附件 1

深圳市国资委网络安全加固项目采购需求

一、项目概况

为进一步落实《网络安全法》《网络安全等级保护 2.0》等有关规定，提升服务器与终端系统安全保障水平，加强国资委服务器和办公终端资产的安全防控能力，优化办公终端、服务器资产台账信息，解决终端和服务器病毒防护、挖矿行为检测、恶意文件鉴定、漏洞利用、后门文件留存、风险运营需求，通过本项目建立覆盖终端和服务器端的端侧防护运营体系；现拟以公开招标方式选定 1 家供应商为市国资委建设 1 套服务器安全管理系统和 1 套终端安全管理系统。请有意参加投标的供应商在市国资委网站（http://gzw.sz.gov.cn）获取采购需求，并带上统一社会信用代码证、法人授权书、有效身份证件等材料（盖单位公章）于 2022 年 8 月 16 日 14:30 时（北京时间）前递交投标文件。

二、评标定标方法

如通过资格审查的供应商不少于 3 家，市国资委将根据响应情况对各供应商进行评审（具体标准详见《深圳市国资委网络安全加固项目评审表》）后，采用综合评标法确定成交供应商。其中：

（一）评级档次中，得分高的供应商为候选中标供应商；

（二）如评级档次得分相同，则报价低的为候选中标供应商。

评标信息：

<table>
<tr><td>序号</td><td colspan="4">评分项</td><td>权重</td></tr>
<tr><td>1</td><td colspan="4">价格</td><td>20</td></tr>
<tr><td>2</td><td colspan="4">技术部分</td><td>50</td></tr>
<tr><td rowspan="2"></td><td>序号</td><td>评分因素</td><td>权重</td><td>评分方式</td><td>评分准则</td></tr>
<tr><td>1</td><td>技术规格偏</td><td>50</td><td>招标单</td><td>评审内容：</td></tr>
</table>

		离情况		位评分	投标人应如实填写《技术规格偏离表》，评审委员会根据技术需求参数响应情况进行打分，各项技术参数指标及要求全部满足的得50分，一般参数每项负偏离扣1分，带“▲”指标项为重要参数，对“▲”重要技术参数每负偏离一项扣3分，扣完为止，带“★”指标项为实质性条款，如出现负偏离，将被视为未实质性满足招标文件要求作投标无效处理。 证明材料：提供《技术规格偏离表》及相关证明文件并加盖投标人公章。
3	商务部分				30
	序号	评分因素	权重	评分方式	评分准则
	1	商务条款偏离表情况	13	招标单位评分	评审内容： 投标人应如实填写《商务条款偏离表》，评审委员会根据商务条款响应情况进行打分，各项商务条款要求全部满足的得13分，一般参数每项负偏离扣1分，扣完为止。 证明材料：提供《商务条款偏离表》及相关证明文件并加盖投标人公章。
	2	拟安排的项目经理情况（仅限一人）	4	招标单位评分	评审内容： 项目经理：投标人提供 1 名具有 ITIL（IT 服务管理）、CISAW(信息安全保障人员安全运维)、CISP 注册信息安全专业人员、PMP 项目管理等相关证书的项目经理，负责整个项目的规划和管理，项目经理同时具有上述四个证书得 4 分；项目经理同时具有上述三个证书得 3 分，项目经理同时具有上述两个证书得 2 分，其他情况不得分。 证明材料： 1.项目负责人必须为响应供应商自有员工，投标截止日前由投标人为其缴交的近三个月（具体指投标截止日所在月的上一个月起倒算）（已退休返聘人员需提供聘用合同），如开标日上一个月的社保材料

					因社保部门原因暂时无法取得，则可以往前顺延一个月；证明资料可为社保收缴部门盖章证明资料、社保窗口打印资料或社保官网截图； 2.须提供相关资质证书扫描件。
	3	项目实施与售后服务人员配备（3人）	3	招标单位评分	评审内容： 技术实施人员（项目负责人除外）：投标人为本项目投入至少3名技术实施人员，技术实施人员具有ITIL、CISP、华为HCIE三种证书中的任意一种，每提供一种得1分，全部提供得3分（同一人具有多个证书按一种证书计算，计1分），其他情况不得分。 证明材料： 1.上述技术实施人员必须为响应供应商自有员工，投标截止日前由投标人为其缴交的近三个月（具体指投标截止日所在月的上一个月起倒算）（已退休返聘人员需提供聘用合同），如开标日上一个月的社保材料因社保部门原因暂时无法取得，则可以往前顺延一个月；证明资料可为社保收缴部门盖章证明资料、社保窗口打印资料或社保官网截图； 2.须提供相关资质证书扫描件。
	4	类似项目业绩	4	招标单位评分	评审内容： 提供投标人 2019 年 6 月至投标截止日（以合同或协议签订日期为准）承担过的类似终端安全或服务器安全类项目，每提供 1 个得1分，本项最高得4分。 证明材料：提供项目合同（或协议）关键页扫描件，原件备查，否则不得分。如未按要求提供证明材料，或所提供的证明材料未能体现上述评分内容的，视为该证明材料无效。
	5	投标人资质情况	6	招标单位评分	评审内容： 1.投标人具有中国网络安全审查技术与认证中心颁发的信息系统安全集成服务资质证书，一级得 2 分，二级得1分，其它不得分； 2.投标人具有中国网络安全审查技术与认

					证中心颁发的信息安全应急处理服务资质证书，得 1 分； 3.投标人具有中国网络安全审查技术与认证中心颁发的信息系统安全运维服务资质证书，得 1 分； 4.投标人具有中国网络安全审查技术与认证中心颁发的信息安全风险评估服务资质证书，得 1 分； 5.投标人具有中国电子信息行业联合会颁发的信息系统集成及服务资质证书，得 1 分； 以上 5 项得分累计，最高得 6 分。 证明材料：提供在有效期内的相关证书扫描件，原件备查。如未按要求提供证明材料，或所提供的证明材料未能体现上述评分内容的，视为该证明材料无效。

三、采购清单

序号	项目类别	数量	备注
1	终端安全管理系统	1 套	含 1 套服务端管理中心软件和至少 310 个办公终端防护软件授权。 满足招标文件需求中技术要求。
2	服务器安全管理系统	1 套	含 1 套服务端管理中心软件和至少 130 个服务器端防护软件授权。 满足招标文件需求中技术要求。

四、供应商资格要求

1.在中华人民共和国国内注册的具有合法经营资格的法人或是具有独立承担民事责任能力的其它组织（提供营业执照或事业单位法人证书等证明资料扫描件，原件备查）；

2.本项目不接受联合体投标，不接受投标人选用进口产品参与投标；

3.参与本项目投标前三年内，在经营活动中没有重大违法记录（由供应商在《政府采购投标及履约承诺函》中作出声明）；

4.参与本项目政府采购活动时不存在被有关部门禁止参与政府采购活动且在有效期内的情况（由供应商在《政府采购投标及履约承诺函》中作出声明）；

5.具备《中华人民共和国政府采购法》第二十二条第一款的条件（由供应商在《政府采购投标及履约承诺函》中作出声明）；

6.未被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单（由供应商在《政府采购投标及履约承诺函》中作出声明）。

注：“信用中国”、“中国政府采购网”、“深圳信用网”以及“深圳市政府采购监管网”为供应商信用信息的查询渠道。

五、技术要求

说明：带“★”指标项为实质性条款，如出现负偏离，将被视为未实质性满足招标文件要求作投标无效处理。带“▲”指标项为重要参数，负偏离时依相关评分准则内容作重点扣分处理。其余为一般参数指标。

5.1 终端安全管理系统

类别	序号	功能参数描述
终端安全管理系统	1	管理中心系统软件，支持中标麒麟服务器 V7.0（龙芯 3B3000、鲲鹏 920）、银河麒麟服务器 V4.0（飞腾 FT1500A、FT2000+） 麒麟 v10 服务器（龙芯 3B3000、鲲鹏 920、FT2000+、兆芯 C/E）、UOS20 sp1 服务器（龙芯 3B4000、兆芯 C/E）、中科方德（龙芯、飞腾、申威、X86）等操作系统，可实现对客户端的集中管理，包括终端统一部署、策略配置、任务分发、集中监控、日志报表等终端安全管理功能。
	2	★提供≥310 个 PC 客户端授权，提供三年维保服务。
	3	客户端支持：windows PC 操作系统客户端、中标麒麟（龙芯、兆芯、申威、鲲鹏 920）V7.0、银河麒麟（飞腾 FT1500A、FT2000+）V4.0、银河麒麟 V10(龙芯、飞腾、X64)、银河麒麟(龙芯、飞腾、X64)V10.1、UOS20 sp1(龙芯、龙芯 3A5000、鲲鹏 920、麒麟 9006C、飞腾、X86、兆芯)、中科方德（龙芯、飞腾、申威、X86）等操作系统客户端。
	4	▲支持跨平台统一管理，控制中心可统一接入管理网络中的 WINDOWS 系统终端防病毒、类 LINUX 系统终端防病毒、信创通用终端、信创专用终端防病毒（ZYJ）。**（提供产品功能界面截图证明）**
	5	▲文件分发：支持文件分发到单个终端、部门终端、全网终端的功能，并支持分发到终端桌面、下载目录；支持文件分发落地后立即

		执行，指定时间执行，带参数执行；支持设置终端接收文件运行时需要终端确认、提示后自动运行、不提示。支持设置分发任务有效时间，如一周或者具体的制定日期时间。**（提供产品功能界面截图证明）**
	6	升级管理：支持对指定范围的终端下发升级主程序、升级病毒库、升级补丁库任务，支持查看终端版本分布、病毒库版本分布饼状图。
	7	支持控制中心数据库的备份及还原；支持定时备份；支持备份到指定 FTP 服务器。
	8	▲支持生效规则和生效时间条件设定，策略可以根据生效规则下发到不同范围类型的终端上去，同时可针对多个策略设置的不同的生效时间条件，确保策略在管理员指定的时间和条件范围内生效。**（提供产品功能界面截图证明）**
	9	支持对内置光驱的读取及刻录、USB 光驱的读取及刻录、U 盘的只读及写入、闪存的只读及写入、移动硬盘的只读及写入权限控制。
	10	支持对终端各种外设（USB 存储、硬盘、存储卡、软驱、光驱、打印机、扫描仪、磁带机、键盘、鼠标、红外、蓝牙、摄像头、手机、平板等）的使用进行权限控制。
	11	▲终端密码防护：支持防退出密码保护和防卸载密码保护，支持静态密码和动态密码。**（提供产品功能界面截图证明）**
	12	▲支持对终端进行 CPU、内存和磁盘占用的资源实时监测，并可将占用和使用情况上报管控中心。**（提供产品功能界面截图证明）**
	13	▲展示全网已部署终端数、在线率、运行天数、日均在线时长、待处理任务。**（提供产品功能界面截图证明）**
资质要求	1	▲所投产品厂商应具备较高的信息化能力和信用水平。投标人具备 ICSCE 信息化能力和信用评价证书。（提供有效证书复印件加盖投标人公章，原件备查，未提供或无法判断的不得分）
	2	▲所投产品厂商为 CNCERT 网络安全应急服务支撑单位（APT 监测分析）；（提供有效证书或者官方截图证明加盖投标人公章，原件备查，未提供或无法判断的不得分）
	3	▲所投产品厂商为 CVND 国家信息安全漏洞共享平台技术组成员单位，且近两年贡献排名前三。（提供有效证书或者官方截图证明加盖投标人公章，原件备查，未提供或无法判断的不得分）

5.2 服务器安全管理系统

类别	序号	功能参数
服务器安全管理系统	1	★提供≥130 个服务器端防护软件授权，提供三年维保服务。
	2	支持 windows/linux/中标麒麟等主流操作系统，包括但不限于以下操作系统：Windows Server 2003 SP2（x86/x64）、Windows Server 2008（x86/x64）、Windows Server 2012、Windows Server 2016、Windows Server 2019； RedHat 5.5~RedHat 5.11（x86/x64）、RedHat 6.0~RedHat 6.7

		（x86/x64）、RedHat 7.0~RedHat 7.2 RedHat8.0 ； CentOS 4.3~CentOS 5.11（x86/x64）、CentOS 6.0~CentOS 6.10（x86/x64）、CentOS 7.0~CentOS 7.6、Centos8.0； Ubuntu10.0 以上； Suse 10~Suse 10 sp3、Suse 11~Suse 11 sp3、Suse12；中标麒麟、红旗 Redflag3~4；。
	3	▲支持自我防护技术，即使客户端被意外关闭，防护依然有效。**（提供产品功能界面截图证明）**
	4	▲支持全量资产的关键字及语法搜索，支持检索的语法包括但不限于：服务器资产类、进程资产类、账号资产类、软件应用类、web 资产类、web 服务类、web 框架、数据库类、端口资产类、网络连接类、启动服务类、安装包类、计划任务类、环境变量类、内核类、类库资产类、注册表类、证书资产类进行检索。**（提供产品功能界面截图证明）**
	5	支持以列表的形式，统一列出 Windows/Linux 的硬件配置，并在列表中显示硬件配置，包括但不限于 CPU 品牌及核数、内存、硬盘容量、硬盘分区数、硬盘空间、硬盘使用率等信息。 支持梳理学习主机上的应用运行情况，并进行白名单管理，针对白名单外的应用告警。
	6	支持自动学习服务器的网络外连行为、命令执行行为、文件创建行为，并自动进行时序、归化处理。
	7	▲支持对操作系统、文件、软件中存在的后门进行检测，包括：发现时间、后门名称、后门类型、风险等级、服务器名称、服务器 IP、操作系统等，并可进行隔离、删除、加白、下载等操作，并提供后门的详情信息。**（提供产品功能界面截图证明）**
	8	可对服务器杀毒引擎进行综合的设置，支持本地查杀、控制中心查杀的设置与切换，并可对某台服务器的查杀规则进行详细设置。
	9	▲支持对暴力登录系统的账号进行自动发现并上报暴力破解入侵事件，支持对 RDP、SSH、FTP 等服务的暴力破解行为进行检测拦截，支持设定暴力破解行为的请求范围、失败次数，针对暴力破解的 IP 支持设定锁定时长。**（提供产品功能界面截图证明）**
	10	支持以违规登录视角对异常登录行为进行监控及告警，并可查看违规登录的账号、来源 IP、登录区域、服务器 IP、操作系统等信息，并可进行登陆规则策略的设置和告警设置
	11	支持以可疑登录的视角对可疑登录行为进行监控，包括登录 IP、发现时间等信息，并可创建可疑登录的监控规则和例外规则。
	12	▲支持对提权行为的事件进行监控及检测，并对提权事件进行进程阻断、加白等处置方式。**（提供产品功能界面截图证明）**
	13	支持记录当前所有服务器产生的事件日志，并提供筛选的功能和自定义时间段筛选查询，用户可通过安全日志快速锁定问题服务器，并进行相应处理。同时支持对安全事件进行溯源分析，对安全事件的等级、攻击类型、ATT&CK ID、ATT 攻击阶段进行匹配。
资质要求	1	▲所投产品厂商应具备较高的信息化能力和信用水平。投标人具备 ICSCE 信息化能力和信用评价证书。（提供有效证书复印件加盖投

		标人公章，原件备查，未提供或无法判断的不得分）
	2	▲所投产品厂商为 CNCERT 网络安全应急服务支撑单位（APT 监测分析）；（提供有效证书或者官方截图证明加盖投标人公章，原件备查，未提供或无法判断的不得分）
	3	▲所投产品厂商为 CVND 国家信息安全漏洞共享平台技术组成员单位，且近两年贡献排名前三。（提供有效证书或者官方截图证明加盖投标人公章，原件备查，未提供或无法判断的不得分）

六、商务要求

序号	目录	招标商务需求
（一）售后服务要求		
1	原厂商服务	1.1、提供不少于三年产品原厂商质保服务；
		1.2、产品原厂商质保服务包括但不限于提供三年软件版本及配套规则库免费升级维护，时间自最终验收合格并交付使用之日起计算；
		1.3、提供不少于三年的原厂商 7*24 小时免费服务支持。
2	服务响应时间	2.1、中标单位需要在系统出现故障 2 小时内响应，4 小时内解决；远程无法解决的，应该在 24 小时内到现场解决。
3	培训服务	3.1、原厂商工程师实施及提供系统相关的培训，提供原厂产品培训至少 1 次 。
（二）其他商务要求		
1	关于交货	1.1、交货期：合同签订后 15 日内交货；
		1.2、交货时间内，中标单位向用户交付试运行（不含试运行时间、项目终验）。交付内容包括但不限于用户指南、操作手册、安装指南和测试报告等；
		1.3、中标单位必须承担产品的运输、安装调试、验收检测等其他类似的义务；
		1.4、交货地点：深圳市福田区深南大道投资大厦 20 楼 2021 室；
		1.5、中标后建设方有权就以上招标产品的功能项进行验证，若发现与交付产品功能不符，可拒绝中标单位的产品，并向有关部门汇报中标单位的虚假应标情况。
2	关于验收	2.1、中标单位产品到达采购单位指定地点，经过双方检验认可后，签署项目到货验收报告；中标单位根据采购单位现有终端与主机情况完成系统整体规划，并完成产品的安装调试。
		2.2、服务事项完成后，中标单位应以书面形式向采购单位递交验收通知书，采购单位在收到验收通知书的 7 个工作日内，安排具体日期，由双方按照合同的规定完成项目验收。 当满足以下条件时，采购单位才向中标单位签发验收报告： a、2022 年 9 月 30 日之前完成所有服务事项：完成环境搭建、

		系统部署、客户端安装，提供病毒查杀、漏洞修复等功能，实现对服务器、终端统一安全管控； b、中标单位已按照合同规定提供了全部产品及完整的技术资料； 如不符合要求，供应商仍应予以整改，并承担相关费用，同时延长验收期限，直至项目完全符合验收标准。
3	报价要求	3.1、本项目预算金额：68 万元，含所有税费，超出预算的报价为无效报价。
4	其他要求	4.1、知识产权要求：为本项目设计的服务器安全管理系统、终端安全管理系统以及相关资料等，全部知识产权归采购单位所有。本项目使用的供应商已有知识产权产品，产权归供应商所有，但采购单位拥有免费使用权。