市局机关网络安全和中心机房维保项目清单

序号	服务项目	服务内容	服务具体内容	具体设备清单
1	资产信息统计	设备统计	1、网络设备和中心机房硬件设备型号、数量、版本等信息统计记录；2、中心机房硬件设备软件产品型号、版本和补丁等信息统计记录；3、网络结构、网络路由、网络IP地址统计记录；4、其它附属设备的统计记录。	包含运维期间新增设备
2	网络安全系统运维	攻防演练设备	1、定期检查设备的物理状态，确保设备的外观完好无损，没有松动或破损的部件，定期清洁设备的内部和外部；2、保持设备的软件和固件更新至最新版本，以确保设备具有最新的安全补丁和功能改进；3、安装并定期更新防病毒软件，确保设备免受恶意软件和病毒的攻击；4、定期备份攻防演练设备上的重要数据和配置文件；5、日志监控：定期检查设备的日志文件，以便及时发现和解决任何异常活动或潜在的安全漏洞。	1、锐捷交换机RG-S5750-28GT-S 2、H3C交换机-S5560 3、锐捷无线网关RG-WS7204-A 4、H3C交换机-MSR50-40 5、H3C交换机-S7506E-S 6、网络攻防演练设备1套
3		网络预防性维护	定期对网络安全检测与评估，对内部网络实行安全性能检测，对各类网络的线路及相关在线网络设备进行状态监控、性能监测。	
4		网络访问控制监控	主要监控各VLAN状态、访问控制策略、防火墙控制策略等情况，测试不同网段是否互通，测试访问控制列表是否限制特殊访问，测试防火墙控制策略是否生效。	
5		网络性能监控	主要监控网络的分网运行情况、带宽占用情况、链路收敛情况、质量控制情况、地址转换情况。	
6		网络设备状况监控	主要监控路由器和交换机、各类防火墙等网络设备的CPU利用率、内存使用率、RTO值等关键运行参数，同时还要对网络设备的状态等进行监控。	
7		定期巡检维护	每季度对网络设备进行一次除尘、清洁服务；每季度对所列网络安全设备进行一次全面检查；每半年对机关办公场所内各配线间进行一次清洁和连线整理；每半年对网络性能进行一次全面测试，根据测试结果，提出相应的网络规划和配置建议。	
8		精密空调	1、负责精密空调的维保工作，确保机房环境温湿度稳定；2、如空调出现故障时，应急处置不得产生水淹、温度过高等次生伤害；3、提升精密空调的使用寿命、包含但不限于空调滤网清洗、间歇启动策略调整等；4、确保精密空调工作效率，定期对空调进行压力测试；5、定期对于空调外机进行清洗清理工作（每年不低于6次，其中5-9月应安排不低于3次清洗清理工作），保证排水与散热良好。	2台艾默生DME12MOP1精密空调
9		不间断电源服务	1、每天检查主机工作状态；2、定期测试电源插座；3、定期保养UPS电池；4、定期检修电源控制柜；5、定期记录机房环境参数；定期检查电源接地及防浪涌装置；6、根据检查测试结果采取相应的保障措施，确保UPS不间断电源系统正常工作。7、停电后，检查UPS供电系统是否正常运行，并检查系统相关部分是否运行正常。8、季度对UPS电源电池进行1次充放电处理，以确保电池处于良好的运行状态延长电池使用寿命。	1台

市局机关网络安全和中心机房维保项目清单

序号	服务项目	服务内容	服务具体内容	具体设备清单
10	机房环境设备维护	动态环境监测设备	1、防水检查：每年清洁一次水浸传感器，确保传感器灵敏，并检查其工作正常；2、门禁：检查端子和接头是否松动，确认模块的性能指标和状态指标正常，检查电源、锁、控制和电路；3、动态环境控制：工程师每年至少访问工厂两次，定期等待并确保设备处于最佳状态；4、硬件性能检查：方式检查、传感器/变送器检查、网络设备控制；5、软件功能检查：数据完整性识别、功能识别、报警功能检测、移动语音报警功能检测通过软件和安全控制确保报警功能正常，数据库功能正常。	1套
11		消防器材	1、消防灭火器维保保养时要做到整洁无灰尘、喷嘴通畅，放置符合规定要求，压力值正常，四周没有堆放其他物品，以防发生火灾时影响正常使用和操作；2、自动灭火系统、消防排烟设备，防火门和消防栓都要定期进行测试，凡失灵损坏的要及时维修更换，确保其处于正常的预警预防状态；3、根据消防设备器材的用途、特性，应制定具体合理定期消防设备维保维修知识点计划，且做到专人专责，执行到位。	1套
12	（云）平台服务器运维	服务器	1、日常维护：检查机房服务器系统状况，定期观察服务器的运行情况，定期对数据库运行情况分析。对出现有错误日志的服务器，及时记录错误信息，分析错误日志，并反馈给负责人员；发现有严重错误事件，立即分析解决，并形成书面解决方案提交给用户负责人。及时下载安全及系统补丁、防止有安全漏洞、提高服务器性能；2、操作系统维护：为用户提供的各种正版操作系统进行安装，对服务器进行DNS、WINS、DHCP、域控制器等系统功能的安装调试。根据各厂商的通告，定期为各相关主机设备的系统软件更新补丁，升级版本；3、主机系统维护：对使用过程中遇到的疑难问题进行支持；对系统性能优化提供建议及支持；根据应用需求，配置新版本操作系统，并恢复应用系统；保证机关提供的服务器操作系统软件安全性和合法性；4、定期巡检维护：制定年度预防性维护计划，对全部服务器主机设备提供每季度一次的预防性维护；5、对主要设备的运行情况、安全状况等进行全面检查，对其性能进行全面测试和调优，对相关设备运行环境、网络环境以及操作系统日志进行检查与分析，排除故障隐患和安全漏洞，并在维护后提交完整的报告。	包括但不限于华为SMC和MCU服务器等旧有或新增服务器。
13	信息安全服务运维	网络安全	1、日常巡查服务:每月针对机关的重点业务系统和服务器设备（应用服务器、数据库服务器等）进行安全巡检服务，查找系统安全漏洞，系统自身漏洞检查、漏洞补丁更新并进行分析统计。每季度对机关的桌面设备（笔记本电脑、台式电脑）进行全面的安全巡检服务，查找系统安全漏洞，并进行分析统计。每季度对机关的网络设备（交换机、防火墙）进行全面的安全巡检服务，进行状态检测、策略配置校验，并进行分析统计；2、安全通告服务:不断关注安全技术的发展和新的漏洞的出现，并根据机关信息系统中的信息资产情况，通过邮件、电话等方式机关提供相应的安全信息通告，提高用户的安全防范意识。	1、绿盟DDOS网关ADS 200 Series 2、H3C防火墙F1030 3、深信服上网行为管理AC-1800 4、网神防病毒 5、含新增网络安全设备

市局机关网络安全和中心机房维保项目清单

序号	服务项目	服务内容	服务具体内容	具体设备清单
14	安防存储设备运维	磁盘阵列	1、定期检查磁盘状态和 RAID 配置，防止单点故障导致数据丢失；2、定期检查网络连接和存储空间使用情况，防止网络故障和存储空间不足导致业务中断；3、对于重要数据需加强数据备份和安全性管理，防止数据泄露和损坏；4、每半年或一年进行一次包括设备清洁、硬件检查、软件升级、数据备份等。	海康威视磁盘阵列存储
15	运维报告	网络安全和机房运维、专项运维报告	运维项目应当按月、季度、半年、年度形成书面运维报告，运维报告应当至少包含运维工作开展情况，事件处置情况等内容。如未提供或未及时提供书面运维报告，视为未完成相关工作。	
16	驻场服务	驻场服务	运维单位应当安排专人驻场服务（每周不少一个工作日，且不低于8小时）。	