情况：默认 3 年保修	台	1	
二、集成部分					
（一）、红外报警系统					
1	电话型语音报警器	99 路无线防区，接警真人语音播报；添加迎客门铃功能，增加智能求救报警； 主机具有防破解功能、同频干扰提示、系统密码保护、多防区模式；拥有智能防区实现零误报，报警事件查询，电话断线报警、抢线报警；报警时有声无声可调、布防延时、报警延时 0-99 秒可调；远控制电话振铃次数，外出全设防、在家部份设防、定时布撤防功能；可远程控制主机或报警后电话远程主机控制功能；标准配置：主机 1 部+遥控器 2 个+门磁 1 个+红外探测器 1 个+喇叭 1 个+电源适配器 1 个+电话线 1 条	套	1	
（二）、气体消防灭火系统					
1	气体喷射装置	含柜体、储瓶、压力表、电磁驱动阀、压力信号器、高压软管	套	1	
2	灭火剂	七氟丙烷	kg	83	

3	感烟探测器	内含 CPU，安装部位天花	只	2	
4	感温探测器	内含 CPU，安装部位天花	只	2	
5	气体灭火控制器	壁挂式，液晶汉字显示；总线制，，直接连接现场设备；具有火灾报警控制器功能。	台	1	
6	放气指示灯	无地址编码，直接连接	只	1	
7	手动启/停按钮	直接连接，带指示灯、防护罩	只	1	
8	气体泄压阀	气体泄压阀	项	1	
9	声光报警器	配声光底座使用	只	2	
10	检测费	第三方公司检测费用	项	1	
11	辅助材料	线管、RVV 连接线、接头、固件等	批	1	
（三）、监控报警系统					
1	网络高清室内半球	200 万 1/2.7”CMOS ICR 日夜型半球型网络摄像机	台	4	
2	8 路硬盘录像机	1U 标准机架式 IP 存储/嵌入式处理器/8 路 H.265、H.264 混合接入，HDMI 支持 4K	台	1	
3	监控硬盘	3T	块	1	
4	网孔门机柜	42U；前后单开门	台	1	
5	安装调试费		项	1	
（四）、门禁系统					
1	门禁一体机	用户数：5000 人；指纹容量：3000；通讯方式：TCP/IP、RS485/232；电源规格：DC12V/3A	台	3	
2	单门磁力锁	≥350 kg力,灯指示,单门磁信号	套	3	
3	门禁专用电源	流输入标准 220VAC ，50HZ；直流输出标准 12VDC，5A；外形尺寸 180*77*77MM	块	3	
4	玻璃门夹	国产优质	套	1	
5	闭门器	国产优质	套	2	

6	地弹簧	国产优质	套	1	
7	出门按钮	86*86*38mm	个	3	
8	超五类非屏蔽网线	超五类 4 对非屏蔽双绞线	箱	2	
9	镀锌钢管	φ25	米	150	
10	安装调试费		项	1	
11	系统工程辅助材料	水晶头、扎带、胶粒、螺丝钉、胶布、材料配件及接头固件等	批	1	

六、技术要求

应在综合安全网关、网闸、交换机等网络设备数据传输顺畅不堵塞的前提下、计算环境分别对各类型应用服务器、工作站、业务应用系统，其中主机操作系统的安全至关重要，为此我们通过身份鉴别、安全审计、入侵防范和恶意代码防范等功能，确保应用系统自身运行的安全可信，从而在整体上达到等级保护。

本项目软硬件配置必须达到国家广电总局对广播电视播出系统的三级安全等保要求，能通过等级保护评测和验收，提供本项目信息安全等级保护最终测评报告。

1、边界安全

根据对安全保护等级达到等级保护三级的基本要求，必须符合以下技术要求：

1) 满足与外部网络数据交换时应采取带宽分配策略保障重要业务运行；

2) 网络访问控制设备应启用基于 IP 地址段及端口级的允许/拒绝访问控制策略；

3) 边界网络设备和关键网络设备，应对重要网段采取网络地址与数据链路地址绑定或其它网络准入控制措施等技术手段防止地址欺骗；

4) 外部网络用户应采取安全接入方式，基于用户级对用户权限进行管理；

1.1 身份鉴别

身份鉴别是对信息系统访问者身份合法性的确认，是对其访问权限进行分配与管理的前提，同时也是审计功能及用户数据保护的先决条件。

应满足以下条件：

内部业务人员在使用业务系统前，应通过强制身份认证方式鉴别是否是合法用户；

业务人员在系统内部登陆服务器/工作站、业务系统时，用户登录需采用用户名和静态密码、动态密码结合的方式进行认证；

身份鉴别、账户及密码的具体安全策略需求如下所示：

项目	序号	策略	目的
身份鉴别	1	重命名超级用户 administrator 的名字，更改成非 administrator	Administrator 为默认账户，恶意直接利用该账户通过字典方式破解密码
	2	禁用 guest 或者其它无用账号	禁止默认 Guest 账户登陆操作系统，Guest 账号容易被非法利用
	3	禁止 administrator 作为业务系统登陆使用，建立专用业务账户： 业务账户：如 dayang 归属组：administrator 组 权限：建立 administrator 同样权限的一个系统专用管理账户，用于操作系统日常管理，更名后的 administrator 用于涉及操作系统硬件或者自身疑难问	增加账户破解的难度

		题的情况下使用、以及业务软件的安装等	
	4	设置非授权登陆提示信息	提示非授权用户登陆的错误信息
密码策略	1	密码设置策略如下： 密码必须符合复杂性要求已启用 密码长度最小值 8 个字符 密码最短使用期限 0 天 密码最长使用期限 180 天 强制密码历史 3 个记住的密码	设置复杂密码，并定期更换，防止密码猜测和泄露、防止弱口令容易被猜测
	2	密码锁定策略如下： 帐户锁定时间 3 分钟 帐户锁定阀值 5 次无效登录 重置帐户锁定计数器 3 分钟之后	合法账户如果多次探测密码，则对该账户进行锁定，防止字典攻击

1.2 访问控制

通过对操作系统进行安全加固，严格限制文件访问和系统使用权限，防止非授权使用高安全区业务数据、或者非授权登陆操作进行非法操作。

具体的安全策略需求如下所示：

项目	序号	策略	目的
访问控制	1	修改 snmp 沟通串	默认配置沟通串 public/private 能够远程探测和管理该服务器
	2	共享文件夹权限授权	禁止任何人都能访问到共享的资源
	3	系统关键位置文件夹/文件权限保护	防止非授权对 windows 操作系统关键配置文件进行恶意操作

1.3 安全标记与访问控制

根据 GD/J038-2011 基本要求，高清播控系统定级为等级保护三级系统，标准如下：

重要服务器应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限，应对重要信息资源设置敏感标记，应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

网络业务系统应具有对重要信息资源设置敏感标记的功能，应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

2、入侵防范

2.1 主机防入侵

针对主机操作系统的入侵防范，首先使用漏洞扫描系统，评估主机的脆弱性，然后通过操作系统安全加固，对主机操作系统补丁进行定期更新、对主机的外设和默认的服务进行集中管理，以减少系统漏洞。

通过域控制器策略进行部署，具体的安全策略需求如下：

项目	序号	策略	目的
入侵防范	1	补丁管理	关闭系统不必要的服务，提高系统安全，否则系统面临容易被攻击、渗透或利用的风险
	2	禁用系统不必要的服务	
	3	关闭默认共享$	
	4	关闭外设自动播放功能	防止移动介质容易引发病毒传播
	5	禁用移动存储介质	
	6	关闭服务器默认 web 管理	服务器默认具备后台以 web 方式管理服务器，利用默认的账户和密码容易引发安全风险

2.2 网络防入侵

针对整个系统边界的入侵防范，应能够在信息系统的网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、

IP 碎片攻击和网络蠕虫攻击等，节目上载终端、收录服务器等高清播控系统的边界可根据需要进行部署；

当检测到攻击行为时，应记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。

3、恶意代码防范

为了防止恶意代码对网络业务系统进行恶意传播或者破坏，应部署具有统一管理功能的防恶意代码软件，并定期更新防恶意代码软件版本和恶意代码库。系统当前未部署防病毒软件的设备，应选择几个测试机经过测试并试运行 1 个月左右，如果无任何影响，则分布安装部署防病毒软件。

应在信息系统的网络边界处进行恶意代码检测和清除，并维护恶意代码库的升级和检测系统的更新，节目上载终端、收录服务器等与播出直接相关的边界可根据需要进行部署；防恶意代码产品应与信息系统内部防恶意代码产品具有不同的恶意代码库。

4、集中安全审计

信息系统的安全审计就是对系统中有关安全的活动进行记录、检查及审核。检测和阻止非法用户对信息系统的入侵，并显示合法用户的误操作。审计作为一种事件追查的手段来保证系统的安全，它对涉及系统安全的行为做一个完整的记录。

审计为系统进行事故原因查询、定位，为事故发生前的预测、报警以及事故发生之后的实时处理提供详细、可靠的依据和支持，以备有违反系统安全规则的事件发生后能够有效的追查事件发生的地点和过程以及责任人。

安全审计应涉及两个方面：一个是日志，另一个是审计。日志是安全事件及行为的记录，审计则是对日志的分析。

4.1 网络审计

应对关键网络设备的运行状况、用户行为等重要事件进行日志记录；

审计记录应包括事件的日期、时间、用户名、IP 地址、事件类型、事件是否成功等；

应提供保护审计记录的功能，避免受到未预期的删除、修改或覆盖等，并且审计记录可保存 6 个月；

应提供定期对审计记录进行分析的功能，以便及时发现异常行为；

应为安全管理中心提供集中管理的接口。

4.2 主机安全审计

播出系统定级为等级保护三级系统，标准要求如下三级系统服务器/工作站审计达到如下要求：

1）应保护审计进程，避免受到未预期的中断；应保护审计进程，避免受到未预期的中断；

2）应保护审计记录，避免受到未预期的删除、修改或覆盖等至少存应保护审计记录，避免受到未预期的删除、修改或覆盖等至少存应保护审计记录，避免受到未预期的删除、修改或覆盖等至少存应保护审计记录，避免受到未预期的删除、修改或覆盖等至少存应保护审计记录，避免受到未预期的删除、修改或覆盖等至少存应保护审计记录，避免受到未预期的删除、修改或覆盖等至少存 6 个月；

3）应定期对审计记录进行分析，以便及时发现异常应定期对审计记录进行分析，以便及时发现异常应定期对审计记录进行分析，以便及时发现异常行为；

4）应为安全管理中心提供集的接口。

根据主机审计的要求，提出了相应的解决方案，具体来说，需要在业务服务器上均开启安全审计策略，通过在服务器上部署 Agent 方式（Windows 类服务器）

或 SYSLOG 方式（UNIX/LINUX 类服务器）统一采集安全审计日志，并发送到安全管理平台进行集中分析与管理，服务器需要审计的内容包括：

1）接口服务器、应用服务器和数据库服务器应开启操作系统安全审计功能，对重要用户行为（如用户创建、登录、注销）、系统资源的异常使用情况（如特权使用、文件权限更改）、重要系统命令（如 FTP、TELNET）使用情况进行审计；

2）审计记录至少应包括事件的日期、时间、类型、用户名、终端 IP 地址、访问对象和结果等；

3）审计记录应通过 SNMP、SYSLOG 或专用接口等方式发送到安全管理平台进行审计集中管理，审计记录应至少保存 6 个月以上；

4）应保护审计记录，避免受到未预期的删除、修改或覆盖等；

5）应定期对审计记录进行分析，以便及时发现异常行为。

4.3 数据库审计

根据 GD/J 038-2011 基本要求，对数据库的审计应至少包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；

审计记录至少应包括事件的日期、时间、类型、用户名、客户端 IP 地址、访问对象、结果等。

4.4 应用审计

应至少提供覆盖到每个用户的审计功能；

审计内容应至少包括用户登录、修改配置、核心业务操作等重要行为，以及系统资源的异常使用等；

审计记录应至少包括事件的日期和时间、事件类型、客户端 IP 地址、描述和结果等；

保证无法单独中断审计进程；

保证无法删除、修改或覆盖审计记录，审计记录保存 6 个月；

提供对审计记录数据进行统计、查询、分析及生成审计报表的功能；

保证为安全管理中心提供集中管理的接口。

4.5 集中管理

应保证对基础网络、边界安全、服务器及应用系统的安全审计进行集中管理；

应保证对审计记录进行统计、查询、分析及生成审计报表；

应提供对 6 个月以上的审计日志进行归档，归档日志保存一年以上。

5、运维监控

应支持对 PC 工作站、服务器整机的性能指标及工作状态进行监控；

应支持对网内交换机、存储等周边网络设备的性能指标及工作状态进行监控；

应支持对数据库运行状态及关键指标、关键软件进程状态进行监控；

应支持对系统中的业务流程运行状态进行监控；

应保证各监控项可设定监控指标，并可对指标预设警告和报警阈值，超过报警阈值的异常指标可实现多种形式的报警。

七、详细技术参数要求

一、综合安全网关	
参数项	指标要求
★产品规格	双电源，千兆电口≥12， SFP 光口≥12，SFP+光口≥2，硬盘≥1T
	设备最大吞吐量≥10 Gbps，HTTP 吞吐量≥8 Gbps，最大并发连接数≥400 万，每秒新建连接数≥20 万，SSL VPN 接入数≥1500，IPSec VPN 隧道数≥1024
部署模式	支持路由模式、透明模式、混合模式，可将多个物理网口加入一个网桥中；支持端口镜像和被镜像；
内网资产监控	▲支持实时监控并展示内部网络资产的操作系统类型、风险级别、杀毒软件、IP 地址等，提供产品功能截图并加盖原厂商章。

安全策略	▲支持一体化安全策略配置，可以通过一条策略配置接口、地址、应用、服务、用户等属性，配置入侵防御、病毒防护、URL 过滤、应用过滤、终端过滤等（提供产品功能界面截图证明，并加盖公章）。
IPS	支持入侵检测功能
	可自定义 IPS 特征，可通过 IP、UDP、TCP、ICMP、HTTP、FTP、POP3、SMTP 等 8 种协议自定义攻击特征。
	系统默认 4000+条攻击规则。
AV	支持对 HTTP，FTP，POP3，SMTP，IMAP 流量进行病毒查杀
	可查杀邮件、网页及下载文件中包含的病毒
	支持扫描查杀未知病毒
	支持对最多 20 级压缩文件的病毒查杀，提供产品功能截图并加盖原厂商章
SSL 解密	支持 SSL 协议解密，解密类型包括 https 和邮箱，提供产品功能截图并加盖原厂商章。
弱口令扫描	支持弱口令扫描功能，针对 IP 或 IP 段做空密码检测、弱口令检测、用户名和密码雷同检测。
业务告警	支持设备状态，业务信息告警；可设置告警阀值；可以导出告警日志
统计报表	支持统计设备健康状态、用户行为、网络质量、网络安全等报表
	支持 HTML、PDF 等报表格式，并可通过邮件、FTP 等方式外发
其他	▲需提供原厂三年售后服务承诺函并加盖公章。
★产品资质	具备公安部颁发的防火墙《计算机信息系统安全专用产品销售许可证（增强级）》
二、网闸	
参数项	指标要求
基本要求	支持文件交换、数据库同步、数据库访问、安全浏览、FTP 访问、邮件传输、定制访问、消息传输、流媒体传输等基本功能；
接口	内、外网分别配置 6 个 10/100/1000M 电口，≥4 个 SFP 插槽，≥4 个 SFP+插槽；内外网主机系统分别具有独立的网络口、管理口、HA 口（热备口）；≥4 个 USB 口；
	内外网主机系统分别具有 1 个 RJ45 串口；
★性能	系统吞吐量不小于 9000Mbp；并发连接数不小于 60 万；
IPv6 环境支持	支持纯 IPv6 网络环境，能够在纯 IPv6 网络环境下正常工作（提供产品功能界面截图证明，并加盖公章）
	支持断点续传；支持内容过滤，支持文件大小传输限制，支持时间策略；
数据库同步	▲支持 oracle、Sql Server 、DB2、Sybase 等主流数据库同步；（提供产品功能界面截图证明，并加盖公章）
	支持数据库同步客户端的双机热备技术，为用户提供更高的冗余技术支持；
	支持数据库同步数据统计功能；
	支持数据库同步异常邮件报警功能；
管理审计	支持中文日志显示；支持 FTP 方式上传日志；日志实现按功能模块分组管理
	支持配置文件以加密的方式导出

可靠性	双机热备支持配置同步；
	双机热备支持抢占模式
其他	▲需提供原厂三年售后服务承诺函并加盖公章。
★产品资质要求	具备公安部《计算机信息系统安全专用产品销售许可证》；
三、数据库审计系统	
参数项	指标要求
硬件规格	系统：审计产品采用专用工控机硬件架构，非普通 PC 服务器， MTBF(平均故障间隔时间)≥65000 小时；
	★网口类别≥6 千兆电口；≥4 千兆光口；硬盘：≥1T*2（支持 RAID1） 内存≥8G*2；电源：双电源；支持 2 个扩展槽位；
	审计性能：能够稳定、流畅地同时支持 12 个数据库数审计能力，不会产生漏审；
部署管理	旁路部署模式下无须在被审计数据库系统上安装任何代理即可实现审计
	▲针对缺少物理端口的数据库服务器环境，例如云环境、虚拟化环境等内部流量无法提供镜像流量的场景,支持在目标数据库安装 agent 代理解决数据库的审计；(提供国家权威检测机构检测报告复印件并加盖原厂商章)；
	支持在审计页面配置审计代理的 CPU 通适性、最大 CPU 使用率、最大内存使用率、CPU 使用率阈值、内存使用率阈值、流量接收端口、抓包过滤串；（提供功能截图并加盖厂商章）
处理能力	吞吐能力：≥2000M，日处理业务操作数：≥4 亿条
	峰值处理能力：≥2 万条/秒
审计协议	支持 Oracle、SQL-Server、DB2、Informix、Sybase、MySQL 等六种主流数据库审计；
	支持 PostgreSQL、Teradata、Cache、人大金仓、达梦、南大通用等数据库审计；
	支持 MongoDB、Hbase、Hive、impala、ElasticSearch、HDFS、canssandra 非关系型数据库审计；（提供功能截图并加盖厂商章）
	▲支持以导入证书的方式实现安全审计，支持对 Mysql5.7 及以上版本、SQL server（2005 及以上版本）数据库采用了加密协议通讯的审计；(提供功能截图证明并盖原厂章)
审计功能	支持数据库操作类、表、视图、索引、存储过程等各种对象的所有 SQL 操作审计；
	支持对操作时间、执行结果、返回结果集、影响行数、执行时长、数据库用户名、实例名、源/目的 IP、源/目的端口、源/目的 MAC、客户端主机名、客户端程序名称、客户端操作系统用户名、业务主机群、SQL 语句、SQL 模板、会话 ID、事件唯一 ID 等至少 21 个条件进行审计；
	▲双向审计：支持数据库的双向审计（请求和返回），包括请求语句、返回结果集、返回行数、运行时长、运行结果、客户端信息、服务器端信息等内容，支持通过返回行数和内容大小控制返回结果集大小； (提供功能截图，和提供国家权威检测机构检测报告复印件(加盖原厂商章))；
	支持跨语句、跨多包的绑定变量名及绑定变量值的审计
	支持导入审计关联的账号信息，支持通过 IP 和账号关联到具体 SQL 是哪个自然人操作。
智能发现	自动识别流量中存在的数据库，也可通过扫描发现网络中的数据库(提供功能截图证明并盖原厂章)。
审计策略	内置审计规则库不少于 200 条。支持事件类型和策略分组，同时支持黑白名单方式策略
	告警分析应支持根据 SQL 模板排行分析，便于告警处理。

	告警查询应支持根据登陆用户、客户端工具名、客户端 IP、规则进行归并分析，能详细展示每类告警占总告警数量百分比，便于告警分析处理（提供截图证明并盖原厂章）；
统计报表	报表支持严格按照塞班斯（SOX）法案、等级保护标准要求生成多维度综合报告；
	支持根据单个数据库或逻辑数据库组生成报表
	支持报表自定义，自定义的条件不少于 20 个（提供功能截图并盖原厂章）
模型分析	▲支持对数据库自动建模及智能对异常行为告警功能；（提供产品功能截图，加盖原厂公章，并提供国家权威检测机构的检测报告证明）；
	可通过行为轨迹图方式展示数据库访问行为
	可基于账号、IP 地址、访问权限、客户端工具等维度对行为模型做钻取分析、变更分析，对学习的安全基线以外的行为自动智能的进行告警（提供功能截图并盖原厂章）
	可以自动对比不同时期的行为模型，以区分其审计日志数趋势、用户、IP 地址、工具、访问权限的差异情况；
系统管理	▲支持用户界面告警、钉钉、SNMP、邮件、短信五种方式告警；（提供功能截图并盖原厂章）
	采用 B/S 架构管理
其他	▲需提供原厂三年售后服务承诺函并加盖公章。
★产品资质	具备国家信息安全测评中心颁发的《信息技术产品安全测评证书》，级别 EAL3+
	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》，数据库安全审计国标-增强级
四、堡垒机	
指标要求	指标要求
★硬件规格	最大字符协议数≥100 个，最大图型协议数≥20 个。
	千兆电口≥6，硬盘≥1T
可管理设备数	可管理设备数量≥100 个，运维用户无限制
身份认证要求	支持多种双因子认证同时使用，基于不同的用户设置不同的双因子认证模式，如用户 1 使用 USBkey、用户 2 使用动态令牌、用户 3 使用手机 APP 动态口令认证
设备管理要求	支持常用的运维协议：SSH、TELNE、FTP、SFTP、rloginT、RDP、VNC；可通过应用发布的方式进行协议扩展
	除 SSH、RDP 等常见运维协议，须支持 mysql、sqlserver、oracle、DB2 等主流数据库协议代理运维，无须输入密码可实现自动登录、无需另外使用应用发布前置机
运维方式要求	支持 Web 访问方式：支持多种浏览器打开堡垒机的 Web 页面直接调用 SecureCRT、Putty、winscp、flashFXP、FileZilla、SecureFX、mstsc、VNC、Xshell 等运维客户端工具
	支持 Web 客户端方式：支持 ssh、telnet、rlogin、rdp、vnc 协议的 web 客户端运维，无需本地运维客户端额外安装工具
	数据库运维可通过堡垒机页面直接调用本地 Windows 系统里的 plsql、 sqlplus、toad、sqlwb、ssms、mysql.exe 等数据库客户端工具。
	提供客户端访问方式：支持使用本地 mstsc/Xshell/SecureCRT /Putty 等客户端工具登录堡垒机访问图形或字符设备，视图界面一致
	SFTP/FTP 的客户端登录支持使用本地的 winscp/flashFXP/SecureFX 等客户端工具登录堡

	垒机访问 SFTP/FTP 设备
▲审计要求	运维审计日志支持对运维操作会话的在线监控、实时阻断、起止时间、来源用户、来源 IP、目标设备、日志回放、协议/应用类型、命令记录、操作内容的详细行为日志。
	Zmodem 传输审计支持 SSH 运维协议，且能保存运维中通过 rz 命令上传下载的文件，便于运维过程文件泄密的追踪溯源。提供国家权威检测机构检测报告证明并加盖原厂商章
	SFTP/FTP 传输审计支持保存运维过程中使用 SFTP、FTP 协议上传下载的文件，便于运维过程文件泄密的追踪溯源。提供国家权威检测机构检测报告证明并加盖原厂商章
	RDP 粘贴板审计能够对 windows 远程桌面协议（RDP）桌面之间复制-粘贴（粘贴板）传输文件进行保存，提供国家权威检测机构检测报告证明并加盖原厂商章
	RDP 磁盘映射审计能够对 windows 远程桌面协议（RDP）磁盘映射所上传下载文件进行保存，便于运维过程文件泄密的追踪溯源。提供国家权威检测机构检测报告证明并加盖原厂商章
安全策略要求	运维规则策略支持通过基于用户/用户组、设备/设备组、设备账号、命令关键字、控制动作、黑白名单、时间、IP/IP 段等组合访问控制策略，授权用户可访问的目标设备。
	支持对重要设备的登录审核功能，运维人员必须向管理员申请登录，管理员允许之后才可登录；否则无法登录
	支持对重要命令进行审核：运维人员执行命令后，须等到管理员审批通过后才可执行成功
系统管理要求	支持自身审计，包括但不限于：登录日志、系统状态检测、运维访问日志、系统配置、日志用户配置日志、设备配置日志、授权配置日志、策略配置日志等
	支持系统日志报表统计功能，统计包括但不限于登录日志统计、配置日志统计、运维访问日志统计等，可以导出报表
其它	▲需提供原厂三年售后服务承诺函并加盖公章。
★产品资质	产品获得公安部颁发的《计算机信息系统安全专用产品销售许可证》
	产品获得中国信息安全认证中心颁发的《IT 产品信息安全认证证书》
	产品获得国家网络与信息系统安全产品质量监督检验中心颁发的《信息技术产品安全分级评估证书》（EAL3+）
五、入侵检测	
基本参数	双电源；可用磁盘空间不小于 1T；10/100/1000M 以太网端口≥6 个
	旁路镜像模式部署，不影响业务和网络架构；
	网络层≥1Gbps，应用层≥500Mbps，WEB 检测≥7 万/秒，文件检测≥3 万/24 小时
审计协议	▲支持检测 WEB、FTP、SMTP、POP3、SMB、IMAP、NFS、TELNET、MYSQL、MSSQL、ORACLE、DB2 等协议，支持检测 VXLAN 镜像流量，支持通过上传证书检测 SSL 流量，具备 LDAP 协议登陆行为分析功能。（提供产品功能截图并加盖原厂商章）。
检测风险类别	支持检测 WEB 攻击、异常访问、远程控制、WEB 后门访问、恶意文件攻击、DGA 域名请求、SMB 远程溢出攻击、WEB 行为分析、隐蔽信道通信、暴力破解、挖矿等风险
告警黑白名单过滤	▲支持告警信息黑白名单过滤功能，可对邮箱、域名、客户端 IP、服务端 IP、邮箱、域名、WEB 风险进行白名单设置；提供截图证明加盖厂商章
弱口令风险检测	▲支持常见协议协议的弱口令检测，包括 FTP、SMTP、IMAP、POP3、TELNET 等。（提供产品

	功能截图并加盖原厂商章）
双向审计	支持双向审计，对请求和响应都进行审计
场景分析	支持场景化的分析能力，对发现的告警进行二次关联，支持对勒索病毒、网站后门、邮件APT 攻击等事件进行预警。
解析协议	支持 HTTP、FTP、SMB、SMTP、POP3、IMAP、HTTPS、SMTPS、POP3S、IMAPS 等协议传输的文件进行检测
文件动态沙箱分析	支持对存在问题的文件输出完整的二进制动态分析报告； 支持动态执行可疑文件，分析代码的注册表、进程、网络、文件等行为，评估安全风险； 对文件关键行为进行截图保存；
文件威胁分析	可对文件进行检测，并展示威胁文件样本 MD5、威胁指数、传播次数，病毒检测、静态动态检测结果等内容；提供功能截图证明并加盖原厂商章
快速排错	▲可以一键登录排错平台，进行系统后台配置和排错，可一键检测故障、核对配置、检查分区、检测数据库表、同步验证、信息收集等功能。提供功能截图证明并加盖原厂商章
告警与报表	告警可详细展示风险级别、发生时间、告警名称、客户端 IP、服务器 IP、报文内容
	支持 kafka、短信、邮件、syslog、snmp、ftp 等告警方式，提供功能截图证明并加盖原厂商章
日志数据管理	▲日志数据保留策略应至少支持天数和百分比两个控制参数，且恢复数据不影响正常的审计功能。提供截图证明加盖原厂商章
其它	▲需提供原厂三年售后服务承诺函并加盖公章。
★产品资质	产品获得公安部颁发的《计算机信息系统安全专用产品销售许可证》
	产品获得中国信息安全认证中心颁发的 ISCCC 增强级认证
六、日志审计系统	
参数项	指标要求
★硬件规格	2U 标准机架式，冗余电源； ≥6 个千兆电口， 1 个 console 口 内存≥8GB，磁盘≥4T；双电源；
处理性能	支持审计 100 个日志源； 平均处理能力（每秒日志解析能力 EPS）≥4000EPS； 峰值处理能力（每秒日志解析能力 EPS）≥5000EPS。
日志收集	支持 Syslog、SNMP Trap、FTP 协议日志收集
	支持安装代理的方式提取日志并收集；
	支持主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等
	可对 VMWare、XEN、Hyper-V 等主流虚拟化系统的日志进行采集。需提供截图并加盖原厂公章。
性能监控	▲支持对目标主机的性能进行监测，包括 CPU、内存、磁盘、磁盘、流量等性能情况，并可设置告警阈值（提供国家权威检测机构检测报告证明并加盖原厂商章）
日志备份	支持根据存储空间剩余大小百分比进行告警和数据清理，可手动或按周期自动备份系统数据，支持将数据自动上传至远程数据仓库。

日志分析	支持对收集到的重复日志进行自动聚合归；
	支持基于内存的实时关联分析，跨设备的多事件关联分析；
	▲具备三维关联分析功能：支持将漏洞扫描结果导入，与系统中已有的知识库和资产进行关联，形成弱点库，当发生安全时间时，与弱点库进行匹配，生成关联分析的安全事件日志，提供国家权威检测机构检测报告证明并加盖原厂商章。
告警功能	支持数据阀值设置，超过阀值将产生告警；
	可以通过邮件、短信和屏幕显示进行告警；
综合查询及报表管理	内置合规性报表 1000+种；
	内置 SOX、ISO27001、WEB 安全等解决方案包
	内置等级保护合规报表，需提供截图并加盖原厂公章。
	内置综合性自动化审计报告；支持用户自定义报表；自定义的报表支持多个统计维度的数据集合；支持报表导出为 PDF 和 Word 格式文件。
资产管理	注册用户资产时，提供自动发现识别能力。提供故障排除功能。提供自助式的升级接口，支持对产品升级、规则升级。 ▲资产拓扑支持按照实际的用户环境进行编辑发布并可以和资产进行绑定，拓扑可以显示资产采集的事件数量被采集资产的状态等信息（提供国家权威检测机构检测报告证明并加盖原厂商章）
其他	▲需提供原厂三年售后服务承诺函并加盖公章。
★产品资质	所提供的产品必须获得国家信息安全认证中心最新颁发的《IT 产品信息安全认证证书》，产品取得国家权威机构销售许可。
七、主机安全及管理系统	
参数项	指标要求
支持的操作系统	Windows server 2003、Windows server 2008、Windows server 2012、Windows server 2016、win xp 、win 7、win 8、win 10、Centos 5.0 +、Redhat 5.0 + 、Suse11 +、Ubuntu 14 +等操作系统。
系统性能监控	可对 CPU 使用率监控、磁盘监控、内存占用率监控、流量监控，支持配置阈值并在达到时报警。
	支持网络通信全时监控。
系统安全防护	防端口扫描，防违规外联，锁定恶意端口扫描及外联行为，以及记录告警。
	违规外联支持黑、白名单双模式，白名单模式支持配置是否允许访问特定网站、IP；黑名单模式支持自定义恶意 IP，且提供告警和阻断。
	内置内核级防火墙（业务间流量东西向隔离）功能，包括协议、IP、端口、流向等细粒度权限控制。
	▲支持主机流量画像展示；可展示威胁横向扩散路径与并能一件阻断威胁；支持违规外联路径展示，可一键阻断违规外联。提供截图证明加盖厂商章
	支持登录防护，包括以系统账号为粒度的异常登录防护、支持多种维度的系统登录访问策略设置、防暴力破解、弱口令检测并告警。触发登录防护后，自动联动添加微隔离规则。
	具有系统漏洞扫描和修复功能，提供真实漏洞补丁。管理中心可作为补丁服务器，提供离线补丁下载器按需智能获取所需补丁。
	支持文件添加、修改、删除的审计。
	支持进程黑名单功能，可阻止不信任的程序启动。
	支持进程白名单功能，只允许信任的进程启动。
防病毒	支持文件实时监控，在进程启动、存储介质接入、新建文件时自动触发。

	提供专门的勒索风险评估功能。包含：系统漏洞检测、恶意进程检测、弱口令检测、高危端口检测等能力。
	提供专门的针对已知勒索病毒的防御引擎，并提供功能开关项。对于已知勒索病毒确保进程无法启动。
	▲具有独立未知勒索病毒的防御引擎，并有按钮一键启/停该功能，保证未知勒索病毒无法对文件加密，该引擎具有白名单功能。提供产品功能截图并加盖原厂商章
	▲具有独立挖矿病毒实时防御引擎，并有按钮一键启/停功能。提供产品功能截图并加盖原厂商章
	支持强力查杀，支持对顽固病毒文件强制停止进程并隔离或动态移除到删除队列。
	支持部分病毒感染文件的修复，对于二进制文件可剥离感染部分，保证应用正常使用。
集中管控	管理平台支持一键卸载客户端、一键停止/恢复所有防护、一键设置客户端卸载密码、一键解除绑定。
可视化功能	可展示各个服务器或主机节点的信息，活动规律、行为变化趋势、运行状态和详细资料，可对历史行为数据查询等。
	可监测节点遭受网络攻击的趋势信息，可直观了解攻击目标、攻击方式、攻击源的变化趋势与详细资料。
其它	▲需提供原厂三年售后服务承诺函并加盖公章。
产品资质	获得公安部颁发的《计算机信息系统安全专用产品销售许可证书》（需提供相关证明材料并加盖原厂商章）
八、视频监控系统	
网络高清室内半球	▲1、1/2.7″ Progressive Scan CMOS ▲2、0.002 Lux @(F1.2,AGC ON), 0 Lux with IR；2.8mm, 水平视场角: 113.5°；H.265 / H.264 / MJPEG 3、ONVIF(PROFILE S,PROFILE G),GB28181,ISAPI； 4、1个 RJ45 10M / 100M 自适应以太网口； 5、支持低码率、低延时、ROI 感兴趣区域增强编码、SVC 自适应编码技术,支持 smart265 编码； 6、码流平滑设置，适应不同场景下对图像质量、流畅性的不同要求； 7、采用 EXIR 点阵式红外灯技术,照射距离可达 20-30 米； 8、支持 smart IR，防止夜间红外过曝； 9、支持 3D 数字降噪，支持 120dB 超宽动态； 10、支持智能后检索，配合 NVR 支持事件的二次检索分析； 11、支持 GB28181 接入,支持 E 家平台接入,支持萤石云平台接入； 12、提供公安部型式检测报告。
8路硬盘录像机	▲1、网络视频接入带宽≥80Mbps； 2、网络接口：不少于 2 个千兆网络电口，2 个 USB2.0 接口、1 个 USB3.0 接口，1 个 eSATA 接口； 3、不少于 2 个 HDMI，2 个 VGA。 4、支持 8 路 H.264、H.265 混合接入； 5、支持 8*1080P 解码，支持 H.265、H.264 解码； ▲6、支持人脸评分机制，支持设置人脸比对失败和陌生人报警提示语，支持报警布防和联动，支持推送报警信息至客户端（以公安部检测报告为准,需提供相关证明材料） 7、支持按姓名检索人脸抓拍图片，人脸检索结果支持导出电子表格（以公安部检测报告为准，需提供相关证明材料） ▲8、支持客户端实时展示人脸比对结果，比对成功人员可查看人脸抓拍图、样本图、相似度、姓名、性别、联系方式、证件类型、证件号、生日、省市、年龄段、戴眼镜等信息；比对失败人员可查看实时抓拍的人脸图片、性别、年龄段、戴眼镜等信息，支持倒叙显示 24H 统计的人脸检测记录（以公安部检测报告为准，需提供相关证明材料） 9、支持报警输入触发一键撤防功能，撤防的报警类型可选（弹出报警画面、声音警告、上传中心、发送邮件、触发报警输出（以公安部检测报告为准，需提供相关证明材料）

九、门禁系统	
门禁一体机	▲1、用户数≥5000 人；指纹容量≥3000；记录容量≥10 万条； ▲2、通讯方式：TCP/IP、RS485/232； 3、电源规格：DC12V/3A； 4、其它功能：高级门禁、Wiegand in/out； 5、使用温度：0℃～45℃；使用湿度：20%～80%。

八、项目其他要求：

1、交付期：合同签订之日起 60 天内；

交付地点：海口市龙华区中沙路 15 号，海口广播电视台。

2、投标人必须完成本项目设备的安装、调试及培训等工作，投标报价须包含设备、安装、调试、培训费、运输费及税金等费用，采购方无需再另行支付任何费用。

3、为了满足项目售后服务应急需求，投标人必须提供详细的保修期内技术支持及服务方案，具体内容包括（但不限于）：

1）、整体工程提供不少于三年的免费维护，设备按原厂商标准提供维护。

2）、提供每周 7×24 小时技术支持和服务，4 小时内作出实质性响应，对重大问题提供技术支持。

4、为保证本次采购货物的质量，严禁投标人低于成本价恶意报价。如投标人的报价低于预算金额的 80%，则投标单位必须在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；若报价证明材料不符合规定或经评标委员会认定为恶性报价的，则报价分计 0 分。

5、培训要求：

中标人应在项目实施的过程中为使用单位人员提供培训。

培训应包括硬件、软件、安全等。投标人必须为使用单位提供业务操作培训并提供详细的培训方案、培训手册及技术资料。

中标人的培训师能够全面介绍系统的整体架构及流程，讲解系统的设置及维护维修方法。

中标人应提供满足需求的中文培训手册以及培训时间表。培训师应结合现场进行操作培训和理论培训，使受培训人员理解如何操作以及维护系统。