信息安全设备采购项目需求公示材料

一、 技术要求

（一）具体技术指标要求

1.建设内容

在网络中构建安全保密服务区，分别部署 1 套防篡改系统，强化应用安全防护能力；分别部署 1 套数据防泄露系统、1 套数据脱敏系统和 1 套应用安全网关，对数据生产流转过程提供可靠安全的防护，对敏感数据进行脱敏处理，强化数据存储安全，构建全面的数据防护机制；分别部署 1 套安全审计系统和 1 套网络安全态势感知系统，对网络设备、安全设备进行统一监管，日志数据统一收集，实时监视网络的运行状态，并提供安全事件报警服务。建设运维管理系统，可实现部署在用户不同的网络中，有效提升各网系整体的运维管理效率。根据用户要求进行应用安全等级检测和应急响应预演，同时提供至少一年人员驻场服务。

2.采购清单

序号	物资/服务名称	单位	数量
1	防篡改系统	套	3
2	数据脱敏系统	套	3
3	数据防泄漏系统	套	3
4	应用安全网关	套	3
5	安全审计系统	套	3
6	运维管理系统	套	3

7	网络安全态势感知系统	安全态势平台	套	3
		安全态势探针	台	6
8	应用安全等级（三级）检测		次	5
9	应急响应预演		次	5
10	技术服务力量		项	1

3.主要技术参数

投标供应商所投的网络安全设备须为国产自主品牌,须在投标文件中提供承诺函。

3.1 防篡改系统

序号	指标项	详细要求
1	基本要求	★网页防篡改保护系统基本包，含软件狗，必配基本包，按照需求配置 Windows，Linux，中标麒麟、银河麒麟等国产化系统客户端授权许可。支持国产操作系统的安全防护，兼容飞腾、鲲鹏等国产软硬件平台，并具有软件著作权。
2	功能要求	1.支持 docker 容器技术。支持 IIS、Apache、Weblogic、Tomcat、WebSphere 等 WEB 发布类型，支持各类网页文件的保护，包括静态和动态网页以及各类文件信息。（要求提供功能截图证明材料，并加盖投标供应商公章）
		2.B/S 管理方式，Linux 平台部署中心,采用基于文件过滤驱动保护技术、事件触发机制相结合方式。

		3.支持对指定文件夹以及子文件夹的保护,避免上传非法文件及木马等恶意文件或插入恶意代码。
		▲4.支持基于目录、进程、IP、用户、时间等进行设置篡改项。(要求提供功能截图证明材料，并加盖投标供应商公章)
		▲5.智能检测并防御CC攻击、SQL注入、跨站脚本攻击等，能通过策略配置保证网页防篡改能力，达到等保三级中网站防护要求。
		6.与网页防篡改同一客户端，同一管理平台即可实现容器篡改防护，将容器镜像内目录保护后，任何以该镜像创建的容器内的目录都将进行篡改保护，目录下的所有目录、文件(包括子目录和文件)都将无法修改。
		▲7.具备网站静态数据监测、网站动态数据监测、网站目录监测功能。(提供具备CNAS标识的关于网站数据监测功能的产品功能检测报告或功能截图证明材料，并加盖投标供应商公章)
		▲8.具备网站静态数据防篡改功能、网站动态数据防篡改功能、网站目录防篡改功能。(提供具备CNAS标识的关于网站数据防篡改功能的产品功能检测报告或功能截图证明材料，并加盖投标供应商公章)
		9.支持邮件、Syslog、SNMPTrap、平台告警等多种告警方式，对非授权用户篡改网页提供实时报警提示，支持多种日志级别，日志导出。

3.2 数据脱敏系统

序号	指标项	详细要求
1	基本要求	★标准机架式设备，采用国产化软硬件平台(国产化软件具有软件

		著作权），标配包含数据库授权及文件授权,≥2U,冗余电源,可参考脱敏速度≥38G/小时，脱敏单元格≥28000 个/S。数据脱敏系统内置丰富的敏感算法，自动发现敏感数据，通过对敏感数据漂白、变形、遮盖等处理，实现脱敏后的数据安全可用；支持大表、大文件等大规模数据脱敏场景。
2	功能要求	1.基本数据库：MYSQL、SQL SERVER、ORACLE、MSSQL、DB2、POSTGRESQL 等。 文件：TXT、CSV、XLS、XLSX、XML、JSON、DICOM 等。 国产数据库：DM（达梦）、GBASE（南大通用）、KINGBASE（人大金仓）、HIGHGO（瀚高）等。 大数据组件及其他：HIVE、MONGODB、ELASTICSEARCH、HBASE 等。
		2.支持对于敏感标签对应的发现规则进行配置，配置内容包括：判断主体、发现条件。（要求提供功能截图证明材料，并加盖投标供应商公章）
		3.支持全量/增量两种方式进行敏感数据发现，同时支持对于数据采样行业、命中阈值、脱敏模版进行配置。（要求提供功能截图证明材料，并加盖投标供应商公章）
		4.支持对于脱敏任务的基础信息及对应的脱敏规则进行配置，基础信息包括任务名称、数据流向、输入源、对象同步、脱敏表格、增量配置、数据筛选、输出目标、数据覆盖方式。（要求提供功能截图证明材料，并加盖投标供应商公章）

		▲5.提供单独的数据对比能力以对比生产数据和测试数据或脱敏前和脱敏后的数据内容差异。提供数据对比任务新增、管理、运行等功能，可对数据对比任务的采样比例等多项参数进行配置。（要求提供功能截图证明材料，并加盖投标供应商公章）。
		6.支持以 API 形式将数据脱敏与数据水印能力进行对外提供，跟其他应用平台对接实现脱敏算法查询、数据脱敏、数据水印处理等功能。
		7.提供针对数据资产与任务运行的统计分析报表。
		8.数据脱敏任务运行以实例方式进行管理，并提供可视化监控。
		9.支持对敏感数据发现任务发现的敏感字段进行导入或导入操作，用户可在离线文件中快速修改和确认字段敏感标签。
		10.提供管理用户登录相关的安全配置，包括密码尝试次数、锁定时长、重置计数器、密码有效期、页面超时设置、强密码校验、IP 黑白名单、数据权限开关。
		11.管理员权限支持配置、授权、审计分立，管理权限相互制约。

3.3 数据防泄漏系统

序号	指标项	详细要求
1	基本要求	★标准机架式设备，采用国产化软硬件平台（国产化软件具有软件著作权），采用软硬件一体机模式，集业务平台和审计引擎于一体，支持旁路部署和串联部署,≥2U,配置≥4 个千兆电口，≥2 个千兆光口，≥2 个万兆光口（默认含不少于 1 个管理口、不少于

		1个HA口），7层最大检测吞吐≥700Mbps，提供网络监控和网络阻断功能。
2	功能要求	1.支持实时双向流量的内容审计,支持对上传和下载文件内容进行识别和过滤（要求提供功能截图证明材料，并加盖投标供应商公章）
		2. 支持识别包括但不限于以下文件类型及内容： 办公类：doc、docx、xlsx、xls、xlsm、xltm、ppt、pptx、pps、docm、pdf、wps等； 图片类/OCR识别：jpg、jpeg、png、bmp、gif、tif、tiff等； 压缩类：rar、zip、7z、tar，war等，支持处理压缩炸弹，压缩层级支持设置; 网页类：xml、htm、html等； 文本类：txt、rtf等； 源代码类：c++、cs、php、py、js、java、class、go、bat、vb、vbs、vbe等； 设计图纸类：dwg、dxf等； 音视频类（类型识别）：mp4、avi、wmv、mov、wma等。
		3.支持对分卷压缩包的还原及内容识别。
		4.数据标识符包括身份证、银行卡、手机号、车牌号、护照、地址、邮箱、工作证、MAC地址、金额等。（要求提供功能截图证明

		材料，并加盖投标供应商公章）
		5.支持通过本地上传的方式，自动生成结构化指纹，通过指纹匹配策略，可识别具有该指纹信息的相关文档。（要求提供功能截图证明材料，并加盖投标供应商公章）
		6.支持无监督学习，生成自动分类模型，通过用户上传文件夹，系统依据相似度自动对文件进行聚类，并生成文件关键词及其权重。（要求提供功能截图证明材料，并加盖投标供应商公章）
		▲7.可进行文件数据内容识别、网络协议数据内容识别，符合《信息安全技术数据泄露防护产品安全技术要求》GA/T 912-2018 中所述的有关要求。 （提供具备CNAS标识的关于数据内容识别的产品功能检测报告或功能截图证明材料，并加盖投标供应商公章）
		▲8.数据泄露防护的响应动作，符合《信息安全技术数据泄露防护产品安全技术要求》GA/T 912-2018 中所述的有关要求。 （提供具备CNAS标识的关于数据泄露防护的响应动作的产品功能检测报告或功能截图证明材料，并加盖投标供应商公章）
		9.支持查看所有文件资产,可查阅文件对象及其时间范围内的流转分析，包括文件基础信息，文件传输通道，命中策略规则信息等。（要求提供功能截图证明材料，并加盖投标供应商公章）
		10.支持通过邮件发送告警通知，支持常见的运维管理功能，包括

		网络抓包、网络连通性检测、路由追踪、服务连通性检测等功能，且上述所有功能可以在 WEB 页面进行自行配置和管理。

3.4 应用安全网关

序号	指标项	详细要求
1	基本要求	★1.标准机架式设备，采用自主研发的国产化操作系统和全国产自主可控的 CPU(≥8 核,≥2.3GHz,≥16 线程)和存储芯片,16GB DDR4 内存、2 块 2TB3.5 寸硬盘、800W AC 白金电源(冗余电源)、≤4U，配备不少于 4 个 10G 光口、2 个千兆电口，每个光口配置 1 个相同传输速率的光模块（不少于 1 个管理口、不少于 1 个 HA 口）。提供不少于 500 个资产授权，并提供不少于 3 年软件免费更新维保服务。 2.支持无插件化的浏览器访问主流操作系统、数据库、WEB 应用、C/S 架构应用等资产;支持 Oracle、Postgresql、MySQL、SQL Server、ClickHouse、MongoDB、Redis 等主流数据库以及达梦、人大金仓、瀚高等主流国产数据库的审计功能。
2	功能要求	1.支持用户的批量导入/导出，按用户类型等分组方式；支持用户安全策略功能，如密码锁定次数、密码复杂度、用户有效期等。
		2.支持基于角色的权限访问控制，根据用户角色不同，提供不同的功能。角色权限可以细化到最小颗粒度，如查看、创建、更新、删除资产权限。
		▲3.支持管理、操作、审计权限分立。管理权限提供用户管理、资

		产管理等功能，审计权限提供会话审计、日志审计等功能，操作权限提供Web终端访问、文件管理等功能。（要求提供功能截图证明材料，并加盖投标供应商公章）
		4.支持对数据库命令进行阻断及审批。支持本地客户端、远程应用发布等方式连接数据库。
		5.支持对运维操作会话的实时阻断、日志回放 ，包括起止时间、来源用户、来源IP、目标设备、协议/应用类型等日志内容。
		6.支持查看该用户授权的资产、资产授权规则、用户登录规则、连接的资产会话信息。（要求提供功能截图证明材料，并加盖投标供应商公章）
		7.支持界面设置，可以自行设置登录页面标题、登录页面图片、网站图标、管理页面Logo等，满足内部规范化管理。（要求提供功能截图证明材料，并加盖投标供应商公章）
		8.提供无插件化的浏览器访问方式，支持通过浏览器即可登录Linux、Windows、WEB应用、C/S架构应用等资产。（要求提供功能截图证明材料，并加盖投标供应商公章）
		9.自动改密码：支持对unix资源、网络资源、windows资源、数据库资源、中间件资源进行密码变更；密码变更可以根据密码策略的要求进行变更，变更的密码符合密码策略中关于密码强度的要求。支持周期性执行改密任务。

3.5 安全审计系统

序号	指标项	详细要求

1	基本要求	★采用国产 CPU 和操作系统（国产化软件具有软件著作权）,≤4U,配置≥3 个千兆电口（2 业务口+1 管理口）、≥2 个万兆光口（满配光模块）,冗余电源,系统盘≥240G SSD，数据盘≥4T*4，默认 Riad5，冗余电源，日志采集处理均值≥20000EPS，峰值≥35000EPS，默认包含 100 日志源。支持主流主机服务器、网络设备、安全设备、数据库等日志事件的收集分析。
2	功能要求	1.支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等不少于 26 类 300 种日志对象的日志数据采集。
		▲2.支持对日志流量非常大但是日志重要程度低的 syslog 类型日志源进行限制接收速率，降低对系统资源的占用，保障重要日志的收集。（要求提供功能截图证明材料，并加盖投标供应商公章）
		3.支持日志归一化处理，将不同设备所产生的不同格式、难以理解的日志数据进行统一格式化处理，提炼出有用信息，清晰明确的展示给管理者。
		▲4.支持设置被采集源的日志、报表数据存储时间为 1 个月、3 个月、6 个月和永久保存等参数。（要求提供功能截图证明材料，并加盖投标供应商公章）
		5.支持日志备份功能，支持本地备份和 FTP 备份方式，支持自动备份和手动备份。
		6.支持实时告警展示，可根据告警规则、告警级别两个维度进行实时告警监视，并可对刷新事件间隔进行设定。

		▲7.支持对重点日志源的关注设置，并可通过关注列表快速查看重点日志源的状态、当日日志量、采集日志总量、最近接收时间、业务组等基础信息。（要求提供功能截图证明材料，并加盖投标供应商公章）
		8.支持以业务角度将日志源进行分组，支持在日志查询时以业务组进行查询，支持在首页拓扑展示时以业务组进行展示。

3.6 运维管理系统

序号	指标项	详细要求
1	基本要求	★要求配置不少于500个设备节点永久性授权。
2	功能要求	1.平台采用B/S架构模式，支持基于HTTPS中文Web图形化界面管理。
		2.具备设备管理、告警管理、运维数据查询等功能。
		3.支持不少于20个并发用户同时登录系统并进行操作。
		4.支持设置访问会话超时、超时自动退出功能，即管理员在规定时间内无操作时，管理平台自动退出，重新登录后方可再次进行管理任务。
		5.支持密码保护与检测策略，同一账号密码连续多次错误一段时间内禁止登录。
		▲6.提供所投产品的数据可视化、数据报表功能二次开发接口，同时承诺支持与需求单位屏蔽机房动环控系统进行数据对接。（提供承诺函并加盖投标供应商公章）

		7.支持交换机、路由器、OLT、ONU、无线设备、防火墙、网闸、WAF、IDS、IPS等基础网络及安全设备的统一监控，能够持续监测运行状态、CPU使用率、内存使用率、丢包率、延迟、接口流量、接口速率等性能指标。
		8.支持自动生成网络拓扑图，实时展示全网络设备运行状态；同时具备拓扑定期自动修正功能，以适配实际网络架构。
		9.支持网络设备配置备份功能，包含手动备份和自动备份两种方式。
		▲10.支持网络中非网管交换机、路由器等设备的连接信息检测。（提供中国软件测评中心出具的测试报告并加盖投标供应商公章）
		▲11.支持子网自动扫描和手动添加，能够统计各子网IP使用率；支持子网IP使用状态可视化展示，包括IP在线状态和分配状态统计；支持IP和MAC地址绑定，针对IP地址冲突进行告警提示。
		12.支持对网络系统环境进行全方位巡检，实时获取最新故障信息。
		▲13.支持交换机网口检测功能。实时查询交换机网口使用率，同时支持交换机闲置网口（长期未激活网口）检测。（要求提供功能截图证明材料，并加盖投标供应商公章）
		▲14.支持网络时钟监测功能。要求平台能够对接NTP服务器，对监控节点进行时钟监测，并对时钟异常的节点进行告警通知。（要求提供功能截图证明材料，并加盖投标供应商公章）
		15.支持以业务视角对关联的数字资产进行发现和整合，构建符合业务逻辑的业务模型，实时展示业务节点的运行状态和性能指标，针对故障节点进行高亮显示和提醒。

		16.支持业务系统健康度、繁忙度的实时监测和历史趋势分析，可根据实际业务场景进行算法规则调整；支持业务监测数据快照处理，能够进行业务故障溯源分析。
		17.支持业务巡检功能，可对业务系统的网络环境、系统环境、应用环境进行自动化巡检，并生成PDF格式巡检报告发送到指定用户。 ▲18.支持安全检查功能，能够对业务主机的弱口令、账号权限、密码策略、入侵防范等安全配置项进行扫描，并提供检测结果，针对存在的风险配置给出加固建议。
		▲19.支持等保自评功能，能够根据等级保护的相关要求进行政策信息的解读，按照三级系统认证规则自行测评；支持等级保护备案信息录入及相关文件上传。（要求提供功能截图证明材料，并加盖投标供应商公章）
		20.支持对Windows、Linux、麒麟、统信等主流操作系统的监控，包括服务器运行状态、CPU、内存、磁盘、网络连接状态等指标。 支持对Oracle、MS SQL、MySQL等主流数据库以及达梦、人大金仓、瀚高等主流国产数据库的监控，包括死锁、线程、会话、请求、失败作业、数据文件等指标及锁表语句进行分析和查看。
		21.支持Oracle表空间使用统计以及AWR报告生成和导出功能。
		22.支持宿主机、虚拟机资源使用统计和性能分析，包括CPU、内存、磁盘、网络等指标；支持容量使用预测，提示虚拟化资源扩容；支持虚拟化告警信息采集和通知。
		23.支持业务系统API接口监听，能够通过Web端进行告警通知。

		24.支持对 Tomcat、Apache、Nginx、Weblogic 等主流中间件的监控，包括会话、内存、组件加载、计数器、IO 性能、连接信息等指标。
		25.支持对存储设备的电源、风扇、磁盘、控制器等硬件状态的监测，以及对存储设备的 LUN 性能、磁盘性能、IOPS 等性能指标的监控。
		26.支持对视频监控系统、门禁系统、多媒体会议系统等智能化系统所依赖的物联网终端设备进行统一监控和管理，通过构建业务视图，以可视化的方式实时展示每个终端设备的运行状态。
		▲27.支持以业务、资产等视角对信息化资产进行全方位、立体化展示，提供综合运维大屏、业务大屏、资产大屏、网络大屏等多种展示方案。（要求提供功能截图证明材料，并加盖投标供应商公章）
		28.支持故障统计报表、业务综合报表、流量报表等多种类型的报表；支持 PDF 格式文件的生成和下载,能够通过移动端进行推送和查看。
		▲29.支持智能巡检功能，能够对网络设备、安全设备、主机系统、虚拟化、数据库等不同类型的监控资产按照日、周、月等周期设置巡检计划，可通过 PC 端实时统计和查看资源运行状态和性能指标。（要求提供功能截图证明材料，并加盖投标供应商公章）
		30.支持故障信息的统一管理，能够按照对象类型、故障等级、故障状态等条件进行筛选；支持自定义设置监控对象的阈值。
		31.支持告警策略管理，能够按照资源类型、监控对象、告警等级等条件设置不同的消息接收人，并支持连续推送和分级推送方式。
		▲32.具备故障通知、工单通知、报表预览、设备管理、告警管理、运维数据查询等功能。

3.7 网络安全态势感知系统

3.7.1 安全态势平台

序号	指标项	指标要求
1	基本要求	★采用国产 CPU 和操作系统（国产化软件具有软件著作权）；≤4U,配置≥2 个千兆电口、≥2 个 10G 光口(含 2 个光模块), 每个光口配置 1 个相同传输速率的多模光模块。冗余电源,存储≥24TB，内存≥128G。
2	功能要求	1.支持态势大屏展示，包括全网态势、资产态势、漏洞态势、攻击态势，支持大屏展示时间设置，支持态势大屏中相关信息下钻跳转到对应的详细页面。
		▲2.支持自定义大屏界面展示顺序，支持多种地图、拓扑展示方式，支持 logo、大屏超时设置、介绍文案。
		3.支持以地图实时展示网络攻击态势,支持以不同颜色攻击线展示攻击过程，支持攻击源展示，支持攻击目的进行相关标记的显示。
		4.支持对安全处置情况进行概览分析，包括待处置告警数、待处置漏洞数、待处置风险资产数、待处置威胁源数、待处置漏洞。
		5.支持工单管理，支持指派相关人员进行处理，支持对工单进行分组管理，分组类型包括我的工单、待处置工单、已处置工单、历史工单。
		6.支持对攻击线索追踪溯源分析，支持追溯结果多维度展示；支

		持多维度威胁源画像分析，支持对全部资产进行画像分析，支持以列表形式展示资产相关信息。
		7.支持内置多种分析模型，包括但不限于 FTP 登录失败、敏感文件信息泄露、成功暴力破解、文件上传漏洞等。
		8.支持自定义资产设备拓扑，支持在拓扑图中查看设备的基本信息；
		9.联动处置：支持安全事件威胁处置功能，包括展示风险主机和攻击 IP。支持对攻击 IP 进行处置，包括封堵时间、网侧处置联动设备选择、端侧处置联动设备选择。 支持联动已有的下一代防火墙、WEB 应用防火墙等安全设备下发安全策略（IP 封堵与解封），支持联动漏洞扫描设备下发扫描任务，且联动功能应兼容第三方设备。

3.7.2 安全态势探针

序号	指标项	指标要求
1	基本要求	★采用国产 CPU 和操作系统（国产化软件具有软件著作权），≤4U，配置不少于 1 个管理口，不少于 1 个 HA 口，≥4 个千兆电口，≥4 个千兆光口，≥2 个 10G 光口，每个光口配置 1 个相同传输速率的多模光模块。硬盘≥16T,冗余电源，≥2 个扩展槽位,综合威胁检测能力≥2Gbps，TCP 最大并发连接数≥100W。默认含 3 年打包升级许可，包含攻击检测规则库、应用识别库、威胁情报库、URL 分类库。
	功能要求	1.支持能够检测包括扫描探测、暴力猜解、拒绝服务攻击、后门控

2		制、溢出攻击、代码执行、非授权访问、注入攻击、URL 跳转、跨站攻击、WebShell、浏览器劫持、文件漏洞攻击、工控漏洞攻击、物联网漏洞攻击等在内的 15 大类超过 13000 种以上网络攻击事件。
		2.支持针对邮件、文件、远程访问、数据库、WEB 应用等协议类型进行暴力破解检测，包括 SMTP、IMAP、POP3、FTP、SMB、TELNET、LDAP、ORACLE、MYSQL、MSSQL、MONGODB、POSTGRESQL、DB2、REDIS、HTTP 等协议的口令暴力破解行为。
		3.采用僵尸主机与控制主机异常通信行为检测的方式，能够对多种僵尸主机行为进行监测。
		4.支持对网络中传输的异常流量进行检测，包括服务器非法外联、DGA 域名、DNS 隧道、HTTP 隧道、加密流量、邮件监测、异常行为等异常流量类型。
		5.支持对恶意程序实现机器学习检测、内置虚拟沙箱检测、YARA 检测等多种检测方式，并且多种检测方式相互独立、互不影响，可对检测到的恶意文件设置相应警告、联动阻断动作；支持专业沙箱设备联动检测。
		6.本地嵌入独立的威胁情报库，不依赖其他设备或情报平台，即可独立的实现威胁情报检测能力，可对检测到的恶意文件、恶意 IP、恶意域名、恶意 URL、恶意邮箱设置相应捕获/取证、联动阻断动作。
		7.支持全流量取证，将事件发生前后的流量一起留存，支持攻击取证、僵尸主机取证、恶意程序样本、恶意程序无风险样本、威胁情

		报样本、威胁情报取证、WEB 防护取证、异常流量取证，取证类型支持报文取证和样本文件取证两种形式。

3.8 应用安全等级（三级）检测

序号	指标项	指标要求
1	基本要求	1.指定系统提供等级保护备案服务； 2.获取公安部门颁发的《等级保护备案证明》
2	服务质量	**测评机构项目组人员资质要求，参与项目测评的测评师数量和等级应与被测对象等级保护级别（三级）相符：** **1.** 实施三级项目测评的测评师应不少于 4 名，其中高级测评师、中级测评师应各不少于 1 名。 2.测评师的测评能力应得到保障，按要求参加培训，持等级测评师证上岗。 3.应配置专职渗透测试人员至少 1 名，根据采购单位要求视情开展渗透测试。 4.投标供应商配备测评售后服务组，设立 7×24 小时服务热线，在测评结束后免费提供关于本次技术服务内容的远程支持与技术咨询服务，协调各方资源解决采购单位问题；远程支持需求在 30 分钟内予以响应和回复，一般性问题当场解决，需要现场解决的，在 2 小时内安排上门服务。 5.测评内容 由具有资质的测评机构，依据国家信息安全等级保护制度规定，按照有关管理规范和技术标准，对采购单位互联网

		的安全物理环境、安全通信网络防护设计、安全区域边界防护设计、安全计算环境防护设计、安全管理中心设计等方面的运行状况进行检测评估。
3	安全及保密	1.确保测评工作的安全、规范，测评工具和方法要在双方认可的情况下使用，不对被测评系统运行造成影响，工作结束后不驻留任何程序并销毁不需要的文档和资料。 2.在测评实施前签订保密协议，对于测评过程中取得的相关敏感信息严格保密不外泄，现场实施人员接受采购单位管理。

3.9 应急响应预演

序号	指标项	指标要求
1	基本要求	根据应急预案设计应急预演活动，各参演人员根据预演计划进行应急预案的宣贯和突发网络安全事件的应急预演，使用通用漏洞环境场景进行攻击、监控、应急处置的演示。自行搭建应急预演平台，提供预演所需所有软硬件资源。 本次应急响应预演一年一次，共分为 5 次。一年内预演（包括但不限于）以下几种场景： 1.恶意程序事件包括计算机病毒、网络蠕虫、特洛伊木马、僵尸网络。 2.网络攻击事件包括安全扫描器攻击、暴力破解攻击、系统漏洞攻击。 3.网站及 Web 应用安全事件包括网页篡改、网页挂马、非法页

		面、Web 漏洞攻击、网站域名服务劫持。 4.拒绝服务事件包括 DOS 和 DDOS 大流量攻击事件。
2	安全及保密	1.确保预演工作的安全、规范，预演工具和方法要在双方认可的情况下使用，不对预演系统运行造成影响，工作结束后不驻留任何程序并销毁不需要的文档和资料； 2.在预演实施前签订保密协议，对于预演过程中取得的相关敏感信息严格保密不外泄，现场实施人员接受采购单位管理。

3.10 技术服务力量

指标项目			技术要求
1	集成要求	实施	提供实施服务。
		布线上架	按采购单位要求完成所有设备的上架安装和综合布线工作。
		系统集成	配合采购单位完成的整体集成、联试等相关工作。
	安全服务要求	资产梳理	首次进行服务范围内资产的全面梳理（梳理的信息包含不限于终端资产状况，包括硬件、软件和操作系统的等详细信息；终端资产与终端用户实名制管理。系统运转的操作系统、数据库、中间件、应用系统的版本，类型，IP地址；应用系统管理方式、资产的重要性以及网络拓扑），并将信息汇总至综合分析报告进行管理。
		安全设备管理	对设备的物理运行情况、清洁情况、系统运行情况、系统资源利用情况、系统运行日志、物理保护环境等

指标项目			技术要求
			进行检查并记录，并及时对系统进行软件升级，排除可能存在的安全问题和隐患。每月对设备配置、日志进行一次备份。
		安全策略管理	对安全设备业务访问策略进行梳理分析，发现过期、冗余、无效、不明确用途等策略，根据分析结果提供优化调整建议。
		安全培训服务	为满足系统使用要求,培训材料包括但不限于全运维、渗透测试、网络攻防、移动安全、逆向分析、安全工具、应急响应、代码审计、无线安全等。
2	技术服务力量	驻场运维具体要求	1.人数及服务时间：提供不少于1人的驻场运维人员，服务周期不少于一年。 2.驻场运维人员的资质要求： ★（1）教育背景与工作经验：具有计算机或相关专业的本科及以上学历，并且有相关的工作经验。（投标供应商需提供承诺书并加盖公章） ★（2）专业资格与技能：持有相关的专业资格证书，驻场人员资质：具备CISP认证证书或华三（H3CNE、H3CSE）、华为（HCIP、HCIE）、锐捷(RCNP、RCIE)任意一种网络工程师认证证书。（投标供应商需提供承诺书并加盖公章） （3）技术能力:具备扎实的技术能力，包括但不限于

指标项目			技术要求
			网络建设架构、安全防护、系统维护、数据库管理等。 （4）沟通能力与团队合作：具有良好的沟通和团队协作能力，具备工作责任心和服务意识，以确保能够有效地协调和沟通。 （5）应急处理能力：能够及时处理突发的技术问题或安全事件，快速响应并采取有效措施。 3.驻场人员守则：（1）严格遵守采购单位的办公时间，不得迟到早退，对所担负的工作争取时效，不拖延、不积压；（2）遵守采购单位的一切规章制度及工作守则；（3）事假需提前一天向采购单位管理人员申请，得到采购单位管理人员同意后提交请假说明，让确认盖章。 4.中标供应商职责：（1）遇到驻场人员请假或提出辞职时，中标供应商需及时安排一名储备人员立即顶岗；（2）储备人员无论专业资质还是技术能力与驻场人员要求相当；（3）遇到采购单位要求驻场人员加班时，所产生的薪酬由中标供应商承担。
		驻场服务内容	1.基础环境运维：负责中心机房供配电系统、消防系统、精密空调系统、新风系统、视频监控系统、门禁系统维护等。

指标项目			技术要求
			2.硬件设备运维：负责主机设备、网络及网络设备、存储设备、安全设备、桌面及外围设备以及其他硬件维护。 3.负责WINDOWS/LINUX，包括国产化环境的性能优化、升级更新、故障处理、日常维护、监测分析和响应等工作；负责有关国产中间件性能优化、升级更新、故障处理、监测分析和响应等工作。 4.负责服务器及应用系统日志分析、故障排除、日常巡检、监测分析和响应等工作，保障各信息系统的稳定运营。 5.负责网络安全设备管理维护，进行安全漏洞评估及异常事件处理等工作。

关键性技术指标参数前标记“★”符号，重要技术指标参数前标记“▲”，一般性指标参数（即非“★”且非“▲”的参数）前不作标记。带“★”和“▲”条款需提供技术支持材料，其中技术要求明确了技术支持材料的按照要求提供；未明确的，投标供应商的技术支持材料可以从（不限于）以下支持材料选择：产品规格表、产品宣传彩页、技术白皮书、制造商官方网站发布的产品信息、说明书等或检测机构出具的检测报告等技术材料。

二、 商务要求

★（一）交付时间、地点和方式

1.交付时间：合同签订之日起30个日历日内采购清单内（防篡改系统、数据脱敏系统、数据防泄漏系统、应用安全网关、安全审计系统、运维管理系统、网络安全态势感知系统）所有货物到货；到货后30个日历日内完成安装及调试。

2.交货地点：江苏省南京市。

3.交货方式：中标供应商提供设备的各项技术性能指标必须达到合同规定的要求，应用安全等级检测和应急响应预演以采购单位通知为准。

（二）产品包装和运输要求

包装应适应于远距离运输、防潮、防震、防锈和防野蛮装卸等要求，以确保物资安全无损地运抵指定现场。由于包装防护措施不妥而引起的损坏、丢失由中标供应商负责。

（三）售后服务

★1.自交货验收合格完毕之日算起，所有货物质保期至少3年，在质保期内，投标供应商对提供的货物因产品质量而导致的缺陷，必须免费提供包修、包换、包退服务，因此导致的损失采购单位有权向中标供应商追偿。中标供应商在质保期内为采购单位免费提供软件升级、维护，对采购单位使用中的各类问题提供免费的电话咨询和免费现场支持服务。超出质保期后，终身提供技术支持维护，设备使用寿命期内，供应商应当提供上门维修服务，仅收取成本费。投标时需提供售后服务方案，包含不仅限于信息系统安全集成售后项目服务流程、信息安全产品电话维护流程、信息安全产品现场维护流程。

2.中标供应商需向采购单位提供不少于2次现场培训（含系统使

用、管理和维护等内容），培训地点由采购单位指定。

3.投标供应商须承诺，投标供应商须有常驻售后服务机构，对质保期内提供7×24小时原厂免费保修服务，电话响应时间不超过30分钟，故障解决时间不超过4小时，紧急故障2小时内到达现场解决。质保期满后，供货商应根据采购单位要求，参考市场价标准，以年服务费不高于采购合同价的标准继续提供质保服务。

4.中标供应商免费提供全方位技术培训，包括安装服务、试运行指导服务；中标供应商在现场根据本单位要求提供设备安装，确保学校运维人员具备系统使用运维能力；安装完毕后提供详细的操作演示视频、中文技术文档等。

★（四）知识产权和保密要求

1.投标供应商应当保证采购单位在使用该物资或其任何一部分时，不受第三方侵权指控。同时，投标供应商不得向第三方泄露采购机构提供的技术文件等材料。

2.中标供应商必须做出保密承诺，并与采购单位签订保密协议后方可签订合同。

3.基于项目合同履行形成的知识产权和其他权益，其权属归采购单位所有，法律另有规定的除外。

★（五）物资编目编码、打码贴签要求

本项目对物资的编目编码、打码贴签要求，投标供应商应当予以明确响应，相关费用包含在报价中。

★（六）付款及结算方式

1.付款方式

1.1 设备付款方式（防篡改系统、数据脱敏系统、数据防泄漏系

统、应用安全网关、安全审计系统、运维管理系统、网络安全态势感知系统）

1.1.1 合同签订设备到货并验收合格后付至设备合同款的 30%；

1.1.2 设备运行验收合格后付至设备合同款的 95%（预留 5%作为质量保证金）；

1.1.3 质量保证金在设备质保期满且无质量问题，采购单位在接到中标供应商的质量保证金返还申请后全额支付（无息）。

2.服务付款方式

2.1 应用安全等级检测付款方式

按照采购单位要求，五年内一共进行五次信息系统安全三级等级保护测评，每次费用按合同中该项单价进行支付，总共分五次支付。

2.2 应急响应预演付款方式

按照采购单位要求，每年进行一次应急响应预演，每次费用按合同中该项单价进行支付，总共分五次支付。

2.3 技术服务力量

按照采购单位要求，驻场服务完成且考核合格后，按合同中该项单价一次性支付。

★（七）履约保证金

中标供应商签订采购合同前，应当按总合同金额（投标总价）的5%向采购单位提交履约保证金。

1.设备验收合格后，返还设备合同款（防篡改系统、数据脱敏系统、数据防泄漏系统、应用安全网关、安全审计系统、运维管理系统、网络安全态势感知系统）5%的履约保证金；

2.合同全部履约完成并验收合格后，返还剩余服务合同款（应用

安全等级（三级）、检测应急响应预演、技术服务力量）5%的履约保证金；

（八）实施人员要求

中标供应商按照招标文件要求安排项目团队。团队中需配备一名项目经理和若干实施人员，所有人员需签订保密协议，方可进场实施。

（九）生产及安装调试等要求

投标文件中需提供项目实施方案，方案包含不仅于项目人员组织管理、实施进度安排、实施步骤、安全策略调优、系统试运行、项目验收、质量保证与安全监督体系等文档。其中人员组织管理需提供本次项目经理、产品实施人员名单。

（十）报价要求

1. 投标价格不得高于限价，高于最高限价的做无效投标处理。

★2. 报价包含运输费、培训费、设备安装调试费、质保期内硬件设备维护维修费用以及售后服务期内中标方提供技术服务支持产生的所有费用，报价必需列出采购内容中所有设备的单价。

（十一）验收要求

1.项目验收前，中标供应商需向采购单位提供编制成册的全部设备的装箱清单、合格证、用户手册、操作手册、测试报告、部署文档等各种资料（含电子文档）。部署文档包括：安装配置、账号登录信息、日常运维流程等。

2.按照采购技术指标以及合同要求进行项目验收。

3.采购单位在验收过程中，如发现有与合同规定不符的，应向中标供应商提出书面异议，不签发验收合格凭证；中标供应商应在收到采购单位书面异议3个工作日内予以纠正，并承担由此发生的一切费

用和损失。如果再次验收仍不合格，采购单位有权取消或解除采购合同，由此造成的损失，由中标供应商承担一切费用和损失。

4.在验收合格之前，因中标供应商的原因进行设备或部件更换、部件维修所发生的费用，包括部分设备或部件维修及往返需求单位现场的费用、运输及保险费将由中标供应商承担。

5.验收方式：按照合同要求进行项目验收。

三、 投标供应商资格条件

（一）具有企（事）业法人资格（有行业特殊情况的银行、保险、电力、电信等法人分支机构，会计师、律师等非法人组织，行业协会等社会团体法人除外）；

（二）国有企业；事业单位；军队单位；成立三年以上的非外资（含港澳台）独资或控股企业，国内市场无类似或可替代产品的企业除外；

（三）具有良好的商业信誉和健全的财务会计制度；

（四）具有履行合同所必需的设施设备、专业技术能力、质量保证体系和固定的生产经营、服务场地；

（五）有依法缴纳税收和社会保障资金的良好记录；

（六）参加军队采购活动前3年内，在经营活动中没有受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款（200万元以上）等重大违法记录；

（七）未被中国政府采购网（www.ccgp.gov.cn）列入政府采购严重违法失信行为记录名单，未在军队采购网（www.plap.mil.cn）军队采购暂停名单处罚范围内或军队采购失信名单禁入处罚期和处罚范围内，以及未被“信用中国”（www.creditchina.gov.cn）列入严重失信

主体名单或国家企业信用信息公示系统（www.gsxt.gov.cn）列入严重违法失信名单（处罚期内）。

（八）单位负责人为同一人或存在直接控股或管理关系的不同供应商，不得同时参加同一包的采购活动。生产场经营地址或注册登记地址为同一地址的不同生产型企业，股东和管理人员（法定代表人、董事或监事）之间存在近亲属或相互占股等关联关系的不同非国有销售型企业，也不得同时参加同一包的采购活动。近亲属指夫妻、直系血亲、三代以内旁系血亲或近姻亲关系。

（九）法律、行政法规规定的其他条件。

（十）本项目特定资格：投标供应商具备有效的武器装备科研生产单位二级（或以上）保密资格证书或涉密信息系统集成资质证书乙级（或以上）资质。