需求任务书

一、 项目概述

第1节 项目概况

北京市委、市政府一直以来高度重视北京广播电视台新型全媒体技术发展，并希望以此为突破，助力提升全市宣传工作效果。北京市政府、广电总局在“十四五规划”及多项产业发展指导文件中要求积极推进超高清产业发展，紧抓技术发展趋势、顺应冬奥转播要求，加快北京广播电视台“冬奥纪实 4K 超高清频道”建设工作。2020 年，经向市委宣传部请示同意，市财政局审核通过，广电总局批准，全面启动建设冬奥纪实 4K 超高清频道项目建设。项目一期工程已于 2020 年基本完成，并于 12 月 30 日成功实现 4K 频道开播。2021 年，在一期项目建设成果基础上，拟对前期拍摄、后期制作、传送播出等技术系统进行规模扩容和功能完善，全面满足资讯、赛事、综艺等多种形态节目规模化业务生产能力，为冬奥会、冬残奥会期间冬奥纪实超高清频道提供完整的超高清电视制播业务支持。通过两期项目建设，共同建成一个具备完整策、采、编、播、发能力的 4K 电视频道技术支撑体系，为 2022 年冬奥会、及至 2022 年后冬奥纪实频道转型为以体育、休闲为主要方向的精品化 4K 频道做好技术铺垫。

北京广播电视台 4K 二期项目融合制播网络部分是本次总体项目中涉及信息化制播系统的部分，也是对实现电视台超高清网络化节目生产起着核心作用的生产业务支撑系统部分，该部分主要包含硬件、软件、配套工程等内容。4K 二期项目融合制播网络部分将打通录制、生产、播出、发布等 4K 超高清节目生产网络化全流程，支撑起北京广播电视台冬奥纪实频道 4K 超高清节目的生产与传播。

第2节 项目需求

4K 二期项目融合制播网络部分采用云计算、人工智能、5G 等先进关键技术与 4K 超高清视频技术相结合方式，实现 4K 超高清节目的一次采集、共平台生产、多渠道发布，构建起 4K 超高清节目制作能力。

在项目中，将实现 4K 超高清节目的上载、收录、编辑、合成、转码、审查、播出、发布等全流程生产环节。同时按照北京广播电视台制播体系的整体建设规划，与全台网业务打通，实现完整

的节目流程化生产。

第3节 建设原则

4K 二期项目融合制播网络部分建设需要充分遵照北京广播电视台统一技术发展规划，既要满足本期业务需求，又要考虑到未来发展和与其他业务之间的整合对接，为此在方案设计时，要坚持以下原则：

- **遵照统一技术发展规划**

遵照全台统一技术发展规划，尽可能在原有 4K 一期和台内制播云环境基础上进行横向拓展，避免非必要重复投资。

- **采用云架构**

采用云计算、分布式计算技术，保障系统的高可用性，提高系统的敏捷性和服务能力；遵循云架构分层建设模式，在各分层间逻辑独立和充分解耦的基础上，实现层与层间的对接联动与业务高效衔接。

- **规范性**

本项目建设应遵循国家级、行业级、市级、台级各项规范及标准。

- **开放性**

平台应提供开放的接口标准，实现用户、数据统一管理，使原生工具和第三方工具能够与平台实现对接。

- **前瞻性**

平台须具备一定前瞻性，考虑技术发展趋势，并对未来新业务形态、管理模式予以充分考虑。

- **通用性**

平台软硬件应尽量满足通用性要求，开发和应用环境应采用主流软件平台。

- **安全性**

遵照《网络安全法》《信息安全技术网络安全等级保护基本要求》《信息安全技术网络安全等级保护安全设计技术要求》《广播电视安全播出管理规定》等相关法律、法规、标准、规定，建立

配套的播出安全及网络安全防护体系和应急措施，保障业务连续性和端到端安全，平台内相关软硬件应符合台内网络安全基线要求。

- **可扩展性**

平台各模块应可支持横向扩展和功能迭代，以保证平台性能和功能的高可扩展性。

- **数据规范性**

保证平台内各类基础数据的标准性、规范性和一致性，使平台具备数据化管理、运维、运营能力。

- **运维管理支持**

具备关键运维数据收集与展现能力，能够通过数据体现业务态势，辅助人工运维，保障系统的高可用性和健壮性。

- **绿色环保节能**

按照国家创建绿色节能型社会的要求，本期项目建设应充分考虑采用节能减排、绿色节能型设备。

第4节　设计依据

本项目建设过程中涉及到的技术标准如下（凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包含所有修改单）适用本文件）：

《国家信息化领导小组关于加强信息安全保障工作的意见》

《中华人民共和国国家安全法》

《中华人民共和国保守国家秘密法》

《中华人民共和国计算机信息系统安全保护条例》

《中华人民共和国计算机信息网络国际联网管理暂行规定》

《中华人民共和国计算机信息网络国际联网管理暂行规定实施办法》

国家公共安全行业标准《计算机病毒防治产品评级准则》

国家标准《计算机信息系统安全保护等级划分准则》

所有硬件设备必须符合计算机及通信专业相关的国家、国际标准，如采用工业标准或厂家自定

标准的，在投标文件中明确指出。应支持包括但不限于下列国际标准：

- IEEE 802.2/3 局域网协议标准
- IEEE 802.3ab/802.3z 千兆比以太网标准
- IEEE 802.3ab 以太网链路聚集
- IEEE 802.3ad 端口捆绑标准
- IEEE 802.1p 服务等级和优先级标准
- IEEE 802.1q IEEE 虚拟局域网标准
- IEEE 802.3Z 1000BaseX 标准
- IEEE 802.3ae 万兆以太网
- RFC 2328 OSPF 版本 2
- RFC 768 UDP
- RFC0791 网间网协议（IP） 1981.9
- RFC0792 互联网控制消息协议 1981.9
- RFC 793 TCP
- RFC0826 以太网地址解析协议（ARP）1982.11
- RFC950 IP 相关子网
- RFC922 IP 广播
- RFC1058 RIP v1 协议
- RFC1075 距离矢量组播路由协议（DVMRP）
- RFC1112 IP 组播中的主机扩展 1998.8
- RFC1155 TCP/IP 互联网的管理信息的结构和标识
- RFC1156 MIB-I
- RFC1157 简单网络管理协议（SNMP）
- RFC1212 简明 MIB 定义
- RFC1213 MIB-II
- RFC1253 OSPF MIB
- RFC1519 无类域间路由
- RFC1573 MIB-II 接口组扩展
- RFC1643 以太网链路 MIB

- RFC1661 PPP 协议
- RFC1723 RIP v2 协议
- RFC1724 RIP v2 MIB 扩展
- RFC 1757 Four groups of RMON
- RFC1812 对 IP v4 路由器的要求
- RFC1850 OSPF v2 MIB
- RFC1902-1907 SNMP v2
- RFC1983 互联网用户词汇表
- RFC 2030 Simple Network Time Protocol
- RFC2131 动态主机配置协议（DHCP） 1997.3
- RFC2236 网间网组管理协议（IGMP） 1997.11
- RFC2362 协议无关组播协议-稀疏模式 （PIM-SM）
- RFC2401 Internet 协议安全体系
- RFC2402 IP 认证头
- RFC2406 IP 安全负荷封装
- RFC2475 Diff-Serv 体系结构
- RFC2819 RMON MIB
- RFC2863 接口组 MIB
- SMPTE 2022
- SMPTE 2110
- SMPTE 2059

本次规划设计主要依据国家、国际相关标准和国际电信联盟的建议。

数字电视基础标准类

GB/T7400.11 数字电视术语

GY/T134 数字电视图像质量主观评价方法

GY/T144 广播电视 SDH 干线网管理接口协议

GY/T145 广播电视 SDH 干线网网元管理信息模型规范

GB/T17881-1999 广播电视光缆干线同步数字体系（SDH）传输接口技术规范

GY/T156-1999 有线电视广播系统技术规范

GY/T148-2000 卫星数字电视接收机技术要求

GY/Z174 数字电视广播业务信息（SI）规范

GY/Z175 数字电视广播条件接收系统（CA）规范

GB/T16649-1996 智能卡接口规范

GB/T17953-2000 4：2：2 数字分量图像信号的接口

GB/T17975.1-2000 信息技术运动图像及其伴音信号的通用编码第 1 部分系统

GB/T17975.2-2000 信息技术运动图像及其伴音信号的通用编码第 2 部分视频

GY/T 307-2017 超高清晰度电视系统节目制作和交换参数值

GY/T 315-2018 高动态范围电视节目制作和交换图像参数值

GY/T 316-2018 用于节目制作的先进声音系统

演播室参数标准

GB/T 14857 演播室数字电视编码参数规范

GB/T 17953 4∶2∶2 数字分量图像信号的接口

GY/T 155 高清晰度电视节目制作及交换用视频参数值

GY/T 156 演播室数字音频参数

GY/T 157 演播室高清晰度电视数字视频信号接口

GY/T 158 演播室数字音频信号接口

GY/T 159 4∶4∶4 数字分量视频信号接口

GY/T 160 数字分量演播室接口中的附属数据信号格式

GY/T 161 数字电视附属数据空间内数字音频和辅助数据的传输规范

GY/T 162 可升级至高清晰度电视串行接口中作为附属数据信号的 24 比特数字音频格式

B11 GY/T 163 数字电视附属数据空间内时间码和控制码的传输格式

B12 GY/T 164 演播室串行数字光纤传输系统

B13 GB/T14919 数字声音信号源编码技术规范

B14 GB/T14920 四声道数字声音副载波系统技术规范

B15 GY/T167 数字分量演播室的同步基准信号

B16 GY/T165 电视中心播控系统数字播出通路技术指标和测量方法

GY/T167-2000 数字分量演播室的同步基准信号

GY/T170-2001 有线数字电视广播信道编码与调制规范

GY/Z174-2001 数字电视广播业务信息规范

GY/Z175-2001 数字电视广播条件接收系统规范

GY/T180-2001 HFC 网络上行传输物理通道技术规范

视频编码及复用标准

GB/T 17975.2 信息技术——运动图像及其伴音信号的通用编码

MPEG-2 视频标准在数字（清晰度）电视广播中的实施准则

MPEG-2 系统标准在数字（清晰度）电视广播中的实施准则

信道编码及调制标准

GB/T 17700-1999 卫星数字电视广播信道编码及调制标准

GY/T170-2001 有线数字电视广播系统信道编码及调制规范

GY/T143 有线电视系统调幅激光器发送机和接收机入网技术条件和测量方法

GY/T146 卫星数字电视上行站通用规范

GY/T147 卫星数字电视接收站通用技术要求

GY/T148 卫星数字电视接收机技术要求

GY/T149 卫星数字电视接收站测量方法——系统测量

GY/T150 卫星数字电视接收站测量方法——室内单元测量

GY/T151 卫星数字电视接收站测量方法——室外单元测量

GY/T198－2003 有线数字电视广播 QAM 调制器技术要求和测量方法

计算机网络综合布线类

ISO/IEC 11801 商业建筑物综合布线系统国际标准

EIA/TIA 568A 商业建筑物综合布线系统美国标准

EIA/TIA 569 通信布线管线和空间设计施工标准

CECS 72:97 建筑与建筑群综合布线系统工程设计规范

CECS 89:97 建筑与建筑群综合布线工程施工及验收规范

GY/T211-2005 广播影视网络专有 IP 地址规划

以上标准如有过期或废止，以最新标准为准。

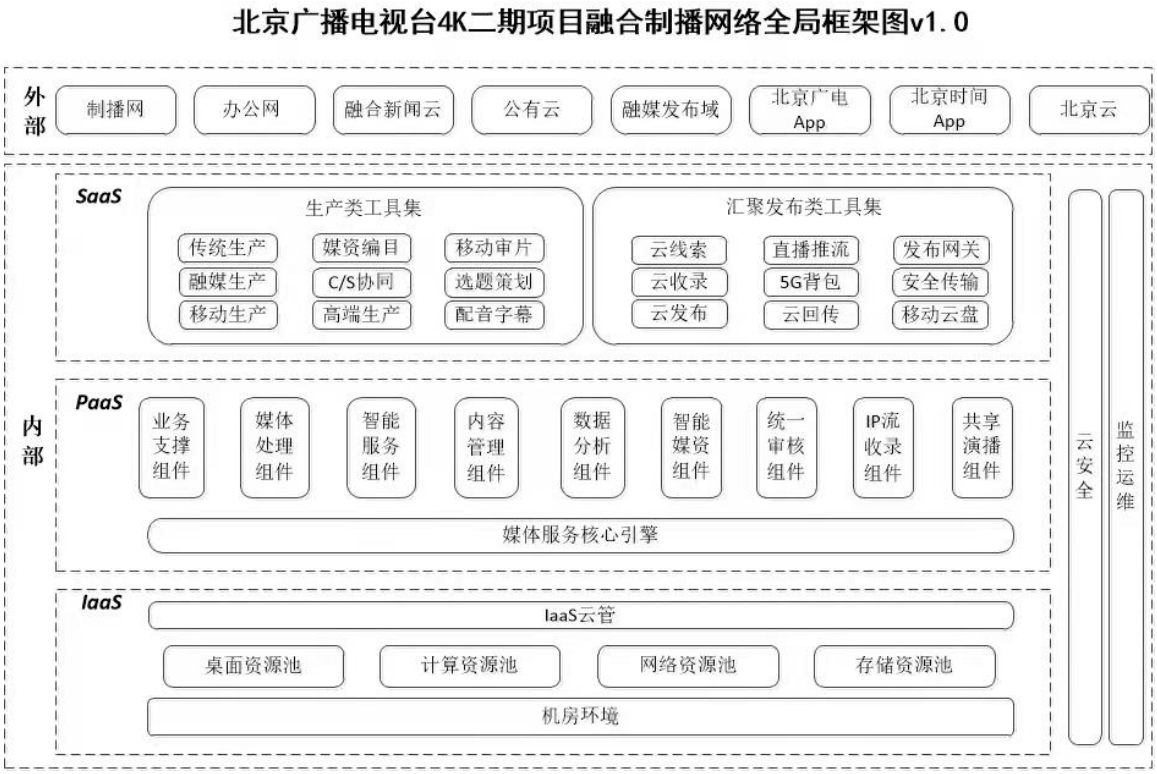
二、 总体要求

第5节　建设要求

北京广播电视台 4K 二期项目融合制播网络部分总体要求是以 4K 超高清视频技术发展为契机，进一步加强顶层设计和统筹谋划，紧抓融媒发展机遇，将内容、平台、终端、人才、资源进行深度整合，继而实现采编专业化、管理智能化、制播移动化，使北京广播电视台技术体系进一步满足 4K 超高清视频技术和融媒发展要求，构建 4K 超高清时代传媒“互联网+”的驱动模式。

本项目计划在台内现有制播云体系下进行系统建设，实现 4K 超高清制播能力扩展，并按照全台统一技术发展规划，完成配套共享性服务系统的云化改造和重构，以及 AI 智能能力的扩充与整合，并实现与高清业务系统及发布端的内容安全交换，以完整支撑 4K 超高清制播业务，从而实现 4K 超高清节目生产的信息化、智能化、移动化。

第6节　整体架构要求



北京广播电视台 4K 二期项目融合制播网络全局框架图

整个平台基于云架构模式，构建 4K 超高清汇聚、生产、发布、智能应用、移动化制播的采编播一体化服务体系，实现电视端和网络端 4K 超高清节目生产、播出、发布。如上图所示，总体架构自下而上的三个层次分别为基础资源层（IaaS）、媒体服务层（PaaS）、业务应用层（SaaS）。

1. **基础资源层（IaaS）**

IaaS 资源层通过计算资源池、存储资源池、网络资源池以及 IaaS 云管理系统构建出企业级、安全、可靠、弹性的私有云基础资源平台，实现私有云基础资源的统一管理，并将基础资源以标准服务的方式对外提供。

2. **平台服务层（PaaS）**

PaaS 服务平台起到向下对接资源，向上对接工具“承上启下”的重要作用，是体现 4K 超高清生产能力和媒体特性的关键层。本层包含媒体服务引擎，各类业务支持组件，面向内部专业用户及外部受众用户的统一用户管理，全媒体内容库，能够提供媒体公共处理能力以及智能处理能力的各类服务集合，数据分析能力，智能媒资、统一审核、IP 流收录、共享演播等配套媒体能力服务组件，以及使内部各模块和外部各系统协同工作的流程驱动引擎。在此基础上，媒体服务层可以通过服务管理系统的统一管理和串联实现平台能力的统一管控、基于媒体能力的自服务提供、基于大数据的数据分析与决策辅助、以内容和数据为核心的媒体运营支撑。

3. **业务应用层（SaaS）**

SaaS 工具集需要提供满足 4K 业务需求生产类工具以及汇聚发布类工具，满足平台用户内容策划、生产、播出、发布的业务需求，提供云端良好的使用体验。

4. **其他部分**

云安全管理模块、监控运维管理模块是平台中重要辅助模块，分别对平台的网络安全保障、运维体系建立起到重要支撑作用。

第7节　建设目标要求

1.7.1　业务目标

北京广播电视台超高清制播系统（二期）建设项目的总体目标是对现有系统进行分析梳理，根据新业务形态的需求找出其中的不足，同时积极引入新的理念与技术，建设一套集超高清节目的上载、收录、编辑、合成、转码、审查、播出以及科学的流程与人员管理为一体的冬奥纪实频道超高

清制播系统，适配北京广播电视台冬奥纪实超高清频道，打造出具备国际国内一流水平的体育节目生产与传播体系。

在业务上需要实现如下目标：

- 超高清节目制播
- 网络化、流程化超高清节目生产
- 共平台生产与多平台分发
- 智能应用与超高清生产有效结合
- 5G 移动化超高清生产

1.7.2 技术目标

通过本项目建设在技术上需要实现如下目标：

- 实现超高清视频技术应用
- 充分利用台内现有技术架构
- 实现公共服务云化
- 充分利用视音频 AI 技术应用
- 实现高效移动化生产

三、 融媒制播网络网络安全子项目要求

第8节 总体目标

北京广播电视台 4K 二期项目（第二部分）融合制播网络网络安全子项目基于融合媒体云平台网络安全防护技术体系进行建设，制定适配融合媒体环境的网络安全整体架构，为 4K 二期项目建设的云平台及所承载的应用系统提供网络安全保障措施和监测手段，结合漏洞扫描、安全加固等网

络安全服务，实现系统的等保合规并具备一定的主动防御、流量监测能力，且能够通过等保测评，为 4K 二期项目提供网络安全支撑。

网络安全保障体系架构图

1.8.1 建设要求

本项目采购产品要与现有的网络进行联调，实现网络的连通，系统的正常运行。产品功能符合设备配置要求章节中所提出的要求，能够为北京台业务提供基础的安全保障支撑。投标人在项目实施的过程包括实施方案设计、设备安装、系统联调、测试、验收交付及运行维护等过程，投标人应制定严格的实施方案，至少包括人员组织、质量控制、时间控制等关键要素。

1.8.2 业务目标

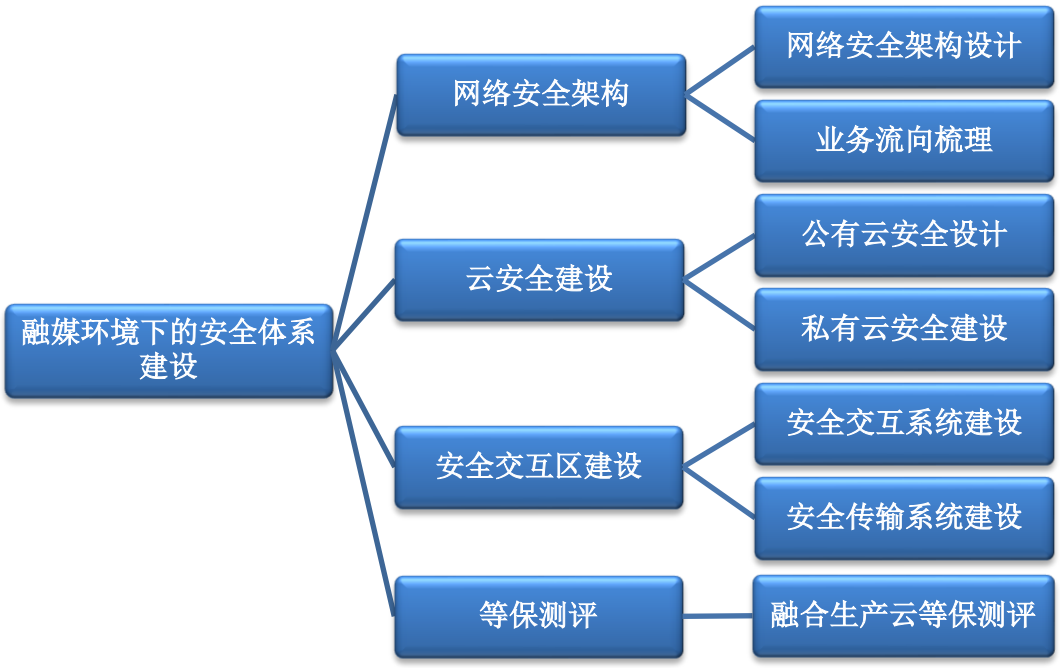
通过本项目的建设，健全和完善北京台的安全防护能力，更好的抵御内外部安全威胁，保障电视台业务有序、稳定运转。

1.8.3 技术目标

通过建设安全交互区，实现业务数据的安全传输和私有云和公有云之间数据的安全交互；通过增加边界安全设备提升办公域与生产域之间、数据中心各边界的安全防护能力；通过增加私有云内安全能力强化私有云的安全；通过对公有云进行整体安全规划增加公有云应用的安全性；通过本项

目的整体安全建设确保 4K 二期整体项目满足等保二级的安全要求。

第9节　主要建设内容



主要建设内容

为了实现网络安全子项目的总体目标，将本项目分解成了以下几个部分：网络安全架构设计、云安全设计和建设、安全交互区建设、等保测评。

网络安全架构设计主要包括网络安全架构设计和业务流向梳理，基于架构设计和流向梳理的结果，进行安全设计和安全部署，并结合整体安全设计方案对各应用系统的维护和开发提供网络安全建议和指导。

云安全设计和建设主要为了实现公有云的安全设计和私有云的安全建设。其中公有云安全主要以购买公有云安全服务为主，因此本项目只对公有云安全进行设计规划，不实际参与公有云安全服务的购买工作。私有云安全主要包括原有安全系统升级、扩容，私有云安全规划以及安全系统的建设等，确保私有云具备边界隔离、防病毒、防攻击、防渗透的能力，并满足等保的相关安全要求。

安全交互区建设主要是为了解决生产私有云与部署公有云上的融合交互域和北京时间相关业务系统进行安全高效的文件和数据交互。在保证安全的前提下实现素材和视频文件的安全快速双

向传输，此外需要根据业务类型和访问关系灵活的将不同应用引流至相应安全设备，实现安全高效的应用访问。

等保测评需要在项目实施完成后由具备等保测评资质的人员对融合生产云进行等保测评，并出具相关报告。

第10节　主要技术需求

北京广播电视台信息系统覆盖了播出、制播、办公等各个方面，随着北京广播电视台信息化和业务的不断融合，北京台形成了以办公云、新闻云、融媒云等私有云和其他公有云为基础的多云混合的融媒制播网络，这张网络已经成为北京广播电视台业务开展密不可分的基础支撑，承载了北京台大部分的信息系统。如果这张网络出现问题导致北京广播电视台的信息系统数据被篡改或服务中断，或被国内外敌对分子或其它别有用心的商业机构利用，将对北京广播电视台的经营发展和品牌形象带来严重影响。因此，北京广播电视台需要健全融媒制播网络的安全，强化各云之间、各安全区域之间的边界安全防护能力。

1.10.1　公有云安全规划

中标方应根据公有云安全服务能力，结合相关安全规范和招标方业务系统特性，对公有云提出安全要求，并提供出可行的公有云安全服务采购列表，由招标方负责从公有云进行安全服务采购。采购的安全服务可包括边界防护类、主机加固、防病毒、安全监测、堡垒机等。

中标方应负责指导招标方对采购的公有云安全服务进行配置并提供相应手段进行安全效果验证，确保招标方在公有云上的应用具备足够的安全防护能力。

投标人在投标文件中需详细描述北京广播电视台部署在公有云融媒交互区中的应用内容及类型，并根据应用类型给出安全建议，提出的公有云安全建议应具备可行性和针对性。

1.10.2　私有云安全需求

投标人应深入了解北京广播电视台 4K 二期项目所建设的融合媒体生产云平台的网络拓扑结构，了解北京广播电视台数据中心三个私有云的相互关系，并绘制出融合媒体生产云平台拓扑图，便于进行整体私有云安全方案设计。

通过本期项目建设要求私有云具备以下安全能力：横向安全隔离能力，安全监测能力，云内轻代理杀毒能力，云边界安全防护能力，统一日志收集和分析能力。为避免重复投资，结合我台现有的实际情况，本项目私有云安全建设以部分新增、部分扩容的方式进行。

1.10.2.1 私有云安全资源池扩容需求

本项目通过对安全资源池扩容实现私有云横向隔离能力的扩展，可将私有云利用安全措施划分成多个安全区域，不同安全区域间可以配置安全策略。具备统一的管理平台对安全策略进行配置，并对安全域进行管理。扩容后的安全资源池应能完美兼容现有安全资源池以及相关安全系统，扩容后可将本期项目新增的基础资源纳入到安全管理的范围内，投标人需提供整体扩容方案。安全资源池扩容的软硬件设备均由本项目采购，根据需求扩容需要增加不少于 2 台基础硬件设备，用于在不同区域部署系统并实现服务可视化展现，配置指标不低于参数要求。

序号	重要性	指标项	指标要求
1.		灵活编排	适用广泛的业务场景，同时支持东西向、南北向流量编排防护；
2.			支持多租户特性，基于 vxlan 报文的引流编排，对 overlay 报文识别区分，完成租户流量的隔离编排；
3.			一套引擎可同时支持串行链路的编排及旁路流量的复制、筛选、分发；
4.	#		支持海量的引流策略，引流表项基于哈希结构，策略数的增长不影响转发性能（需提供截图、彩页或相关证明文件）；
5.		虚拟化层	支持不占用外部网络设备资源的情况下，完成同一个物理机内不同安全组件的流量调度；
6.			支持具备分片路由能力，无需外部 SDN 交换机即可完成跨物理服务器的流量编排；
7.			支持在安全组件业务流量或资源占用到达系统设置的阈值时，动态将部分流量自动迁移到同类型的其他安全组件上；
8.		兼容性	具有广泛的兼容性，支持传统的安全设备，设备使用灵活性高，无论安全设备工作在二层或三层，均能实现自由编排，当工作在

			三层时，甚至可串联起外部已有硬件设备，对其进行编排，充分利旧；
9.			可支持适用于多种硬件架构(x86, ARM, 和 PowerPC)及部署环境(bare metal, VM, container)；
10.			支持基于 dpdk 转发技术，性能优越，针对引流的特定场景对代码做了深度优化，充分挖掘硬件性能，提供高吞吐量、低延迟、高资源利用率的 user space 网络 IO；
11.	#		为保证平滑扩容，要求云流量管理系统完全兼容现有安全管理平台，实现安全服务能力扩充； （需提供产品彩页、使用界面截图等证明文件）
12.		高可用	服务链具备高可用方案，支持负载均衡模式；
13.		部署方式	支持分布式集群部署，可简单方便地做横向扩展；
14.		基础硬件设备指标	处理器不少于 10 核，主频不小于 2.2GHz；内存不小于 32G；存储不小于 1T；具备独立显卡，支持不少于 2 个 HDMI 口；具备千兆网卡；具备调试用显示器支持全高清显示分辨率，刷新率大于 120Hz，支持 HDMI 接口。设备数量不少于 2 台。

1.10.2.2 主机自适应安全系统需求

本项目需求主要以扩容原有主机自适应安全系统覆盖范围为主，在原有系统基础上增加覆盖范围和相应授权，保证 4K 二期项目新增的计算资源能够具备能力。原有系统具备 400 个授权及一套管理平台，本期需在原有基础上增加 300 个授权并增加一套管理平台。整体安全系统需具备资产清点、入侵检测、风险评估、基线检查等功能。由于监测系统分布于多个安全域，需要提供不少于 2 台配置管理设备，配置需求不低于后续指标要求。

序号	重要性	指标项	指标要求
1		客户端要求	支持常见的 Linux 操作系统：Oracle5、Oracle6、Oracle7；

			RedHat5、RedHat6、RedHat7；CentOS5、CentOS6、CentOS7、CentOS8;Ubuntu10、Ubuntu11、Ubuntu12、Ubuntu13、Ubuntu15、Ubuntu17、Ubuntu19;SUSE11、SUSE12、SUSE13、SUSE14、SUSE15;Debian7、Debian8、Debian9、Debian10；OpenSUSE13、OpenSUSE14、OpenSUSE15。 支持常见 Windows 操作系统：Windows server 2008，Windows server2012，Windows server2016，Windows 7，Windows8，Windows10。
2			支持配置升级的时间与升级时长，且应允许配置多个时段。
3			客户端升级支持记录升级时间，对失败的主机可查看升级错误日志，并在下次升级时间自动升级。
4	#	产品安全机制	客户端具有反逆向、反调试功能、自保护功能，客户端和管理中心通信采用安全的加密机制（提供第三方机构出具的产品安全性检测报告）
5		系统管理	支持展示客户端的安装时间、当前客户端版本、最新客户端版本、启动时间、结束时间、更新状态进行展示。
6			能够支持登录产品采用 OTP 双因子认证的方式，增强重保期间账号的安全性。
7			支持自定义主机的标签和颜色，并且当主机有多个网卡时，可自定义主机 IP 显示规则，方便运维工作。
8			提供重要数据的本地数据备份与恢复功能，支持本地自动备份数据，可备份用户客户端连接数据，用户自定义数据，并导入使用。
9			支持创建子账号，创建账号时支持配置其角色、上级账户、绑定服务器，支持添加归属人、手机号、邮箱、备注等附属信息。

10			支持各类日志、安全报表、资产报表、事件报表综合下载导出，并可根据实际情况对报表内容进行自定义导出，报表支持 html、word 格式导出。
11			支持未知资产扫描发现，为防止网络扫描拥堵，扫描时应允许控制扫描速率，包括并发扫描数量，每秒最大发包数量，每次下发间隔。
12		主机资产管理	资产管理功能定期获取并记录主机上的 Web 站点、Web 容器、Web 应用、Web 应用框架、账号、计划任务、端口、数据库、进程、第三方组件、环境变量、Jar 包、系统安装包、软件应用、内核模块等信息，进行统一的管理和清点。
13			支持对服务器主机上的 Apache、Tomcat、Nginx、Weblogic、Jboss、Tongweb 等 Web 应用资产进行梳理，并支持对任意主机的特定 Web 应用资产字段进行导出。
14			支持对服务器主机上的 Mysql、SQL Server、Redis、Oracle、DB2、Hadoop 等数据库系统进行梳理，并支持任意服务器主机的特定数据库资产字段进行导出。
15			自动统计服务器单例进程、重复 UID 等存在安全隐患的资产信息
16			支持清点 Windows 系统注册表项值，选择清点其中与安全相关的重要表项值，至少包括：路径，名称，类型，数据，风险描述等。
17			支持通过自定义应用指纹，识别自研应用或未支持清点应用。
18			支持配置限制资产上报的速度，限制数据上报流量，防止造成网络拥堵。

19		安全管理	支持展示安全体检发现的补丁漏洞信息，应急漏洞模块可采集近期爆发出的高危漏洞，通过应急漏洞的检测功能对主机资产进行快速检测，确认是否有资产受到影响；支持漏洞和主机过滤，通过漏洞类型、风险等级、修复影响、影响软件、漏洞名称、等进行漏洞过滤，通过主机分组、标签、状态、内核版本等进行主机过滤；支持应急漏洞库设置，采集应急漏洞信息、统计应急漏洞总数；支持检测任务设置，可创建检查任务，设置检测漏洞及检测主机范围；（需提供补丁分布式快速扫描机制的专利证明材料，未提供视为不满足）
20			支持针对扫描出的补丁，自定义填写用户修复建议。并查看补丁的修复历史和修复工时统计信息。
21			持查看补丁修复历史，至少应记录补丁危险等级，补丁名称，所属主机，所属业务组发现时间、修复时间、修复耗时等。
22		口令账号风险	支持检测密码为空的账号、影子账号、高权限账号等。
23			展示安全体检的弱口令信息，包含弱口令的说明、风险危害以及修复建议。
24		Webshell 检测	展示安全体检和实时防护的 webshell 文件信息，包含 webshell 的类型、hash、路径，并且提供对 webshell 文件隔离、信任、下载和查看操作。
25			Webshell 支持自定义告警级别，可选择高危级别进行告警和 syslog 发送。
26		RCE 利用	可基于行为分析，检测对外服务的远程命令执行漏洞利用行为，实现实时告警和追溯。
27		反弹 shell	检测可疑的反弹 shell 进程，进程启动参数异常或进程标准输

			入、输出及错误输出被重定向到套接字。 反弹 shell 支持一键屏蔽内网反弹告警。
28		异常行为检测	支持可疑脚本执行检测，实时检查脚本内容是否包含恶意特征，并进行事件告警和处置。
29			支持采集梳理主机外连的 IP、域名情况，并进行异常的外连行为告警。
30		登录和进程异常检测	支持对服务器主机的远程登录行为进行检测，记录登录 IP 地址、账号、时间。
31	#		检测隐藏进程，在系统中查看未能发现，但实际却在系统中运行的进程 检测子进程权限比父进程更高。（需提供功能截图或产品彩页）
32		端口异常检测	可对指定主机配置指定端口作为伪装端口，但伪装端口被扫描或攻击时，则生成告警事件。支持检测和防止恶意的端口扫描。
33			应提供一键处理冲突的操作，方便用户对出现业务冲突的伪装端口进行处理，避免后续同步占用。
34		Web 入侵取证	清点 web 日志中出现的所有 url 地址，查询其访问的频率。
35			检查系统与 Web 应用登录日志中的 IP 是否有国外 IP，有则列出。
36		基线检查	可支持等级保护 2.0 的二级、三级检查、测评、整改的业务检查，系统内置官方等保 2.0 的二级、三级基线模板，满足等保二级及等保三级要求，同时支持用户自定义基线检查任务，支持导出基线检查报告。
37		应急事件调	支持查看 SSH 私钥泄漏的影响范围。

38		查	支持扫描主机上所有进程的网络连接，找到并上报具有内网隧道网络连接特征的进程，用于判断是否存在内网隧道攻击行为。
39		配置管理设备要求	具备便携移动能力，重量小于 1.15kg；处理器型号及主频不低于 Evo i7 2.8GHz；内存不小于 16G；具备千兆网卡；支持 WIFI6 无线技术；配备 SSD 硬盘，存储空间不小于 512G；支持 HDMI 输出。设备数量不少于 2 台。

1.10.2.3 运维管控设备需求

本项目所需的运维管控设备主要为实现对运维人员运维操作的安全管控。

序号	重要性	指标项	指标要求
1		基本规格	标准 2U 机架设备，冗余电源，端口数量：≥2*USB，≥4 电口；内置≥64TB 企业级硬盘,支持 raid0/1/5。
2		节点授权数量	最高支持图形连接并发≥1000 路，字符连接并发≥2000 路。
3			系统包含≥1000 个授权，最大支持≥2000 个授权。
4		部署模式	需支持物理旁路、HA 双机热备；需支持基于水平可扩展的集群化架构设计与部署。
5		发布服务器	≥1 台；硬件配置：≥4G 内存,≥300G 硬盘；内置 Microsoft Windows Server 2008 操作系统。
6		资源管理	需支持对资源及登录账户进行管理功能，包括新增、查询、修改、批量导入、导出、删除、分组等操作；
7			需支持批量导入阿里云、华为云、腾讯云、AWS、Azure 和 Ucloud 等平台云主机。

8			需支持主机资源通过 ip 地址和端口号进行自动发现功能。
9			需支持对资产账户验证功能，可设置连接超时时间；任务完成后通过邮件、短信等方式通知。
10		用户管理	需支持本地账号、USBkey、手机令牌、手机短信和动态令牌等多因子认证功能。
11		策略管理	需支持访问控制类策略管理功能，访问控制策略内容包括访问时间、ip 地址段、上传下载、文件管理、显示水印等内容；登录时间段需满足以周为单位，精确到小时级。
12			需支持对关键资源进行双人授权功能。
13		运维管理	需提供类主机网盘存储功能，支持 RDP、SSH、VNC 协议类型主机的文件上传和下载，并进行审计。
14			需支持邀请其他用户加入自己的会话进行协同操作功能。
15			需支持对工单审批管理功能，包括批准、驳回、撤销等。
16		审计管理	需支持实时会话审计管理功能，支持查看当前正在进行的会话详情、监控当前会话的操作、中断当前会话等。
17			需支持对历史会话进行管理功能，支持历史会话操作视频的在线播放和下载。
18			需支持可根据文本审计的内容为关键字进行图形搜索功能，搜索出来的结果可以直接定位到相关图形画面进行在线播放。

1.10.2.4 私有云防病毒需求

本项目所需的防病毒系统主要为实现融合生产云平台内，虚拟化层和虚拟机的防病毒。防病毒软件需支持 Windows 系统和 Linux 系统，且能够使用同一的管理平台对防病毒软件进行管控。

序号	重要性	指标项	指标要求
1.		操作系统兼容性	操作系统：Windows XP_SP3 及以上/Windows Vista/Windows 7/Windows 8/Windows 10；Windows Server 2008/Windows Server 2012/Windows Server 2016/Windows Server 2019；macOS X 10.11/macOS X 10.12/macOS X 10.13/macOS X 10.14/macOS X 10.15/macOS X 10.16/macOS X 11.0；CentOS 5~8/Red Hat Enterprise Linux 5~8； 提供不低于 600 个授权点。
2.		多终端管控	支持 Windows PC/Windows server/Linux/Mac OS 等不同操作系统使用同一控制中心同台管控，且提供对 XP 系统和 win 7 系统的安全防护能力。
3.		功能要求	产品应具备一定的扩展性，根据不同阶段的需求仅需开启对应授权即可使用更多功能，应至少支持病毒查杀、补丁管理、基线核查、软件管理、外设控制、违规外联控制、移动存储管理、安全水印、数据防泄漏、文件流转审计等功能。
4.		管控要求	产品全功能支持简体中文/繁体中体/英语自由切换。
5.			管理控制中心当登录账号输入密码错误次数超过锁定阈值后账号将被锁定，且可设置锁定时间，该时间内账号登录请求不被接受，同时应支持双因子认证登录方式，提高安全性。
6.			支持自动分组，按 IP 地址、CPU 数量、MEM 容量、主机名、计算机工作组等参数进行自动动态调整分组。
7.			支持对终端节能管理，支持对长时间运行、定时关机、空闲节能、工作时间外开机等节能类型设定策略，支持仅提示、关机、注销、锁定、关闭显示器、锁定+关闭显示器、休眠

			和睡眠处理。并支持提示倒计时弹窗，可设置在终端取消后下一次提醒时间。
8.			支持终端用户和管理员是一套账号管理系统，简化账号管理复杂度，一个账号解决所有身份认证，既可以用于终端登录，也可以用于管理管理中心。
9.		病毒防护	病毒防护概况：终端基础信息、病毒库版本、发现病毒数、未处理病毒数、最后查杀时间、文件防护状态、引擎使用状态、扩展病毒库版本
10.			病毒防护日志包含：病毒查杀日志、查杀任务日志、攻击防护日志、系统防护日志、按分组、按终端、按时间。
11.			病毒报表支持病毒查杀趋势、扫描触发方式趋势、发现病毒趋势、终端感染趋势、病毒类型统计、病毒处理结果统计、病毒发现触、方式统计、趋势图表、按分组、按终端、按病毒名称。
12.			支持手动导入、导出黑白名单，添加黑白名单。支持通过文件导入添加黑白名单。
13.			支持信任区设置，病毒扫描或实时防护时不扫描目录或文件。
14.			病毒扫描支持扫描所有文件和仅扫描程序及文档文件设置，支持对压缩包文件设置最大扫描层数和大小，当发现压缩包内存在病毒时，还需继续扫描压缩包内其他文件。
15.			支持对终端当扫描到感染型病毒、顽固木马时，扫描时不允许终端用户暂停或停止扫描任务。
16.			支持扫描资源占用设置，可设置不限制、均衡型、低资源三种模式。
17.			支持对压缩包内的病毒扫描，支持多层压缩包的扫描，可自定义配置压缩包的扫描层数，至少大约 10 层模式下的扫描。

18.			支持对进程防护、U 盘安全防护
19.			支持不少于两个杀毒引擎混合使用，提高病毒检出率。
20.		补丁管理	支持按照补丁的维度统计补丁安装情况，包括补丁号、系统类型、补丁类型、补丁级别、补丁名称、补丁描述、发布日期、漏洞 CVE 编号、漏洞 CNNVD 编号、未安装、已安装、已安装未生效、已排除、未更新补丁库。并支持导出统计报表。
21.			支持管理员预先设置好灰度发布批次和漏洞修复策略（分时间段、按级别、排除有兼容性问题的补丁等），每当控制台更新补丁库，自动化编排完成漏洞修复——将全网终端划分为由小到大的多个批次，根据企业环境，自动先推送给第一个小批次分组，如无问题自动推送给下一个批次，直到推送给全网。如有问题，只需将有问题的补丁添加到排除列表和卸载已安装的终端即可。整个推送安装过程自动化编排，无需管理员过多参与，只需在有问题时添加排除列表和下发卸载补丁任务。
22.			支持按照补丁的维度统计补丁安装情况，包括补丁号、系统类型、补丁类型、补丁级别、补丁名称、补丁描述、发布日期、漏洞 CVE 编号、漏洞 CNNVD 编号、未安装、已安装、已安装未生效、已排除、未更新补丁库。并支持导出统计报表。
23.			支持开启自动修复漏洞，包括开机时修复，并支持随机延迟执行、间隔修复和按时间段修复，可设置延迟时间、间隔修复时间和修复时间段。
24.		软件管理	支持内置软件库，需包含 1000 款以上应用软件，类别包括：下载工具、主题壁纸、办公软件、压缩刻录、图形图像、安全杀毒、教育学习、浏览器、系统工具、编程开发、网络应用、网银、聊天工具、视频软件、输入法、远程工具、阅读翻译、音乐软件等，以保证软件安装包无捆绑和病毒。

1.10.2.5 边界安全隔离需求

为保证我台数据中心私有云平台的安全，需要具备安全边界隔离功能，因此需要在边界增加安全边界隔离设备。根据部署位置和业务需求不同，需要增加如下设备：

1.10.2.5.1 千兆边界隔离 UTM 设备需求

序号	重要性	指标项	指标要求
1.		硬件规格	标准 1U 机架式设备，双电源，配置不少于 6 个千兆电口、4 个 SFP 千兆接口（含 2 个光模块）及 2 个接口扩展槽。 支持下一代防火墙访问控制、入侵防御、网络防病毒、上网行为及 URL 分类管理、流控和 IPSec VPN 模块。 提供 3 年特征库升级，3 年维保服务。
2.		性能要求	整机最大网络吞吐量不低于 16G，每秒新建连接数不少于 20 万，最大并发连接数不少于 350 万。
3.		流量管理	支持基于地区维度设置流控策略，实现多区域流量批量快速管控功能。
4.		访问控制	支持基于接口/安全域、地址、用户、服务、应用和时间的防火墙访问控制策略。
5.		链路负载	支持多链路智能选路，根据业务对抖动、时延和带宽的要求，在多条不同链路上智能动态选路，通过自动重传技术，实现链路切换时无丢包，业务不掉线。
6.			支持通过 ICMP、TCP、DNS 和 HTTP 协议实现对链路可用性的多重健康检查。
7.		网络特性	支持透明、路由、混合、旁路等部署模式。
8.			支持静态路由、动态路由（RIP、OSPF、BGP4）。

9.			支持 DNS 透明代理功能，可将指定范围内的 DNS 请求自动重定向至管理员指定的 DNS 服务器，且支持多台 DNS 服务器的负载均衡。
10.			支持基于入接口、源地址、目标地址、服务端口、应用类型、域名的策略路由。
11.			支持源 NAT、目的 NAT、静态 NAT，支持一对一、一对多和多对多等形式的 NAT。
12.		高可用性	支持主-主和主-备模式，主备模式下支持基于设备优先级的主设备抢占功能。
13.		威胁情报	支持基于威胁情报云的动态防护功能，防火墙支持将用户对互联网的访问信息发送至威胁情报云进行实时情报查询及防护。
14.		策略管理	支持防火墙集中管理，包括统一状态监控、配置下发、配置自动备份及回滚、版本统一升级、特征库统一升级等功能。

1.10.2.5.2 万兆边界隔离 UTM 设备需求

序号	重要性	指标项	指标要求
1		硬件规格	标准 2U 机架式设备，冗余双电源，配置不少于 6 个千兆电口、4 个 SFP 千兆接口、2 个 SPF+万兆接口（含光模块）。 支持下一代防火墙访问控制、入侵防御、网络防病毒、上网行为及 URL 分类管理、流控和 IPSec VPN 模块。 提供 3 年特征库升级，3 年维保服务。
2		性能要求	整机网络最大吞吐量不低于 25G，每秒新建连接数不少于 25 万，最大并发连接数不少于 600 万。

3		流量管理	支持基于地区维度设置流控策略，实现多区域流量批量快速管控功能。
4		访问控制	支持基于接口/安全域、地址、用户、服务、应用和时间的防火墙访问控制策略。
5		链路负载	支持多链路智能选路，根据业务对抖动、时延和带宽的要求，在多条不同链路上智能动态选路，通过自动重传技术，实现链路切换时无丢包，业务不掉线。
6			支持通过 ICMP、TCP、DNS 和 HTTP 协议实现对链路可用性的多重健康检查。
7		威胁情报	支持基于威胁情报云的动态防护功能，防火墙支持将用户对互联网的访问信息发送至威胁情报云进行实时情报查询及防护。
8		策略管理	支持防火墙集中管理，包括统一状态监控、配置下发、配置自动备份及回滚、版本统一升级、特征库统一升级等功能。

1.10.2.5.3 边界应用防护设备需求

序号	重要性	指标项	指标要求
1.		硬件规格	标准机架式设备、双电源，配置不少于 1 个 HA 口，1 个 RJ-45 Console 口，不少于 1 个 10/100/1000 Base-T 带外管理口以及 4 个万兆 SFP+接口（含 2 个多模光模块）。 提供 3 年特征库升级，3 年维保服务。
2.		性能要求	网络层吞吐率大于 8G；HTTP 吞吐量不少于 1G；HTTP 最大并发连接数≥35 万；HTTP 最大新建连接数≥3.2 万；TPS 每秒事务处理数≥5 万；业务时延小于<50ms。

3.		高可用	支持集群模式、主-主模式、主备模式、硬件 BYPASS、软件 BYPASS
4.		Web 攻击防护	支持源地址识别，部署在 SSL 网关后面，能够解析到真实的访问者 IP，并能对真实的 IP 进行防护和阻断
5.			支持多条链路数据的防护，防护网段数量不限
6.			支持 ipv4/ipv6 双协议栈
7.			支持自定义 Web 应用防护规则，通过基于正则表达式自定义规则匹配方向、动作、字符串、危险等级、动作、攻击影响、描述等。
8.			支持 CC 攻击防护，支持自定义来源 IP、Referer 防 CC 的次数限制、检测时间和出发阈值，支持特定 URL 防 CC 次数限制和检测时间。
9.			支持防护 Java 反序列化及基于 Java 的通用攻击
10.			应具备业务合规功能，可对业务进行恶意试探、恶意撞库、恶意登录等行为进行检测及拦截。
11.			可基于时间设置对客户端 IP 放行、阻断或检测
12.		Web 安全事件统计分析与报表	应具备 Web 安全事件的报表功能，支持一般的单一条件报表输出、专业的多维度统计报表输出。
13.			应具备自定义报表功能，并支持导出为 WORD\EXCEL\PDF \HTML 等常用公文处理格式。
14.		系统管理	应支持 B/S 管理方式 Web 管理界面。
15.			应具备多设备拓扑显示功能，可以在界面上以图形化的方式显示当前的部署拓扑。

1.10.2.6 日志审计设备需求

为满足等保合规要求，并且具备一定的可追溯能力，需要在我台融合生产云平台和办公云平台增加日志审计系统，由于两个云平台间采购强安全隔离措施，需要部署两套日志审计系统。

序号	重要性	指标项	指标要求
1		硬件规格	2U 标准机架式，冗余电源，专用千兆硬件平台和安全操作系统，配置不少于 6 个千兆电口，不少于 4 个 SFP 千兆接口（含光模块）及 1 个可扩展插槽，不少于 2 个 USB 接口，存储容量 4TB。配置 200 个审计对象授权。
2		功能授权	通过主被动结合的手段，实时不间断地采集用户网络中各种不同厂商的安全设备、网络设备、主机、操作系统、以及各种应用系统产生的海量日志信息，并将这些信息汇集到审计中心，进行集中化存储、备份、查询、审计、告警、响应，并出具丰富的报表报告，获悉全网的整体安全运行态势，实现全生命周期的日志管理。
3		性能要求	产品要求集成数据库，无须再独立安装数据库系统，亦无须对数据库进行专门的维护。
4		运行环境	产品要求至少能够部署在 Windows 和 Linux 操作系统上。
5		日志采集	无需另外安装软件组件，管理中心即可通过 SNMP Trap、Syslog、ODBC\JDBC、文件\文件夹、WMI、FTP、SFTP、NetBIOS、OPSEC 等多种方式完成日志收集功能；可灵活定制不支持的数据源采集，而无须改动代码。
6		日志转发	支持对单个/多个日志源批量转发，支持定时转发，可通过 syslog

			和 kafka 方式转发到第三方平台，并且支持转发原始日志和已解析日志的两种日志。
7		日志范式化	系统必须具备日志范式化功能，实现对异构日志格式的统一化。
8		日志过滤	要支持对无用日志的自动过滤，减少垃圾数据数量；可以建立日志过滤条件;过滤条件可以按照所有范式化后的字段属性来定义。
9		事件分析	可以显示一段时间的动态日志移动图，能够在图上显示每个时间切片的日志数量、等级，并能够在图上显示每秒事件数。
10		告警管理	告警动作支持告警重定义、弹出提示框、播放警示音、发送邮件、发送 SNMP Trap、发送短信、执行命令脚本、设备联动、发送飞鸽传书、光告警、发送 Syslog、设置观察列表等方式。
11		报表管理	系统内置了资产、事件、监控、风险等报表报告，且内置报表编辑器，可以自定义报表。
12		实施要求	要求投标人实施人员能够对产品进行配置调整和日志分析，具备具备中国信息安全测评中心颁发的国家注册信息系统审计师（CISP-A）、人力资源和社会保障部、工业和信息化部联合颁发的系统规划与管理师证书，需提供证书复印件及由投标人缴纳的至投标截止时间止近三个月以来任意 1 个月社保证明材料，并加盖投标人公章。

1.10.2.7 漏洞修复系统需求

为解决我台部分操作系统无法进行补丁升级的问题，需要采购相关软件实现操作系统的漏洞修复，减少操作系统层面的安全风险。

序号	重要性	指标项	指标要求
1		服务器部署	管理端支持 LINUX、CENTOS7.0 以上版本操作系统及 docker 环境部署，授权数量不低于 1000 个。
2		客户端部署	客户端支持部署在 Windows XP_SP3 及以上/Windows Vista/Windows 7/Windows 8/Windows 10 操作系统
3			客户端支持部署在 Windows Server 2003SP2/2008/2012/2016/2019 操作系统
4			支持域控推送统一部署，对终端用户权限无要求。支持通过传加密参数的方式提权到管理员权限来安装。
5			支持 web 安装、离线包安装、邮件、OA 等通讯方式通知给终端用户
6		系统管理	管理端采用 B/S 架构管理端，具备设备分组管理、策略制定下发、全网健康状况监测、统一杀毒、统一漏洞修复、终端软件管理以及各种报表和查询等能力
7		首页	支持展示动态信息，如：全网扫描，漏洞修复趋势、终端系统品牌，浏览器型号等
8			支持展示授权终端的数量、授权期限、接入终端数量、通信质量，支持展示离线在线终端饼状图，支持详情展示终端详细信息
9			按平台 统计及管理每个模块的终端授权使用数量，通过授权文件指定功能模块的开始、结束时间，授权数量，过期的授权，对应的功能将不能管理或减少管理数量

10		任务管理	支持按照终端任务完成百分比判断是否正常执行管理员下发任务
11			支持管理员取消下发的任务，避免终端上线后继续执行此任务
12		漏洞免疫	产品具备微补丁免疫技术，可直接避免漏洞本身被攻击利用。
13		自动化运维	支持将全网终端划分到多个时间段依次分批补丁安装，避免集中下载补丁，造成网络干路拥塞
14		精细化运维	支持自定义漏洞修复时间，可添加多条补丁修复策略，可按照周、日、时间定义补丁安装完成后提示重启/自动重启，包含提醒一次、自定义间隔时间提醒、自动重启、规定时间内重启
15		停服系统	支持针对已经停服的系统（包含 winxp、win7、server2003、server2008 等后续停服的系统），给出升级建议，管理员可以根据建议升级系统，避免被漏洞利用攻击
16		漏洞发现能力	要求产品生产厂商具备面向微软官方级别漏洞发现能力
17		漏洞检测	针对高危漏洞提供非补丁安装层面免疫功能，部署后进行第三方漏洞扫描检测
18		蓝屏修复	支持漏洞蓝屏修复功能，当安装系统补丁出现蓝屏时，可快速修复系统
19		漏洞报表	支持按照自定义的日期展示漏洞处理结果，以数据图形展示，如：趋势图，饼状图

1.10.3 安全交互区需求

安全交互区是本项目建设的实现公有云与私有云安全交互的区域，通过该区域可以在满足安全要求的情况下实现公有云与私有云的互联互通。安全交互区可以接入多个公有云和私有云，通过池化边界安全系统实现公有云与私有云的南北向访问，并对公有云之间和私有云之间的访问进行隔离；利用安全传输系统实现文件的传输并对传输的文件进行全自动的病毒查杀。

投标人需深入了解北京广播电视台内部办公云、融媒云、新闻云三个私有云现状以及与公有云的关系，整理全网架构图，结合架构图进行整体方案设计。

安全交换区的建设分为两个部分：池化边界安全系统建设、安全传输系统建设。中标方需为北京广播电视台 4K 二期项目在公有云内建设的业务系统与私有云内的业务系统提供完整的安全交互方案，该区域涉及的所有网络设备、安全设备和相关配件均由本项目采购并由中标方进行实施。安全交互区采用全万兆互联方式，所有设备均应具备万兆接口。安全交互区内采用主备链路的设计方案并且内部的安全设备支持断电直通功能，保证单一设备故障不会对整体链路的安全性和联通性造成影响。安全交互区的方案需要在保证连通性的前提下针对应用访问和文件传输分别指向不同的路径并分配不同的安全策略。安全交互区中应用交互链路须使用池化的安全方案，不可采用将多个安全设备简单串联的方式，确保用户可以根据应用类型的不同灵活定义服务链，使业务流量能够经过或跳过某个安全设备。单个安全设备的性能不能对整体链路的性能造成影响。

1.10.3.1 池化边界安全系统需求

利用池化安全系统部署在安全交互区的应用交互链路中，实现多个公有云和私有云间安全的应用交互。链路中所有设备采用全万兆互联，且不能由于单一安全模块的性能不足而影响到整个系统的效率。池化安全设备需同时具备（不限于）防火墙、防毒墙、IPS、WAF 等安全能力，且能够与安全交互区的数据安全传输系统进行对接并需要在投标文件中详细描述对接方案。

★ 安全交互区中应用交互链路需采用池化安全方案，不可采用将多种安全设备简单串联的方案。池化安全系统具备定义数据流表的能力，能以服务链的方式实现数据在各安全功能模块间灵活调用。

序号	重要性	指标项	指标要求
1		硬件指标	标准 3U 机箱，1 个管理口，1 个 HA 口，1 个 Console

			口，2 个 USB，≥8 个扩展板卡插槽，≥8T 硬盘，液晶屏，冗余电源， 含三年硬件维修服务。
2		系统吞吐量	网络层吞吐量≥240Gbps，最大并发连接数≥1 亿，每秒新建数≥150 万，支持 IPSec 隧道数≥8000，SSL VPN 并发用户数≥1000。
3		安全组件	采用池化安全方案，所提供的池化安全系统至少包含下一代防火墙、入侵防御、网关防病毒、web 应用防护功能。（投标文件需要提供能够体现上述功能及配置选项的截图）
4		网络协议	支持 VTEP（VxLan Tunnel EndPoint）模式接入 VxLAN 网络，并可作为 VXLAN 二层、三层网关实现 VxLan 网络与传统以太网的相同子网内、跨子网间互联互通；支持通过绑定 VLAN、VNI（VXLAN Network Identifier）、远程 VTEP，手动管理 VxLan 网络；支持 MAC、VNI、VTEP 静态绑定；
5			支持 MPLS 流量透传；支持针对 MPLS 流量的安全审查，包括漏洞防护、反病毒、间谍软件防护、内容过滤、URL 过滤、基于终端状态访问控制等安全防护功能；
6			支持 MTU≥9000byte 的巨型帧 Jumbo Frame ；
7		路由策略	支持基于策略的路由负载，支持根据应用和服务进行智能选路，支持源地址目的地址哈希、源地址哈希、轮询、时延负载、备份、随机、流量均衡、源地址轮询、目的地址哈希、最优链路带宽负载、最优链路带宽备份、跳数负载等不

			少于 12 种路由负载均衡方式，支持基于 IPv4 或 IPv6 的 TCP、HTTP、DNS、ICMP 等方式的链路探测，同时 TCP 与 HTTP 可使用自定义目标端口进行测试；
8		地址转换	支持全面的 NAT 转换配置，包括一对一，一对多，多对一的源、目的地址转换，并至少支持 FULL_CONE 模式和 SYMMETRIC 模式；
9			支持在源地址转换过程中，对 SNAT（源地址转换）使用的地址池利用率进行监控，并在地址池利用率超过阈值时，通过 SNMP Trap、邮件、声音、短信等方式告警。
10			支持 DDNS 功能，支持 Oray 向日葵、Pubyun 公云、Noip、Changeip 提供的 DDNS 服务，将动态获取的 IP 地址映射为固定的域名(投标文件需提供能够体现上述功能配置截图或证明文件)；
11		高可靠性	池化边界安全系统需采用两台以上设备进行集群部署，具备双机或多机热备能力，保证系统可用性，且主备切换不影响整体性能。 支持路由模式、透明模式的 HA 高可靠性部署，可工作于主备、主主模式，会话、用户、配置可实时同步；HA 高可靠性部署支持接口联动，某个端口失效（DOWN），属于同一接口组中其他端口都会进入失效状态（DOWN）；HA 高可靠性部署支持配置接口权重；支持链路探测；
12		应用识别与控制	支持应用识别，应用特征库包含的应用数量（非应用协议的规则总数）大于 2800 种，可深度识别

			每种应用的属性，为每种应用提供预定义的风险系数，并将应用基于类型、使用场景、数据传输、风险等级等特征分类；
13			支持上传、下载、双向的文件内容过滤；内容过滤支持手工及文件批量导入两种方式进行敏感信息定义；内容过滤至少支持 html、doc、docx、xls、xlsx、ppt、pptx、chm、7z 等 30 种常见文件类型；文件类型识别基于文件特征而非扩展名，更改文件扩展名后仍可有效识别；
14		网络适配	支持 vlan、vxlan 数据解包引流至虚拟安全 VNF 网络
15		VNF 系统总览	支持 NFV 资源调配功能，分配比例有 0%、25%、50%、75%；支持 NFV 资源监控功能（CPU、内存、硬盘）；支持显示 VNF 状态（运行中、告警、已关机）；
16	#		支持 PNF 功能，能够按照业务需求将其他物理设备编排到服务链中，实现优化业务流量功能；支持物理接口、物理子接口、聚合接口、聚合子接口设置为服务链模式；支持旁路和串联工作模式，支持定义内外网接口，支持针对 PNF 健康检查（链路探测、回环探测、接口探测）。（需提供针对本项目该功能需求的第三方测试报告，并加盖原厂公章）
17			支持 VNF 监控，显示 VNF 的规格，网络接口信息等，并支持跳转到具体的 VNF 组；支持展示 VNF 告

			警信息，显示告警时间、严重性、告警信息；
18		引流策略	支持引流策略的添加、删除、调序、清除命中数、刷新功能；支持引流策略的启用和禁用功能。
19	#		支持灵活的细粒度引流策略，可基于源安全域、目的安全域、源用户、源地址、目的地址、服务、VLAN、服务链、流量方向（内网到外网/外网到内）。（需提供针对本项目该功能需求的第三方测试报告，并加盖原厂公章）
20		VNF 类型	支持 VNF 健康检查，以及故障 bypass 能力；支持 VNF 按照来源分类显示，包括内置 VNF、自定义 VNF；支持自定义添加 VNF，包括自定义类型、协议类型、规格(CPU/内存/数据盘)等；支持自定义 VNF 时定义 VNF 类型为【主机模式】的部署模式；
21	#	VNF 组	支持以列表形式显示 VNF 组、VNF 类型、规格、组负载均衡算法、网络模式、业务网络、组成员状态（运行、关机、异常）、引用（引用模块）、操作（删除、编写、查看）；支持 VNF 免密登录；（需提供针对本项目该功能需求的第三方测试报告，并加盖原厂公章）
22			支持 VNF 的 web 控制台管理、重启、开机、关机、删除、编辑、查看操作；支持查看各 VNF 的详细规格信息和镜像信息；支持监控 VNF 的每个核的利用率，网络接口的 IP 地址，各接口实时流量（发送速率、接收速率）；

23			支持配置 VNF 业务网络和高性能模式。
24	#	服务链管理	支持灵活的服务链编排功能，支持 PNF 和 VNF 的混合编排，支持串接链和旁路链，支持网元组的方向和位置设置。（需提供针对本项目该功能需求的第三方测试报告，并加盖原厂公章）
25			支持 VNF 开关，决定流量是否发送 VNF。
26		VNF 镜像	支持镜像类型的快速分类筛选；支持安全 VNF 镜像版本管理，包括新增、删除等；
27			添加镜像时支持配置 VNF 类型、产品版本、上传方式（本地、FTP、TFTP）、引导方式（BIOS、UEFI）、网卡多队列、磁盘驱动（virtio、ide,scsi）、网卡驱动（virtio、e1000）。
28		网络攻击防护	支持基于不同安全区域防御 DNS Flood、HTTP Flood 攻击，并支持警告、阻断、首包丢弃、TC 反弹技术、NS 重定向、自动重定向、手工确认等多种防护措施；
29		病毒防护	所投产品必须能够对 HTTP/FTP/POP3/SMTP/IMAP/SMB 六种协议进行病毒查杀；本地病毒库规模大于 3000 万
30		入侵防御	支持漏洞防护功能，同时将漏洞防护特征库分类，至少包括缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL 注入、WEB 攻击等六种分类；漏洞防护支持日志、阻断、放行、重置等执行动作,可批量设置针对某一分类或全部攻击签名的执行动作；支持基于 FTP、HTTP、IMAP、

			OTHER_APP、POP3、SMB、SMTP 等应用协议的漏洞防护；
31			支持在设备漏洞防护特征库直接查阅攻击的名称、CVEID、CNNVDID、严重性、影响的平台、类型、描述等详细信息；
32	#		所投产品的漏洞防护特征库包含高危漏洞攻击特征，至少包括“永恒之蓝”、“震网三代”、“暗云 3”、“Struts”、“Struts2”、“Xshell 后门代码”以及对应的攻击的名称、CVEID、CNNVDID、严重性、影响的平台、类型、描述等详细信息；（提供功能截图证明并加盖原厂公章）
33			支持自定义 TCP、UDP、HTTP 协议的漏洞特征，漏洞特征可通过多个字段以文本或正则表达式的形式进行有序和无序匹配，并可自定义漏洞的源、目的端口范围；同时可标识自定义漏洞的 CVE 编号或 CNNVD 编号。
34			支持自定义基于 TCP、UDP、HTTP 协议的间谍软件特征。间谍软件特征可通过多个字段以文本或正则表达式的形式进行有序和无序匹配；并可自定义间谍软件的源、目的端口范围；
35		WAF	产品具备 SQL 注入、XSS 跨站攻击防御策略，支持特征检测与语义算法检测（提供功能截图证明并加盖原厂公章）
36			产品具备 Web 业务加固防御功能，提供人机识别、

			弱密码检测、会话安全、CGI 安全、跨站请求伪造以及业务流程控制的防御功能（提供功能截图证明并加盖原厂公章）
37			产品具备敏感信息检测防护，检测类型包括：中间件信息保护，数据库信息保护，敏感文件保护，代码错误信息保护，隐私信息保护（提供功能截图证明并加盖原厂公章）
38		SSL 解密	支持 IPv4 和 IPv6 流量的 HTTPS 协议进行解密，支持配置基于源安全域、目的安全域、源地址、目的地址、SSL 协议服务的解密策略，并可同时基于安全域、IPv4 和 IPv6 地址进行例外设置；（提供功能截图证明并加盖原厂公章）
39		IPSec VPN	支持支持 IPSec VPN 功能，支持基于主模式（Main Mode）、积极模式（Aggressive Mode）、国密三种协商模式建立的网关-网关加密隧道；支持本地 CA 并可为参与 IPSec VPN 隧道建立的设备颁发用于身份认证的证书；
40		网络异常感知	支持基于主机或威胁情报视图，统计网络中确认被入侵、攻破的主机数量，至少可查看被入侵、攻破的时间、威胁类别、情报来源、威胁简介、被入侵、攻破的主机 IP、用户名、资产等信息；并对威胁情报发现的恶意主机执行自动阻断；
41			支持基于主机或威胁情报视图，统计网络中存在安全风险的主机数量以及对应的风险等级，至少可查看遭遇风险的时间、威胁类别、情报来源、

			威胁简介、失陷主机 IP、用户名、资产等信息；
42		策略与处置	所投设备可在单条策略中启用病毒防护、入侵防御、网址过滤、文件过滤、文件内容过滤、终端过滤等安全功能选项。
43			支持基于受害主机的一键式阻断链接、记录日志等处置动作，处置周期至少包括 1 天、7 天、30 天、90 天、永久等。

1.10.3.2 安全传输系统需求

安全传输系统由防病毒引擎模块、对象存储模块、网络交互模块等模块组成，需要实现公有云与本地私有云业务之间大文件安全传输。安全传输系统产品形态为软硬一体化设备，设备内置各个功能模块，紧耦合架构。安全传输系统在整个杀毒过程中可进行一次落地并提供不少于三种杀毒引擎的查杀，满足短周期内混合云间业务交互数据的杀毒及高效传输需求。

安全传输系统所包含的所有软硬件均在本项目采购并由设备厂商和集成商进行整体方案的设计和实施，方案应能与池化边界安全系统相结合，实现安全交互区的整体功能需求。

★ 安全传输系统能够根据安全逻辑划分为对应区域，数据写入安全传输系统后，需要自动调用内置安全检测与处置引擎对写入的数据进行病毒查杀及检测，需支持数据杀毒结果及文件数据状态、存储路径主动推送到第三方应用或被动获取。

序号	重要性	指标项	指标要求
1		硬件及资源要求	本次采购为分布式安全传输系统，节点数不少于 3 个； 单台硬件平台资源要求： 规格：2U

			CPU≥2 颗 Silver 4210R 2.4GHz（10C）； 内存≥4*32GB DDR4 2666； 系统盘≥2*240GB SATA SSD； 缓存盘≥2*1.92T； 数据盘≥10*10T； 冗余电源； 接口≥4 千兆电口，6 万兆光口（满配光模块） 提供不少于 300T 存储授权。 包含 3 年硬件质保，3 年系统软件升级
2			本次采购分布式安全传输系统节点间互联网络交换机，为保证兼容性，与分布式安全传输系统同品牌，数量不少于 2 台； 单台网络交换机硬件配置资源要求： 10G SFP+光口≥24 个，40GE QSFP+光口≥2 个，万兆光模块及光纤线≥18 个，配备冗余电源。交换容量不小于 2.5Tbps/23Tbps，包转发率不小于 720Mpps。 支持全端口线速转发。 包含 3 年硬件质保，3 年系统软件升级。
3		分布式安全传输系统存储要求	为保障业务数据安全性，分布式安全传输系统需内置安全检测与处置引擎模块，不接受部署在外置第三方服务器上的安全检测与处置引擎。支持对上传至平台数据的病毒查杀及检测能力，提供不少于三种杀毒引擎对文件进行查杀，有效抵御以勒索病毒为典型的各种病毒。为保证兼容性，分布式安全传输系统与安全检测与处置引擎需为相同品牌。（针对以上功能需提供有效证明材料并加盖厂商公章。）
4			安全引擎对于病毒的查杀结果保存在分布式安全传输系统内，并

			支持以标准的 API 接口或者界面的方式展示查杀结果。
5			数据写入分布式安全传输系统之后，自动调用安全引擎对写入的数据进行病毒查杀，无需任何的外部调用或者人工干预。
6			分布式安全传输系统采用全对称式分布式架构设计，无独立元数据节点。平台数据读写性能随节点数量的增加而近线性提升。提供多控制器负载均衡及故障自动切换功能。
7			分布式安全传输系统要求提供 SAN、NAS+Object 统一存储能力，一套系统并发提供 iSCSI、NFS、CIFS、S3、Swift 服务，实现对台外或第三方人员终端及上层系统的统一对接，具备普式兼容及泛化连接。可实现三节点情况下同时提供块、文件、对象存储服务，落地资源可灵活分配，统一管理。
8			提供统一容量授权，容量授权不区分块、文件、对象存储服务。可灵活分配容量授权到不同存储需求。同时提供块/文件/对象三种存储服务时，可实现单节点损坏和单磁盘损坏存储系统依然可读写，且性能稳定
9	#		配置海量小文件高性能处理功能，支持百亿级海量小文件的高性能处理，可以实现 100 亿小文件高速写入，且性能衰减不超过 5%。提供具备 CNAS(中国合格评定国家认可委员会)认证的三方权威评测机构签字盖章的测试报告并加盖原厂公章。
10			提供高性能块存储，可实现单节点（配置 2 块 960GB SSD，两副本）提供至少 10 万 IOPS。集群可实现线性增长，三节点满足 30 万以上 IOPS 处理能力。
11			文件存储要求配置目录配额管理功能，支持容量和文件数配额。
12			支持一键检测功能，支持用户自行检测系统健康状态，检测包括 CPU、内存、硬盘、网口等硬件故障、告警等问题，同时支持检测

			各类存储服务是否正常启动。针对问题能够提出解决推荐办法。
13			存储拓扑，支持存储拓扑功能，展示块存储当前授权服务器和 LUN 之间的对应关系方便用户查看以及故障定位。
14		病毒防护能力要求	分布式安全传输系统底层安全检测引擎具备基于人工智能的检测引擎，有效应对恶意代码及其变种。
15			提供对分布式安全传输系统落地文件的实时监控，提供布式数据安全平台协议网关的定制化识别能力，接收基于用户需求的定制化素材文件病毒查杀请求，对素材文件病毒进行查杀，威胁文件自动处置。
16			支持针对分布式安全传输系统中流文件格式进行定制化检测协议识别优化，有效提升大文件检测效率。
17			具备针对最新未知的文件，使用 IOC 特征（文件 hash、dns、url、ip 等）的技术，进行云端查询。
18	#		支持安全策略一体化配置，通过一条策略即可实现不同安全功能的配置，包括：终端病毒查杀的文件扫描配置、文件实时监控的参数配置、webshell 检测的检测和威胁处置方式、暴力破解的威胁处置方式和信任目录。(提供具备中国合格评定国家认可委员会和中国计量认证的第三方测评机构出具的测试报告，并加盖原厂公章）
19			支持本地查杀缓存，具备二级缓存机制：终端侧使用全盘文件缓存，加速本地二次扫描速度，减少对本地虚拟化环境的资源消耗；管理平台侧使用全网文件缓存，加速云查杀速度，减少通过互联网进行云查杀的带宽消耗。
20			支持对上传到数据平台的 zip， rar， jar， cab， 7z 等常见压缩文件进行扫描检测，支持压缩文件层级进行策略配置，最大可

			配置检查 10 层压缩文件。
21			可实时监控文件的状态，在文件读、写、执行或者进入数据安全交换平台时主动进行扫描，支持根据用户性能偏好设置高、中、低 3 种防护级别。
22			基于勒索病毒攻击过程，建立多维度立体防护机制，提供事前入侵防御-事中反加密-事后检测响应的完整防护体系，展示勒索病毒处置情况，对勒索病毒及变种实现专门有效防御。
23	#		支持监控诱饵文件，诱饵文件可被实时监控，当勒索病毒对该文件进行修改或加密操作时进行拦截。（提供具备中国合格评定国家认可委员会和中国计量认证的第三方测评机构出具的测试报告，并加盖原厂公章）
24			支持用户直接对勒索病毒的家族名、病毒名、加密文件后缀名执行链接查询，可通过直接上传加密文件的方式确定勒索病毒类型，如果能解密可以提供必要的解密工具。
25			提供挖矿病毒巡检工具，支持通过内存、进程和启动项来检索病毒相关信息。
26	#	文件安全传输要求	隔离分区： 分布式安全传输节点支持创建隔离分区，每个隔离分区支持自定义命名并设置相应的网段，隔离分区可划分为可信区、不可信区、病毒区。每个隔离分区支持设置不同的分区访问权限，可通过 HTTPS 协议对接前端业务系统。支持入站和出站方向分别设置各自的多组隔离分区。(提供产品功能截图，并加盖原厂公章)
27	#		数据安全摆渡:支持上传到分布式安全传输节点的数据自动存储在不可信隔离分区，并与其他分区进行隔离，同时触发分布式安全传输节点内置的防病毒引擎进行并发数据扫描，上传的数据未发现病毒或恶意程序后自动将数据安全摆渡到信任分区；上传的

			数据如发现病毒或其他恶意程序后自动将病毒数据摆渡到病毒分区并进行隔离。整个数据安全摆渡过程对前端业务系统以透明无感知的方式进行，且数据摆渡方式为安全逻辑迁移，不改变数据实际物理位置，以便提高数据摆渡效率。（提供数据安全摆渡的详细技术原理说明，并加盖原厂公章）
28	#		杀毒结果联动： 分布式安全传输节点支持杀毒结果和文件数据状态的通知，支持以推送、标准 API 接口等多种方式与前端业务系统联动，可将数据杀毒结果及文件数据状态、存储路径通过 HTTP URL 的方式推送到第三方应用，也支持第三方应用通过分布式安全传输节点 API 接口进行杀毒结果和文件数据状态、存储路径的获取。支持配置自定义通知目标，以及默认缺省的通知目标。（提供详细的技术原理说明并加盖原厂公章）
29	#	实施要求	实施人员具备中国信息安全测评中心颁发的国家级渗透测试专业认证（CISP-PTE）和工业和信息化人才专业知识测评证书，提供认证证书复印件及由投标人缴纳的至投标截止时间止近三个月以来任意 1 个月社保证明材料，并加盖投标人公章。

1.10.3.3 安全交互区交换机需求

1.10.3.3.1 千兆边界交换设备需求

序号	重要性	指标项	指标要求
1		配置要求	≥48 个 10/100/1000BASE-T 端口，支持≥4 个 10G/1G BASE-X SFP+端口；支持≥1 个扩展槽；交流供电，双电源

2			交换容量≥756Gbps；包转发率≥252Mpps；
3			支持基于 MAC/协议/IP 子网/策略/端口的 VLAN
4			支持对端口接收和发送报文的速率进行限制；支持基于队列限速和流量整形的功能
5		端口聚合	支持 GE 端口聚合,支持 10GE 端口聚合,支持 40G 聚合,支持静态聚合,支持动态聚合, 支持跨设备聚合
6		端口特性	支持 IEEE802.3x 流量控制（全双工）,支持基于端口速率百分比的风暴抑制,支持基于 PPS 的风暴抑制,支持基于 bps 的风暴抑制
7		MAC 地址表	支持黑洞 MAC 地址,支持设置端口 MAC 地址学习最大个数
8		VLAN	支持基于端口/MAC/协议/IP 子网的 VLAN,支持 QinQ，灵活 QinQ,支持 VLAN Mapping，支持 Voice VLAN，支持 GVRP
9		IP 路由	支持静态路由，支持 RIPv1/v2，RIPng 支持 OSPFv1/v2，OSPFv3，支持 BGP4，BGP4+ for IPv6，支持等价路由，策略路由，支持 VRRP/VRRPv3
10		IPv6	支持 ND（Neighbor Discovery），支持 PMTU; 支持 IPv6-Ping，IPv6-Tracert，IPv6-Telnet，IPv6-TFTP，支持手动配置 Tunnel，支持 6to4 tunnel，支持 ISATAP tunnel，支持 IPv6 in IPv6 tunnel，支持 IPv4 in IPv6 tunnel，支持 GRE tunnel
11		智能弹性架构	支持智能弹性架构，支持分布式设备管理，分布式链路聚合，分布式弹性路由，支持通过标准以太网接口等方式进行堆叠，支持本地堆叠和远程堆叠
12		支持 ACL\QoS	支持 L2（Layer 2）~L4（Layer 4）包过滤功能，提供基于源 MAC 地址、目的 MAC 地址、源 IP(IPv4/IPv6)地址、目的 IP(IPv4/IPv6)

			地址、TCP/UDP 端口号、VLAN 的流分类
13			支持时间段（Time Range）ACL
14			支持入方向和出方向的双向 ACL 策略
15			支持基于 VLAN 下发 ACL
16			支持对端口接收报文的速率和发送报文的速率进行限制，最小粒度为 8Kbps
17			支持报文重定向
18			支持报文的 802.1p 和 DSCP 优先级重新标记
19			支持 CAR（Committed Access Rate）功能
20			每个端口支持 8 个输出队列，CPU 口支持 48 个队列
21			支持灵活的队列调度算法，可以同时基于端口和队列进行设置，支持 SP、WRR、WFQ、SP+WRR、WDRR 五种模式
22			支持 WRED

1.10.3.3.2 万兆边界交换设备需求

序号	重要性	指标项	指标要求
1		配置要求	配置≥24 个 SFP+端口和≥6 个 QSFP Plus 端口，交流供电，双电源
2			交换容量≥4Tbps；包转发率≥1600Mpps；
3			支持基于 MAC/协议/IP 子网/策略/端口的 VLAN
4			支持对端口接收和发送报文的速率进行限制；支持基于队列限速和流量整形的功能
5		设备虚拟化	支持分布式设备管理，分布式链路聚合，分布式弹性路由；支持横向虚拟化，支持本地和远程堆叠，支持纵向虚拟化

6		SDN 控制器	支持 SeerEngine-DC
7		MAC 地址表	支持动态、静态、黑洞 MAC 地址表项
8			支持 MAC 地址自动学习和老化
9			支持源 MAC 地址过滤
10		VLAN	支持基于端口、基于协议、基于 MAC 的 VLAN
11		IP 路由	支持静态路由和默认路由；支持 RIP、OSPF、BGP、ISIS 等 IPv4 动态路由协议；支持 RIPng、OSPFv3、BGP4+、ISISv6 等 IPv6 动态路由协议； 支持等价路由、策略路由
12		IPV6 特性	支持 IPv6 ND（Neighbor Discovery）；支持 IPv6 VxLAN over IPv4；支持 PMTU 发现（Path MTU Discovery）；支持 ICMPv6、Telnetv6、SFTPv6、SNMPv6、BFDv6、VRRPv3；支持 IPv6 Portal 和 IPv6 Tunnel
13		镜像	支持流量镜像；支持 N:4 端口镜像；支持 8 个端口镜像 SESSION；支持本地和远程端口镜像 ERSPAN

1.10.3.3.3 交换设备模块需求

序号	重要性	指标项	指标要求
1		模块 A	多模万兆光模块≥24 个
2		模块 B	单模万兆光模块≥24 个
3		模块 C	千兆多模模块≥12 个
4		模块 D	千兆单模模块≥12 个
5		模块 E	单模万兆 40 公里长距模块≥4 个

1.10.4 等保测评服务需求

本项目需对 4K 二期项目所建设的私有云平台及相关系统整体进行一次等保测评并出具报告。测评需由具有相关资质的单位进行，所有相关费用含在本项目经费中。

序号	重要性	指标项	指标要求
1		服务内容	须邀请具备等保测评资质的测评机构对北京广播电视台的 1 个系统进行等保测评，检测和评估信息系统在安全技术、安全管理等方面是否符合已确定的安全等级的要求;对于尚未符合要求的信息系统，分析和评估其潜在威胁、薄弱环节以及现有安全防护措施，综合考虑信息系统的重要性和面临的安全威胁等因素，提出相应的整改建议，并在系统整改后进行复测确认，以确保信息系统的安全保护措施符合相应安全等级的基本安全要求。

1.10.5 融媒交互区应用监测需求

本项目需对北京广播电视台的融媒交互区应用系统进行安全监测，每月出具安全监测报告。

序号	重要性	指标项	指标要求
1		服务内容	通过不间断的安全监测，为北京广播电视台融媒交互区应用系统提供安全监测服务。当融媒交互区应用系统遇到风险状况时安全监测团队需在第一时间进行确认，提供专业的解决方案建议。除此之外，定期（每月 1 次）为北京广播电视台出具周期性的监测报告，帮助北京广播电视台整体掌握融媒交互区应用系统的风险状况及安全趋势。通过专业化的服务工具来实时监测和周期度量网站的风险隐患，评估北京广播电视台融媒交互区应用系统的安全状态，衡量改进情况。
2		服务要求	1、投标人要提供所使用监测工具的功能截图，截图内容要包括风险值评价、漏洞数量、变更情况、被攻击情况；漏洞整改率、网站

			修复率等内容；
3	#		2、投标人所使用监测工具在全国设置的监测点应不少于 6 个，必须在北京外设有监测点并提供监控节点的具体位置证明；
4	#		3、投标人所使用监测工具须具备自主知识产权，需提供监测工具的软著证书。
5		服务范围	针对北京广播电视台的融媒交互区应用系统
6		服务频次	全年 7*24 小时提供
7		服务成果	《北京广播电视台融媒交互区应用系统安全监测月报》

1.10.6 其他服务

在项目执行过程中如需要其他技术服务以保证项目功能需求的完成，其费用由中标人承担。

1.10.7 重点考察项

序号	技术规格要求
1	安全交互区设计方案： 投标人需详细描述北京广播电视台内部三个私有云与公有云的关系，画出访问关系图，图中需标出现有高安全区的位置以及本项目建设的安全交互区的位置。根据技术需求提出安全交互区设计方案，在方案中详细需描述池化安全设备与安全传输系统的整合方案。
2	融媒云安全设计方案： 投标人需详细描述北京广播电视台的融媒云现状，画出融媒云拓扑图，并在拓扑图中标出本期基础资源扩容的部分。依据业务需求提出私有云安全设计方案，安全设计方案要能够贴合北京广播电视台的现状。
3	公有云安全设计方案： 投标人需详细描述北京广播电视台公有云业务形态，列出不少于五个本期公有云上部署的主要应用，根据公有云服务能力和业务需求提出有针对性的可行的安全设计方案。
4	部署实施方案：

	投标人根据北京广播电视台现有业务所面临的安全风险，结合本期项目新增的基础资源以及应用系统的安全需求，提出切实可行的安全系统部署和实施方案，并描述相应安全防护效果。

四、 设备配置要求

以下设备清单中所涉及设备类型和数量，是根据上述技术需求得到的基本要求。集成商可根据上述需求制定相应的技术实现方案，并依据该技术实现方案。

项目内各系统使用的所有网线及光纤跳线需由中标方提供，具体数量和长度根据实际使用量进行调整，以满足使用需求。本项目各系统所用的网线规格不低于六类标准。

所有服务器和工作站上应使用正版操作系统。配备足够授权的软件。

全面实现本项目需求所需要的其它设备，即使未列入本需求设备清单，也应包含在投标设备范围之内。

以下是本项目关键设备的软硬件配置和性能指标的最低要求，未包含在以下指标要求范围内的设备，由投标方根据项目需求和实现方案进行选型和配置，安装软件情况需根据各集成商解决方案进行部署。

本项目的核心产品为私有云-**边界应用防护设备**。

序号	设备名称	配置说明	数量
1	私有云-安全资源池	安全管理平台完全兼容北京广播电视台现有安全管理平台，实现安全服务能力扩充。 安全管理平台能够覆盖 4K 二期项目新增的所有虚拟化资源，实现融合生产云平台整体安全管控。 支持具备分片路由能力，能够完成跨物理服务器的流量编排，并且更简单更高效，无需外部交换机支持 SDN 或者额外路由配置。 支持可选择安全网元进行策略推送，支持同时同步多个安全网元	1 套

		策略模板，推送策略记录。 支持虚拟安全网元共享。 虚拟交换机组件支持分布式部署，支持集群式服务，可实现横向扩展与高可用。 包含不少于两台基础硬件设备，用于在不同安全域部署管理系统并实现可视化展现，硬件指标需满足技术需求中描述的要求。	
2	私有云-主机自适应安全系统	在保证原有控制台和终端授权可用性的前提下，新增不少于一个管理控制台；新增 Agent 授权不少于 300 个，包含一年维保。 维保服务包括但不限于安装部署服务、产品培训服务、规则更新服务、故障响应服务、系统运维服务、版本升级服务及重大保障服务。 主机自适应安全系统支持 Linux 服务器部署，具备资产清点、入侵检测、风险评估、合规基线、安全工具箱等功能。 系统包含不少于两台配置管理设备，具体配置指标不低于技术需求参数中的要求。	1 套
3	私有云-运维管控设备	标准 2U 机架设备，冗余电源，端口数量：≥2*USB，≥4 电口；内置≥64TB 企业级硬盘,支持 raid0/1/5。 最高支持图形连接并发≥1000 路，字符连接并发≥2000 路。 系统包含≥1000 个授权，最大支持≥2000 个授权。需支持物理旁路、HA 双机热备；需支持基于水平可扩展的集群化架构设计与部署。 支持对资源及登录账户进行管理功能，包括新增、查询、修改、批量导入、导出、删除、分组等操作； 支持批量导入阿里云、华为云、腾讯云、AWS、Azure 和 Ucloud 等	1 套

		平台云主机。	
4	私有云-私有云防病毒	支持 Windows PC/Windows server/Linux/Mac OS 等不同操作系统使用同一控制中心同台管控。 提供不低于 600 个授权点。 支持不少于两个杀毒引擎混合使用，提高病毒检出率。 支持对压缩包内的病毒扫描，支持多层压缩包的扫描，可自定义配置压缩包的扫描层数，至少大约 10 层模式下的扫描。	1 套
5	私有云-千兆边界隔离 UTM 设备	标准 1U 机架式设备，双电源，配置不少于 6 个千兆电口、4 个 SFP 千兆接口（含 2 个光模块）及 2 个接口扩展槽。 支持下一代防火墙访问控制、入侵防御、网络防病毒、上网行为及 URL 分类管理、流控和 IPSec VPN 模块。 提供 3 年特征库升级，3 年维保服务。 整机最大网络吞吐量不低于 16G，每秒新建连接数不少于 20 万，最大并发连接数不少于 350 万。	1 台
6	私有云-万兆边界隔离 UTM 设备	标准 2U 机架式设备，冗余双电源，配置不少于 6 个千兆电口、4 个 SFP 千兆接口、2 个 SPF+万兆接口（含光模块）。 支持下一代防火墙访问控制、入侵防御、网络防病毒、上网行为及 URL 分类管理、流控和 IPSec VPN 模块。 提供 3 年特征库升级，3 年维保服务。 整机网络最大吞吐量不低于 25G，每秒新建连接数不少于 25 万，最大并发连接数不少于 600 万。	1 台
7	私有云-边界应用防护设备	标准机架式设备、双电源，配置不少于 1 个 HA 口，1 个 RJ-45 Console 口，不少于 1 个 10/100/1000 Base-T 带外管理口以及 4 个万兆 SFP+接口（含 2 个多模光模块）。 提供 3 年特征库升级，3 年维保服务。	1 台

8	私有云-日志审计设备	2U 标准机架式，冗余电源，专用千兆硬件平台和安全操作系统，配置不少于 6 个千兆电口，不少于 4 个 SFP 千兆接口（含光模块）及 1 个可扩展插槽，不少于 2 个 USB 接口，存储容量 4TB。配置 200 个审计对象授权。 硬件提供三年维保服务。	2 台
9	私有云-漏洞修复系统	管理端支持 LINUX、CENTOS7.0 以上版本操作系统及 docker 环境部署，授权数量不低于 1000 个。 客户端支持部署在 Windows XP_SP3 及以上/Windows Vista/Windows 7/Windows 8/Windows 10 操作系统；支持域控推送统一部署，对终端用户权限无要求。支持通过传加密参数的方式提权到管理员权限来安装。支持 web 安装、离线包安装、邮件、OA 等通讯方式通知给终端用户。	1 套
10	安全交互区-池化边界安全系统	池化边界安全系统需采用两台以上设备进行集群部署，具备双机或多机热备能力，保证系统可用性，且主备切换不影响整体性能。 系统网络层吞吐量≥240Gbps，最大并发连接数≥1 亿，每秒新建数≥150 万,支持 IPSec 隧道数≥8000,SSL VPN 并发用户数≥1000。 虚拟化功能全开模式系统网络层吞吐量≥80Gbps，最大并发连接数≥500 万，每秒新建数≥60 万。 支持灵活的服务链编排功能，支持 PNF 和 VNF 的混合编排，支持串接链和旁路链，支持网元组的方向和位置设置。	1 套
11	安全交互区-安全传输系统	本次采购为分布式安全传输系统，节点数不少于 3 个； 单台硬件平台资源要求： CPU≥2 颗 Silver 4210R 2.4GHz（10C）； 内存≥4*32GB DDR4 2666； 系统盘≥2*240GB SATA SSD；	1 套

		缓存盘≥2*1.92T； 数据盘≥10*10T； 冗余电源； 接口≥4 千兆电口，6 万兆光口（满配光模块） 提供不少于 300T 存储授权。 本次采购分布式安全传输系统节点间互联网络交换机，为保证兼容性，与分布式安全传输系统同品牌，数量不少于 2 台； 单台网络交换机硬件配置资源要求： 10G SFP+光口≥24 个，40GE QSFP+光口≥2 个，万兆光模块及光纤线≥18 个，配备冗余电源。交换容量不小于 2.5Tbps/23Tbps，包转发率不小于 720Mpps。 支持全端口线速转发。 配置海量小文件高性能处理功能，支持百亿级海量小文件的高性能处理，可以实现 100 亿小文件高速写入。 安全传输系统内置杀毒功能并提供不少于三种杀毒引擎对文件进行查杀。 包含 3 年硬件质保，3 年系统软件升级。	
12	安全交互区-千兆边界交换设备	≥48 个 10/100/1000BASE-T 端口，支持≥4 个 10G/1G BASE-X SFP+端口；支持≥1 个扩展槽；交流供电，双电源 交换容量≥756Gbps；包转发率≥252Mpps。硬件设备提供 3 年维保服务。	2 台
13	安全交互区-万兆边界交换设备	配置≥24 个 SFP+端口和≥6 个 QSFP Plus 端口，交流供电，双电源，交换容量≥4Tbps；包转发率≥1600Mpps。硬件设备提供 3 年维保服务。	4 台
14	安全交互区-	模块 A 多模万兆光模块≥24 个	1 套

	交换设备模块	模块 B 单模万兆光模块≥24 个 模块 C 千兆多模模块≥12 个 模块 D 千兆单模模块≥12 个 模块 E 单模万兆 40 公里长距模块≥4 个 硬件设备提供 3 年维保服务。	

五、 项目实施方案及要求

本章所涉及项目实施、实施要求，均针对中标人，各设备提供商应在整个实施计划执行过程中对用户方和中标方予以充分协助。

本项目招标完成后，将分为系统细化设计、软件预研发/系统预调试、现场软硬件安装调试、系统初验（预验收）、用户培训和系统试运行、系统终验、系统正式运行等七个基本工作阶段。

第11节 总体实施要求

1) 中标人须根据前述工作阶段规划和用户方具体要求，制定详细的项目实施方案和准确的项目实施时间安排，合理设置关键任务检查时间点，供用户方核实和掌控软件研发、实施准备、现场施工的进度和质量。每个阶段的阶段性工作成果经用户方检查并确认后方可进入下一工作阶段。
2) 中标人需为本项目成立独立于其它项目的专门工作组，包含足够数量，分别拥有丰富的设计、研发、实施、测试经验的各种工程师，协同负责本项目各执行阶段的整体工作。
3) 项目全程运行过程中，用户方将根据进度要求安排各种形式的检查以确认相关成果和工作进展，中标人应积极配合用户方开展此项工作，并将所需费用计入项目成本。
4) **投标人所投产品和业务系统应满足台内网络安全技术要求，同时负责对其提供的产品和业务系统进行安全加固，不收取额外费用。**
5) **各媒体服务平台与业务应用平台在进行建设与升级过程中，要充分考虑与台内融媒分发域的对接，按照《北京广播电视台融合生产交换域数据接口规范》的要求进行内部分发**

流程改造、服务接口注册和流程联调，具体要求包括但不限于：内部分发流程改造、服务接口注册和流程联调，所含费用已包含在本项目中，供应商在投标时应予以承诺，具体要求如下：

1. 本业务系统需要按照融合生产交换域面向台内与互联网新媒体平台发布的内容标准进行内部流程改造，支持网内完成指定新媒体格式的转码与分发调用；

2. 融合生产交换域将构建应用链接总线平台，具备服务注册与应用模块链接能力，支持服务注册管理、业务系统间的服务交互和数据交换流程的调度和管理，各业务系统需按照标准将分发调用服务接口注册在应用链接总线平台上；

3. 在服务级别、服务同步异步方式、服务安全访问、错误处理和功能联调等层面，应用连接平台会发布统一数据交换对接规范，各业务系统需遵循规范完成对接，确保融媒分发业务流程的可用。

第12节　实施地点与建设周期

1) 项目实施地点为北京市朝阳区建国路甲 98 号，北京广播电视台国贸办公区。
2) 中标人应自合同生效日起 60 个日历日内完成合同约定的所有硬件产品备货，并运至项目实施地点。
3) 中标人应自合同生效日起 180 个日历日内完成系统细化设计、软件预研发/系统预调试、软硬件现场安装调试任务，使之具备用户培训和试运行条件。

第13节　实施团队要求

投标人须为本项目组建稳定的、专业的、独立的项目团队，设立独立的项目经理，项目经理负责整体把控项目进度和项目沟通协调工作，把控完成项目范围内的各项技术任务。针对本项目成立专门的项目组，确保人力、物力的投入，项目组成员必须稳定，项目团队成员在项目终验前如果人员退出或更换，需要征得招标人同意。投标人须提供项目成员至投标截止时间止近三个月以来任意 1 个月社保证明材料。

1. 服务人员基本要求

所有为北京广播电视台提供信息安全服务的人员，均需具备以下基本条件：

（1）工作态度

态度积极，工作认真负责，责任心强，积极主动，吃苦耐劳。驻场服务人员应具备吃苦耐劳的

奉献精神，能够承受复杂情况下的加班以及长时间的连续工作，特别是在节假日等非工作时间。

团队精神。所有服务人员应具备团队合作精神，能够和其他运维厂商、团队内部其他成员相互理解、通力合作。

（2）专业能力

专业技能。所有服务人员应具备相关专业知识和技能，并提供相应的工作经验证明。

应急能力。应急服务人员在出现突发安全事件时具有较强的应急处置能力，能够及时响应并解决安全事件。

2. 服务人员能力要求

（1）项目经理能力要求

项目经理至少具有 5 年以上安全集成服务项目实施经验，需尽量熟悉电视台的具体业务流程，具有文案撰写能力，须提供项目经理的身份证、学历证、人员简历，提供由投标人为项目经理缴纳的至投标截止时间止近三个月以来任意 1 个月社保证明材料。

为确保项目服务的顺利开展，项目经理需具备丰富的网络安全知识、安全从业经验、项目管理经验，能够从整体上对安全系统提供规划、管理、加固建议，具有并提供如下证书复印件或扫描件：

1）人力资源和社会保障局颁发的信息安全工程师证书，可以确保项目经理具备网络安全知识；

2） 人力资源和社会保障局颁发的信息系统项目管理师证书，可以确保项目经理能够使用项目管理的知识对项目进行管理；

3） 人力资源和社会保障部、工业和信息化部共同颁发的网络规划设计师，可以确保具备网络故障、安全故障判别、排查分析的能力；

4）人力资源和社会保障部、工业和信息化部共同颁发的系统规划与管理师，可以确保具备对安全系统提供规划、管理、加固建议的能力；

5）VMware 认证专家，可以确保项目经理具备 VMware vSphere 安装，配置，管理的能力。

（2）信息安全技术人员能力要求

1） 要求从事该项服务的人员具有 3 年以上信息安全技术服务经验，具备中国信息安全测评中心颁发的国家注册信息系统审计师（CISP-A）、人力资源和社会保障部、工业和信息化部联合颁发的系统规划与管理师证书，需提供证书复印件；

2） 熟悉常见信息安全产品，熟练使用采购人的防火墙、VPN、IPS 等产品，能够对产品进行配置调整和日志分析，具备中国网络安全审查技术与认证中心颁发的信息安全保障人员（CISAW ）认证证书（风险管理方向专业级）和中国信息安全测评中心颁发注册信息安全专业人员（CISP）证

书，需提供证书复印件；

3) 全面掌握网络攻防技术，能够从攻击者的角度对安全设备进行策略优化配置，具备中国信息安全测评中心颁发的国家级渗透测试专业认证（CISP-PTE）和工业和信息化人才专业知识测评证书，需提供证书复印件；

4) 能够分析和处理常见网络安全事件，具备中国网络安全审查技术与认证中心颁发的信息安全保障人员（CISAW ）认证证书（应急服务方向专业级），需提供证书复印件；

第14节 细化设计与预研发

1) 在系统细化设计阶段，将针对中标人案进行细化、补充、完善，使之具备可实施性，必要时安排相关测试和验证。在软件预研发/系统预调试阶段，将根据方案细化结果进行定制需求的软件研发，以及研发结果的验证和改进。在上述两个项目准备阶段完成并通过用户方确认后，将进入项目现场，顺序完成现场软硬件安装调试、系统初验、用户培训和系统试运行、系统终验、系统正式运行等工作阶段。
2) 在系统细化设计、软件预研发/系统预调试阶段中，对关键设备选型，中标人应根据用户方具体要求，组织相应适用性测试。用户方将参加该测试并确认测试结果，以确保该设备完全适用于本项目。搭建、运行测试环境所需所有设备由中标人自行解决，所需费用计入项目成本。如果在测试中发现设备不符合项目需求，将由中标人更换相同或更高档次设备（具体设备型号由中标人提出、经用户方认可后确定），重新安排测试，通过测试后按程序进行项目设备变更。该变更可能导致的附加费用，全部由中标人承担。

第15节 设备到货与集成

1) 中标人保证按合同向用户交付的所有货物应是原厂商全新出厂的完善（包含能使本系统能够良好运行的所有选购件）产品，并配有相应的技术资料，产品质量、技术指标符合生产厂家的出厂质量标准和国际技术标准。所提供的软件为正版合法软件。
2) 中标人供货时，应向用户提供原厂产品的相关供货证明文件，若不能提供则招标人有权拒绝接受全部货物。
3) 货物包装箱内应附有详细的装箱清单，装箱清单应清楚标明与主机、附件、各种零部件和

消耗品相对应的编号和名称。在包装箱中必须附有招标文件所要求的所有文件和资料。

4) 货物的包装应为生产厂商出产时的原包装。

5) 中标人应确保所提供的货物在装卸、运输和仓储过程中有足够的包装保护，防止货物受潮、生锈、被腐蚀、受到冲撞以及其他不可预见的损坏。

6) 投标人应将招标文件中未列出而系统实施及设备正常运行又必需的软件、硬件(如接口设备、连接缆线等）予以补齐，以构成一套实用系统；投标人需将有关价格明确列出并包含入投标价中，否则将视为免费提供。如果投标人在中标并签署合同后，在供货时出现软、硬件的任何遗漏，均由中标人提供，采购人将不再另行支付费用。

7) 项目进入现场软硬件安装调试阶段后，中标人应在用户方的统一安排和指挥下，严格遵守相关操作规范和制度，尤其是系统机房施工以及综合布线方面的标准，在不影响其它项目施工和已建成系统正常运行的前提下，确保本项目工作顺利进行。

第16节　联调、测试、试运行及验收

1) 在系统联调、测试、验收阶段和质保期内，中标人应提供原厂商 7×24 小时电话技术支持服务，如果不能解决问题，必须提供原厂商现场服务。

2) 投标人应在最短时间内对承建单位所提出的要求做出反应，投标人保证在接到承建单位故障报修或咨询后 1 小时内给予响应，中标人工程师在 4 小时内到达用户现场。

3) 系统测试、验收包括初验、系统试运行和终验 3 个环节。项目完成现场软硬件安装调试工作后，用户方将组织初步验收，形成初验报告，经用户方、中标人签字确认后，方可进入试运行阶段。试运行阶段为期 6 个月，其间穿插进行用户培训，随后进入终验阶段。

4) 中标人须配合用户和第三方测试单位,制定、实施相应测试验收方案，并根据测试结果进行方案优化,同时针对试运行期间暴露的各类问题，按照用户方需求对系统软硬件进行必要的改进、完善和调换，确保系统具备正式上线运行的条件。

六、 售后服务要求

第17节　质保期

1) 中标人应对**系统整体提供 12 个月的免费质量保证期**，免费质量保证期自终验报告签字之日起计算。

2) 中标人应对**系统内单件设备提供 36 个月的免费质量保证期**，免费质量保证期自设备到货验收合格开始计算。

第18节 质量责任

在设备质量保证期内，除不可抗力及使用不当造成外，某一部件出现四次故障，此部件将终身免费保修或招标人有权要求投标人予以整机更换。

第19节 免费质保服务要求

1.19.1 维修及备件服务

1) 投标人保证在接到用户故障报修或咨询后 1 小时内给予响应，中标人工程师在 4 小时内到达用户现场。
2) 质量保证期内，若故障设备确认在现场不能修复时，提供 5X8 小时的备件先行服务。中标人接到用户通知后，备件响应时间不超过 24 小时，以保证系统正常运行。但故障设备运回维修时不得将存有用户保密和敏感信息的存储媒体带离用户办公场所。
3) 系统所涉及的所有产品，应确保设备使用期的 5 年内均能提供备品备件。
4) 质量保证期内，投标人负责对其提供的产品进行现场维修与维护及更换零部件，不收取额外费用。

1.19.2 技术支持服务

1) 投标人须在系统质保期内，派出至少 1 名驻场工程师，对系统进行现场维护并提供技术支持，保证系统运行正常，及时解决可能发生的系统故障和异常，且不收取额外费用。
2) 中标人须在系统及设备质保期内，提供 7×24 小时原厂电话技术支持服务。
3) 在质量保证期内，遇重要安全播出保障期，中标方应根据台方要求，免费增派技术人员参与技术保障工作。

1.19.3 软、硬件升级服务

1) 中标人承诺在系统建设完成后，继续与用户方合作、根据实际应用需要进行软件完善及升级工作。
2) 对于今后系统可能的升级，承诺软件终身升级免费，硬件升级价格优惠幅度不低于本次

招标优惠幅度。对于今后系统可能的改造和扩容，承诺价格优惠幅度不低于本次招标优惠幅度，积极配合用户方完成。

3) 集成商应向台方提供最终用户为北京广播电视台的第三方关键软硬件设备售后维护合同，售后维护合同不可以单次服务的方式签署，售后维护商的选择要求具备相应维护能力并与已建成的系统设备维护厂商保持一致。

1.19.4 出保后服务要求

质量保证期结束后，中标人为系统涉及的所有软、硬件设备提供终身的有偿维修。

1.19.5 用户培训要求

1) 中标人应在投标书中详细描述针对本项目的培训方案。

2) 中标方应提供不少于 3 人次免费的网络安全专项培训，内容需涵盖网络安全攻防技术、渗透测试技术、入侵检测技术和无线网安全。

3) ★ 培训须免费提供，且在北京广播电视台内进行，并提供承诺函（格式自拟，需加盖投标人公章）。

（招标文件中★项代表实质性指标，不满足该指标项将导致投标被拒绝。）