北京航空航天大学网络信息中心工作专网安全接入与终端隔离设备采购

更正公告

一、项目基本情况

原公告的采购项目编号：2607-HXTC-IU1453

原公告的采购项目名称：北京航空航天大学网络信息中心工作专网安全接入与终端隔离设备采购

首次公告日期：2026年08月06日

二、更正信息

更正事项：采购文件

更正内容：

1、第五章采购需求 二、技术要求 技术指标：零信任网关和沙箱

更正为：

序号	产品名称	重要性	指标项	指标要求
1	零信任网关	*	密码合规	产品须支持SM1、SM2、SM3、SM4等国密算法及相应的加密算法套件。具备国家密码管理局商用密码检测认证中心颁发的《商用密码产品认证证书》，且密码模块安全技术要求达到第二级及以上。
2		*	安全合规	产品具有公安部颁发的《网络安全专用产品安全检测证书》或销售许可证、国家版权局颁发的《计算机软件著作权登记证书》；产品具备IPv6协议一致性测试和IPv6互联互通测试，具有良好的一致性和互通性，具备IPv6 Ready Core Protocols Logo（Phase-）认证；系统整体架构设计须符合国家网络安全等级保护第三级要求。

3		#	基础架构与部署	设备需在在机房以硬件形式部署网关等设备，且必须配备双电源或冗余电源。 设备须支持软硬件自检功能（包括密码算法加解密测试、哈希计算测试、软固件完整性检查等），确保底层物理运行稳定。 设备具有统一后台，管理 PC 和移动端，内置系统所需的组件（操作系统、中间件与数据库等）。
4		#	性能/并发指标	系统（含零信任接入）须支持不少于 2000 个终端的并发在线接入与安全访问。 网关加密流量≥480 Mbps。
5		*	高可用/集群部署/授权漂移	控制中心与代理网关须采用本地集群或高可用部署方案。 本项目实际交付物理节点≥2 个 集群各节点授权数共享，总授权数等于各节点之和。 集群节点故障后可实现授权漂移，剩余节点自动接管业务，集群总授权数保持不变。
6		#	零信任接入/SPA	支持 SPA 单包认证，支持系统业务端口隐藏，终端在 SPA 敲门前无法访问特定 TCP 端口。 网关和客户端双向强身份认证。 支持在回包中直观提示 SPA 登录失败的故障原因，提升排障效率。
7			加密隧道	零信任客户端与零信任网关之间建立应用级国密加密隧道（GM/T 0024/0025 标准）。
8			私有 DNS 与隧道代理	支持通过隧道模式代理业务访问；支持 TCP/UDP/ICMP 隧道代理；IPv4/IPv6 地址/范围/网段；域名及通配符域名；同一资源多地址；支持以私有 DNS 方式发布内部资源，终端用户无需修改 DNS 配置即可顺畅访问。

9		#	虚拟网络域与隔离	支持对终端出、入站网络规则划分虚拟网络域进行管控。支持“单网通”隔离模式，同一终端同一时间只能访问一张网络或指定的应用系统，并支持基于进程、IP 段的例外放行策略。 同一终端关联≥6 个虚拟网络域，支持悬浮球/任务栏切换，适用 Windows/麒麟/统信等系统
10			同步与关联管理	支持周期自动从学校数据中心数据库同步组织架构和人员信息，支持中间表推送或拉取方式。或联动本项目其他组件实现数据同步。
11			账号权限管理	提供账号权限管理能力，可对账号的访权限做出设置，实现沙箱内应用访问、文件传输等行为可控; 支持账号行为审计，确保身份鉴权与权限变更可追溯。
12			HTTP 优化	支持 HTTP 请求和响应改写、HTTP 反向代理转发和 HTTP 重定向等，更好地支撑业务系统对接。
13			全流量加密	网关可实现全流量加密，支持自适应用户—网关、网关—应用的前后端 TLS 和国密 SSL 握手能力，同时支持会话级事件证书或代理证书一次一密向后端传递用户真实身份。
14	沙箱		沙箱模式	交付时或者中标后 3 个月内需提供以下功能: 支持桌面沙箱、窗口沙箱两种运行模式，可以通过策略配置指定终端电脑沙箱以桌面沙箱或窗口沙箱模式运行。 若只支持其中一种运行模式，另外一种运行模式可在中标后 3 个月内提供。

15		*	沙箱模式与数据隔离	提供轻量化沙箱技术，无需额外服务端。沙箱应支持 Windows7/10/11 系统，以及统信 UOS、麒麟 Kylin 等国产化系统。 沙箱支持网络隔离、进程隔离、数据隔离、注册表隔离等功能。 沙箱桌面与普通桌面数据严格隔离存储，普通桌面无法查看沙箱桌面文件。 通过任务管理器可查验进程级用户会话（Session）隔离。 普通资源管理器绝对禁止查阅沙箱密盘，沙箱内应用亦无法另存数据至普通桌面存储分区。 本项目实际交付 pc 终端沙箱并发数量≥500 个,移动端沙箱并发数量≥200 个。
16			独立加密存储区	PC 终端创建独立数据存储隔离区域（安全密盘），沙箱未启动/卸载/PE 系统无法查看
17			数据加密与数据擦除	提供安全沙箱数据清理能力，支持管理员对特定沙箱执行数据擦除。
18			文件另存限制	授权应用打开沙箱文件无法另存到沙箱外，另存为选择框看不到普通磁盘分区
19			审批导出	支持沙箱内文件审批带出，对单次文件导出的数量、大小进行限制; 支持多级会签／或签等自定义审批流程。
20			环境约束与防卸载	支持控制台配置沙箱程序仓库（黑白名单），限制沙箱内外程序的违规运行 沙箱客户端支持本地防卸载功能（卸载须校验卸载码）

21			外设管控	交付时或者中标后 3 个月内需提供以下功能: 支持沙箱外设管控，支持精细化的 USB 设备黑白名单与导入导出规则。 支持针对特定设备实现光盘刻录、打印（网络、直连）、U 盘使用的精细化管控 严禁蓝牙设备接入沙箱用于数据传输。 其中细化的 USB 设备黑白名单设置可在中标后 3 个月内提供。
22		#	打印审计	交付时或者中标后 3 个月内需提供以下功能: 提供打印审计功能，记录打印时间、用户名、打印机名称、打印文件名称、文件大小等信息。
23			拷贝管控	交付时或者中标后 3 个月内需提供以下功能: 支持区分控制剪切板内向外、外向内拷贝。 其中剪切板内向外拷贝控制可在中标后 3 个月内提供。
24			沙箱截屏控制	沙箱窗口禁止截屏，截屏无法截取沙箱窗口，不影响沙箱外截屏
25			网线直连防护	支持防止 PC 终端通过网线直连其他 PC 电脑、仿冒 IP 实现数据越权传输或访问等。
26		#	移动沙箱与管控	内置移动端安全沙箱（支持 Android、鸿蒙系统） 移动沙箱支持防截屏、录屏管控、文件读取控制、内容分享控制、数据拷贝控制、应用水印等功能。 提供移动端沙箱 SDK 模块，供学校自研 APP 集成防护能力。 移动沙箱接管沙箱内所有数据的访问权限，采用路径重定向技术进行了数据隔离。
27			移动端远程管控与信息通知	移动沙箱内应用通过沙箱 APP 发送手机消息通知; 支持远程注销设备、系统消息推送、开关设备安全隧道等功能

28		#	水印与溯源	交付时或者中标后3个月内需提供以下功能: 支持屏幕明文水印与盲水印（矢量点阵水印）溯源。 支持基于HTTP／HTTPS包头自定义字段及网关颁发虚拟IP进行底层安全事件溯源。 支持虚拟IP溯源功能：虚拟IP应由网关颁发，不允许采用虚拟网卡形式，在终端生成虚拟IP，有客户端场景，无客户端场景，均支持基于虚拟IP进行安全事件溯源。 支持将认证及策略请求流量解密后镜像给外部态势感知系统，以完善系统的用户行为审计溯源能力。 其中盲水印（矢量点阵水印）溯源可在中标后3个月内提供。
29		*	多因素认证	支持多因素认证，第一因素为口令，第二因素可选短信验证码、数字证书、生物特征（移动端）等方式
30			认证协议支持	支持OAuth2/OIDC/SAML/LDAP/CAS等主流认证协议
31			证书双向认证	支持RSA/SM2国际和国密用户证书，实现网关和客户端双向强身份认证
32		*	免密与单点登录	支持一次认证，同步完成零信任、沙箱、业务系统单点登录。
33			应用授权(按组织/角色/用户)	直接在应用授权界面分配授权给组织架构/角色/用户，显示授权数量
34			持续信任评估	提供多维度的终端安全评估（防病毒软件状态、注册表、系统服务变更等）。系统可依据安全评分与风险等级，动态执行账号锁定、二次认证、禁止接入等管控动作。
35			同步与关联管理	支持周期自动从学校数据中心数据库同步组织架构和人员信息，支持中间表推送或拉取方式。或联动本项目其他组件实现数据同步。

36			账号权限管理	提供账号权限管理能力，可对账号的访权限做出设置，实现沙箱内应用访问、文件传输等行为可控;支持账号行为审计，确保身份鉴权与权限变更可追溯。
37			三员分立	管理后台必须实现系统管理员、安全管理员、安全审计员的“三员分立”模式。系统管理员、安全管理员、安全审计员的权限完全互斥，严禁一人兼多职。
38			应用访问控制	沙箱内打开的授权应用，只能访问授权的网络地址，禁止访问非授权网络地址；沙箱外的禁止访问授权沙箱访问的网络地址
39		#	性能/并发指标	须支持不少于2000个终端的并发在线接入与安全访问。
40		#	同步与关联管理	支持周期自动从学校数据中心数据库同步组织架构和人员信息，支持中间表推送或拉取方式。或联动本项目其他组件实现数据同步。
41	统一认证对接		安全基线强制控制	系统须支持强制首次登录修改密码、密码复杂度设置（字母／数字／特殊字符限制）、弱密码检测及登录失败试错锁定功能，防范弱口令爆破。
42			异常行为检测及处置	交付时或者中标后3个月内需提供以下功能: 具备暴力破解检测、同一个账号不同设备同时在线检测、短时间异地城市变更检测及缓慢攻击检测能力。触发风险事件时，支持自动执行安全编排动作（禁用用户、开启用户隧道限制、强制要求短信二次校验、邮件告警等）。
43	其他服务		国产化兼容	提供所有产品应支持国产系统包括麒麟、统信、华为鸿蒙等，支持国产CPU包括龙芯/飞腾/鲲鹏/兆芯/海光/海思麒麟等

44			终端盘点与自助排障	交付时或者中标后3个月内需提供以下功能: 支持采集终端硬件（主板、CPU、网卡MAC等）与软件台账信息上报。提供终端一键诊断排查工具（检测网络连通性、注册表、安全组件状态），支持一键修复，减少运维工作。 其中终端一键诊断排查工具可在中标后3个月内提供。
45			门户UI定制化	支持对登录页、Logo等进行修改。 支持修改提示文案并增加外部链接。 支持快讯展示，支持接收消息通知及消息提醒。
46			审计与日志	交付时或者中标后3个月内需提供以下功能: 支持对设备自身的安全状态和策略配置进行巡检，对设备的整体状态进行打分，统计所有检查的正常项、异常项和告警项，并输出巡检报告。 支持记录用户登录日志（登录、注销，含MAC地址、终端类型、浏览器类型等）; 支持记录管理员操作日志（含管理员、接入IP、时间、管理行为、对象）; 支持将具有异常登录行为的用户日志自动打标签为用户安全日志，用户安全日志包括但不限于: 帐号安全（应包含帐号首次登录、异常时间登录、非常用地点登录、弱密码登录、爆破登录、闲置帐号登录、帐号在新终端登录等）、中间人攻击、SPA安全（应包含SPA端口扫描、SPA爆破攻击、SPA敲门伪造、SPA重放攻击、SPA安全码泄漏等）、cookie劫持等 支持将记录设备安全事件日志，事件类型包括但不限于: 接口扫描、接口webshall攻击、接口参数爆破、接口越权调用等设备API防护日志。 除记录用户登录日志和记录管理员操作日志功能外，其他需求可在中标后3个月内提供。
47			单一客户端体验	零信任接入、安全沙箱、防病毒能力须使用统一客户端形态交付，减少终端资源占用。

48	运维保障	#	日志留存与维保服务	用户访问日志、操作日志、安全日志至少存储180天。
49			兼容性开发	沙箱需要对已有的标识系统和防护软件提供兼容性开发服务

2、第五章采购需求 三、商务要求 3. 售后服务（质保期）：

质保期更正为：本项目软件授权为永久授权，不得设置使用期限。 投标人为本次采购的全部硬件设备、软件系统及相关授权提供自验收合格之日起不少于三年的维保服务。

更正日期：2026年8月10日

三、其他补充事宜

本项目其他内容均不变。

校方编号：BUAABX20260033

四、凡对本次公告内容提出询问，请按以下方式联系。

1.采购人信息

名　　称：北京航空航天大学网络信息中心

地　　址：北京市海淀区学院路37号

联系方式：于老师，010-82314733

采购人业务监督联系人：庞老师，朱老师

联系方式：010-82314673，010-82314680

2.采购代理机构信息

名称：北京宏信天诚国际招标有限公司

地址：北京市海淀区复兴路乙12号中国铝业大厦11层1110室

联系方式：赵洁、吴众为、闫文娟、彭怡、成歌、刘京、修海龙、陈博维、姬小雪、王思晨、杨晓楠、王东衍、郝路、刘海英、孙佳、王亚东、黄艳、陈曦、吉国侠、孙银英、李秋萍、王艳艳、王改茹，010-63974645、63976753

3.项目联系方式

项目联系人：赵洁、吴众为、闫文娟、彭怡、成歌、刘京、修海龙、陈博维、姬

小雪、王思晨、杨晓楠、王东衍、郝路、刘海英、孙佳、王亚东、黄艳、陈曦、吉国侠、孙银英、李秋萍、王艳艳、王改茹

电　　话：010-63974645、63976753