衡水市全场景疫情病原体检测信息系统扩容及网络安全设备采购项目

项目编号：HSZFCG2022G10120

合

同

书

甲方：衡水市卫生健康委员会

乙方：河北恒元网络有限公司

2022 年 12 月

目　录

甲方：衡水市卫生健康委员会

乙方：河北恒元网络有限公司

为有效提升衡水市全场景疫情病原体检测信息系统服务能力和网络安全水平，衡水市卫生健康委员会就衡水市全场景疫情病原体检测信息系统扩容及网络安全设备采购项目进行了政府采购（项目编号：HSZFCG2022G10120），项目名称为：衡水市全场景疫情病原体检测信息系统扩容及网络安全设备采购项目，河北恒元网络有限公司（以下简称乙方）中标该项目。现在平等合作原则下，经双方友好协商，订立如下合同：

一．合同总则

工程名称：衡水市全场景疫情病原体检测信息系统扩容及网络安全设备采购项目

二．合同范围

2.1 乙方负责甲方“衡水市全场景疫情病原体检测信息系统扩容及网络安全设备采购项目”的实施（产品详情见附件）。

2.2 乙方负责派遣专业技术人员实施本工程，施工完毕后，由甲方进行验收。

2.3 甲方根据乙方要求，负责协调双方人员的工作，以便施工顺利进行。

三．合同总价

3.1 本合同工程设备及安装费用总金额共计人民币 1946500 元，大写 壹佰玖拾肆万陆仟伍佰元。

四、付款方式

4.1 本项目根据进度支付项目款，项目验收合格后十日内支付100%项目款。

五. 工期

5.1 除去人力不可抗拒因素（如地震、水灾等）或甲方原因，乙方将在合同签订后30个工作日内完工。

5.2 乙方应按照双方约定的时间和进度实施完成本工程。

5.3 如因甲方原因或遇特殊情况，需延长或缩短工期的，甲乙双方协商解决，双方均不承担责任。

六. 工程实施和验收

6.1 甲乙双方共同确认施工环境符合要求。甲、乙双方应各派一名工作人员负责整个工程实施过程中的协调、安排。

6.2 具体工程实施计划由双方协商确定， 双方将严格按照实施计划进行工程的实施。

6.3 乙方应在工程实施完毕时通知甲方验收，乙方须采用专业的检测设备对整个工程进行检测，并出具电子及纸张介质的验收报告。

6.4 甲方需在工程完成5日内依据工程验收标准对工程进行验收。验收合格即向乙方出具工程验收合格证明；甲方超过7日不组织验收，视为乙方完成工程合格。

七. 双方责任

7.1 甲方给予乙方现场勘查的方便。

7.2 在工程施工中，甲方积极配合，为乙方顺利完成施工任务给予支持和方便。

7.3 乙方在施工中，甲方如提出更改设计施工方案，甲方应以书面形式提出，并写出要求，乙方认为可行后方可实施。

7.4 乙方在工程施工中，遇到意外或不可抗拒因素造成的困难，需对工程进度进行调整，必须书面向甲方提出，双方协商解决，并写出记录备查。

7.5 乙方在施工中应用的原材料和设备必须符合招标文件或甲方的要求。

八、不可抗力

8.1 合同生效后，合同任何一方由于不可抗力原因（即事先不能预见和人力无法抗拒的某种强制力量，如战争、水灾、台风、地震、政府行为及双方认可的其他情况等原因）而不能履行合同的，合同可延期履行，并根据情况部分或全部免予承担违约责任。

8.2 受不可抗力影响的一方，采取必要的补救措施，减少或减轻不可抗力造成的不良后果，尽力争取履行合同义务。

九、争议的解决

9.1 因执行本合同及本合同有关协议产生的一切争议，合同双方应首先友好协商解决，如经协商不能达成共识、双方应到甲方所在地的人民法院诉讼解决。

十、售后服务

10.1 服务时间：本次采购所需货物在合同签订后 30 个工作日内到货并完成安装调试，本项目的所有硬件验收合格后 3 年免费质保。

（1）本项目的所有设备提供 3 年免费质保，在接到用户故障报告后反应时间不多于 4 小时，修复时间不超过 12 小时，修复期间确保使

用不中断，并提供免费备件服务。

（2）在3年免费服务期中，乙方根据甲方或项目需要提供维修人员1人驻场进行技术支持，包括驻地技术服务、软件的操作培训等；

（3）乙方提供免费7×24小时电话技术支持，提供24小时内上门服务，在保修期内，提供免费上门维护服务，保修期外提供有偿维修。如设备出现重大故障，及时更换备件或提供备用机。非甲方人为原因而出现产品质量及安装问题时，负责包修、包换或包退，并承担因此产生的一切费用。

十一、违约责任

11.1 本合同签订后，双方严格恪守。任何一方违反本合同规定的义务给对方造成损失的，应承担赔偿责任。

十二、保密条款

12.1 甲方应履行保密义务，未经乙方书面许可，不得向其他泄露任何技术文件或合同有关的数据，包括合同本身。对于来自甲方或用户的有关保密信息，乙方须同样遵守本条的规定。

十三、合同生效及其他

13.1 本合同由双方法定代表人或授权人签署，加盖合同章或公章即生效。

13.2 对本合同条款的任何修改和补充，应由双方授权代表签署书面文件，作为本合同的组成部分，与合同正文具有同等效力。

13.3 本合同未尽事宜，双方可另行协商并签订书面补充协议。

13.4 本合同附件由双方签章确认，并与合同具有同等法律效力。

13.5 合同以中文书写，一式四份，甲乙双方各执一份，衡水

市政府采购办公室和衡水市公共资源交易中心各执一份。

甲方：衡水市卫生健康委员会　　乙方：河北恒元网络有限公司

授权代表人：　　授权代表人：

地址：　　地址：

电话：　　电话：0318-2063388

2020年1月4日

附件：

序号	产品名称	品牌	规格型号	技术参数	单位	数量
1	数据库安全审计系统	深信服	DAS-1000-B1500	1、性能参数：最大吞吐量2Gbps，最大纯数据库流量400Mb/s，数据库实例个数30个，SQL处理性能30000条SQL/s，日志检索性能500000条/秒。 2、硬件参数：1U规格，内存大小8G，硬盘容量2T SATA，冗余电源，千兆电口6个，万兆光口2个。 3、设备支持B/S管理方式，无需在被审计系统上安装任何代理；无需单独的数据中心，一台设备完成所有工作；提供图形用户界面，以简单、直观的方式完成策略配置、警报查询、攻击响应、集中管理等各种任务； 4、设备支持同时审计多种数据库及跨多种数据库平台操作；支持时间段、源IP、客户端程序、业务系统、数据库用户、数据库名、操作类型、表名、返回行数、影响行数、响应时长、响应码等对数据库日志进行精细检索；支持执行SQL语句失败分析，包括登录失败排行，SQL语句失败排行；支持自定义数据库安全策略，可根据业务需要自定义各种场景的安全规则，对于违规的数据库访问可进行实时警告和阻断； ★5、设备通过SQL串模式抽取保障磁盘IO的读写性能；分离式存储SQL语句保障数据审计速度快，支持基于SQL命令的webshell检测；	台	1
2	WEB应用防护系统	深信服	WAF-1000-B1400	1、性能参数：网络层吞吐量6G，应用层吞吐量430Mbps，并发连接数180万，每秒新建连接数6万。 2、硬件参数：1U规格，内存大小4G，硬盘容量64G SSD，千兆电口6个，千兆光口4个。 支持虚拟网线部署、透明部署、路由部署、旁路镜像等多种部署方式，适应复杂使用环境的接入要求。支持通过X-Forwarded-For、Cdn-Src-Ip、Clientip三种方式识别访问的源IP，并用于日志记录和联动封锁。 ★3、设备支持超过6200种防护规则。其中Web应用防护规则超过4900种，Web应用漏洞攻击防护规则超过1300种。 4、我司所投产品设备支持语义引擎用于检测Web攻击，能针对不同类型的Web攻击如命令注入攻击防护等，单独选择开启或关闭语义引擎检测。支持WEB弱口令检测、WEB登录明文传输检测、WEB口令爆破防护。 ★5、设备支持识别和拦截中低频、分布式等高级WEB口令爆破攻击方式。 6、支持用户登录权限防护，支持Web登录和非Web登录方式防护，支持短信验证登入。支持以安全策略模板方式快速部署安全策略，安全策略模板支持默认模板和自定义模板等多种格式。支持通过被动扫描功能，业务系统进行黑链检测、Webshell检测、漏洞风险检	台	1

				测、配置风险检测、弱口令账户检测。安全规则库支持在线自动升级、手动升级、云端实时升级等多种方式。产品支持系统配置自动备份功能，可通过备份文件快速恢复产品系统配置，降低管理员误操作引入的风险。支持语义引擎用于检测 Web 攻击，能针对不同类型的 Web 攻击如命令注入攻击防护等，单独选择开启或关闭语义引擎检测。 7、设备支持主备模式的双机部署，支持心跳线冗余，支持配置同步。支持业务模型学习监督功能，通过智能分析引擎对业务流量进行分析学习，建立用户业务特征模型，解决因 WEB 应用中因代码不规范和安全检测功能冲突导致的业务误判问题。		
3	终端安全管理系统（服务器杀毒）	深信服	EDR	1、本项目配置服务器端防护授权 30 个； 2、采用 B/S 架构的管理控制中心，具备终端安全可视，终端统一管理，统一威胁处置，统一漏洞修复，威胁响应处置，日志记录与查询等功能； 3、支持全网风险展示，包括但不限于未处理的勒索病毒数量、暴力破解数量、WebShell 后门数量、高危漏洞及其各自影响的终端数量； 4、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； 5、支持以安全策略模板方式对指定终端组快速部署安全策略，安全策略模板支持默认模板和自定义模板；支持安全策略一体化配置，通过单一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 检测和威胁处置方式、暴力破解的威胁处置方式和 Windows 白名单信任目录；支持对服务器重要目录进行权限控制，仅允许配置的可信进程操作该目录并提供配置指引；支持客户端的错峰升级或灰度升级，可根据实际情况控制客户端同时升级的最大数量，避免大量终端程序同时更新造成网络拥堵或 I/O 风暴；支持针对管理控制中心性能，安全事件，勒索病毒事件等邮件告警； 6、支持本地查杀缓存，具备二级缓存机制，可通过多维度引擎进行漏斗式检测，保障查杀效果在低误报率的情况下保持高检出率；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；支持展示终端检测到的暴力破解事件及事件详情，包括：攻击源、攻击类型、最后攻击时间、发现方式、攻击内容、攻击历史； ★7、支持展示终端检测到的 WebShell 事件及事件详情，包括：恶意文件名称，威胁等级，受感染的文件，	套	1

				发现时间，检测引擎，文件类型，文件名，文件Hash值，文件大小，文件创建时间；可配置WebShell实时扫描，一旦发现WebShell文件，可自动隔离或仅上报不隔离； ★8、支持管理平台向终端下发脚本(.bat,.sh和.ps1)执行文件，方便管理人员对终端进行脚本下发；支持与本次项目网络防火墙进行安全联动，管理员可以在网络防火墙管理界面下发快速查杀任务，并查看任务状态、结果并进行处置，支持在管理平台查询和统计联动信息。 9、业务系统详情支持展示流量分布Top5、我司所投产品设备业务流量排行Top5(发送，接收)、业务访问趋势（发送流速、接收流速和用户数）；支持图形化显示业务系统、服务器及流量详情；		
4	日志分析管理系统	深信服	SIP-Logger-A600	1、性能参数：默认包含主机审计许可证书数量50，最大可扩展审计主机许可数150，可用存储量64G minisata+2T SATA*2，平均每秒处理日志数最大性能1200； 2、硬件参数：2U规格，内存16G，硬盘容量64G minisata+4T SATA，千兆电口6个，万兆光口2个； 3、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720种日志对象的日志数据采集；支持对日志源的批量采集和日志源数据的批量转发； ★4、支持通过正则、分隔符、json、xml的可视方式进行自定义规则解析，支持对解析结果字段的新增、合并、映射； 5、支持日志文件备份到外置存储节点，支持NFS、NAS、ISCSI三种存储方式，并可查看外置存储容量、状态等信息；支持解码小工具，按照不同的解码方式解码成不同的目标内容，编码格式包括base64、我司所投产品设备Unicode、GBK、HEX、UTF-8等； ★6、支持单条事件进行展开，显示事件详细信息和事件原始信息，支持事件详情中任意字段作为查询条件无限制进行二次检索分析。 7、支持拓扑管理，能够基于拓扑图的资产相关数据信息快速查看资产评分、安全事件分布、告警分布等，支持通过拓扑下钻查看对应资产的关联事件、审计事件、日志数量；提供管理员账号创建、修改、删除，并可针对创建的管理员进行权限设置；支持IP免登录，指定IP免认证直接进入平台；支持只允许某些IP登录平台；支持页面权限配置和资产范围配置，用于管理账号权限，满足用户三权分立的需求；支持usb-key认证； 8、支持网站攻击、漏洞利用、C&C通信、暴力破解、拒绝服务、主机脆弱性、主机异常、恶意软件、账号	台	1

				异常、权限异常、侦查探测等内置关联分析规则，内置关联分析规则数量达到350条以上，支持自定义关联分析规则。 9、支持告警事件归并、告警确认和告警归档，支持基于频率、频次、时间的设定条件。日志进行归一化操作后，对日志等级进行映射，根据不同日志源统计不同等级下的日志数量。		
5	运维安全管理系统（堡垒机）	深信服	OSM-1000-B1150	1、1U规格，接口6个千兆电口，内存8G，硬盘容量2T SATA。 2、要求本次配置运维授权书50，最大可扩展资产数150，图形运维最大并发数100，字符运维最大并发数200。 3、支持通过协议前置机进行协议扩展，至少支持扩展KVM、Vmware、数据库、http/https、CS应用等； 支持从windows AD域抽取用户账号作为主账号，支持一次性抽取和周期性抽取两种方式；支持通过动作流配置提供广泛的应用接入支持，无论被接入的资源如何设计登录动作，通过动作流配置都可以实现单点登陆和审计接入； 4、支持批量导入、导出资源信息；支持手动添加、删除、编辑、查询资源，支持变更默认运维端口；支持一对一、一对多、多对多授权，如将单个资产授权多个用户，一个用户授予多个资产，用户组向资产组授权； ★5、支持在授权基础上自定义访问审批流程，可设置一级或多级审批人，每级审批可指定通过投票数，需逐级审批通过才可最终发起运维操作； 6、可以配置口令长度，是否包含字母及字母的长度，是否包含数字及数字的长度，是否包含符号及符号的长度，口令时效性，口令策略还可以配置禁止包含的关键字；支持命令黑命单，对字符型设备（如linux/unix/网络设备）的高危命令执行进行阻断，如rm、shutdown、reboot等； 7、对字符命令方式的访问可以审计到所有交互内容，可以还原操作过程的命令输入和结果输出，并支持通过搜索操作语句或执行结果中关键字定位审计回放； 全面支持IPV6，设备自身可以配置IPV6地址供客户端访问，并且支持目标设备配置IPV6地址实现单点登陆和审计； 8、支持web页面直接发起运维，无需安装任何控件，并同时支持调用SecureCRT、Xshell、Putty、WinSCP、FileZilla、RDP等客户端工具实现单点登陆，不改变运维人员操作习惯；支持从WEB管理界面重启、关闭设备。 ★9、全面支持Windows、linux、国产麒麟系统、Android、IOS、Mac OS等客户端操作系统下的H5页面	台	1

				一站式运维，实现跨终端适应性 BYOD（Bring Your Own Device；		
6	VPN 网关	深信服	VPN-1000-B1030	1、性能参数：理论最大 SSL 加密流量 100Mbps，理论最大 SSL 并发用户数 300，SSL 理论新建用户数 80 个/秒，IPSec 加密最大流量 70Mbps，IPSec 理论并发隧道数 3000，设备整机理论最大吞吐量 150Mbps，设备整机理论最大并发会话数 35w。 2、硬件参数：1U 规格，内存大小 2G，硬盘容量 64GSSD，单电源，千兆电口 4 个。专业 VPN 设备，采用标准 SSL、TLS 协议，同时支持 IPSecVPN、SSLVPN、PPTPVPN、L2TPVPN，非插卡或防火墙带 VPN 模块设备。 3、支持对基于 HTTP、HTTPS、FileShare、DNS、H.323、我司所投产品设备 SMTP、POP3、我司所投产品设备 Telnet、SSH 等的所有 B/S、C/S 应用系统，支持基于 TCP、UDP、ICMP 等 IP 层以上的协议的应用，例如即时通讯、视频、语音、Ping 等服务。支持终端使用包括 IE6、我司所投产品设备 7、我司所投产品设备 8、我司所投产品设备 10、11 或其他 IE 内核的浏览器，以及最新版本的非 IE 内核浏览器，如 WindowsEDGE，GoogleChrome，Firefox，Safari，Opera 最新版登录 SSLVPN 系统，登录后可完整支持各种 IP 层以上的 B/S 和 C/S 应用。支持用户登录界面、服务界面的完全自定义，上传单独的 Web 页面作为用户登录界面、服务界面。 ★4、提供环境检测、自动修复工具，支持对 Windows 的环境兼容性一键检测能力，以及对检测结果进行一键修复的能力，避免由于用户操作系统环境存在问题影响 SSLVPN 的使用，减轻运维工作。 5、我司所投产品设备产品应具有用户/用户组细粒度的权限分配功能：可以针对被访问资源的 IP 地址、端口、提供的服务、URL 地址等进行权限控制；针对同一 B/S 资源，可对不同用户做到细致到 URL 级别的授权。支持关键文件保护功能，可针对特定应用关键文件进行锁定，防止用户进行篡改进行越权。 ★6、支持设备自身的抗攻击防护，支持防 Host 头部攻击设置，用于防止 Host 头部攻击，设备只允许通过符合设置规则的地址进行访问；支持防 SWEET32 攻击设置，用于防止 SWEET32 攻击。 7、支持 15 级以上用户组树形结构分级管理，下级组可继承上级组的角色，资源及认证方式等属性。支持设置对控制台管理员密码复杂度的要求，提升设备的安全性。支持管理员使用证书/USB-KEY 认证；支持设置允许管理员登录的 IP 地址范围。 8、针对 B/S 资源支持 WebCache 技术，动态缓存页面元素，提高 Web 页面响应速度。支持流缓存技术，实现网关与网关、网关与移动客户端之间进行多磁盘、	台	1

				双向、基于分片数据包的字节流缓存加速，削减冗余数据，降低带宽压力的同时提高访问速度；支持共享流缓存功能，实现多分支网关在总部共享流缓存数据，提高流缓存效果。 9、支持密码找回功能，当用户的密码忘记或者丢失时，可自行找回密码，减轻管理员维护压力。支持HTP快速传输协议，大幅优化无线环境（CDMA、GPRS、WIFI、3G）、高丢包、高延等恶劣网络环境下传输速度及效率；支持根据网络境自动选择并切换至最优的传输协议。		
7	网络交换机	深信服	RS5300-28T-4F	1、性能参数：交换容量432Gbps，包转发率156Mbps； 2、硬件参数：自适应电口24个，万兆光口4个； ★3、支持胖瘦一体化，支持安全交换机和普通交换机两种工作模式，可以根据不同的组网需要，随时在控制器平台灵活的进行切换； 4、我司所投产品设备支持基于交换机单端口、聚合口的ACL策略，支持基于源目IP地址、MAC地址的ACL策略，支持基于协议（例如：OSPF、UDP、ARP），同时支持自定义协议号的ACL策略，支持基于时间的ACL策略，支持基于802.1p、IP及服务等级、DSCP的优先级设置。 5、支持M-LAG技术，跨设备链路聚合（非堆叠技术实现），要求配对的设备有独立的控制平面；为保证内网安全性，防止病毒在内网横向传播，要求交换机具有东西向风险流量安全功能；为禁止非法终端(例如私接路由器)接入，需支持终端类型库，能自动识别PC、路由器、监控终端设备等。 6、支持自定义交换机端口接入终端类型及MAC黑白名单；支持在控制器平台查看交换机面板端口接入状态、交换机容量、端口负载、供电负载；支持交换机端口终端类型变更后通过APP、短信告警；支持防网关ARP欺骗、管理员分级管理、端口保护、隔离、防止DOS、ARP攻击功能、CPU保护功能；支持通过控制器平台一键替换“按钮”即可完成故障设备替换；	台	1
8	集群服务器	华为	Atlas 800	1、品牌：华为，国产品牌；通用2U智能服务器； 2、处理器:2颗2.1GHz主频8Core处理器； 3、内存：128GB，工作频率2933MHz； 4、硬盘：2块1.92T NVMe硬盘；后置4*2.5寸硬盘背板1块； 5、配置独立RAID卡，支持 RAID 0/1/5/6/50/60(2GB缓存，超级电容）； 6、网卡：2个10GE 光口（含10GE多模光模块），2个GE 接口； 7、电源：2个2000W热插拔电源，并提供配套的电源连接线；	台	3
9	主从服务器	华为	Atlas 800	1、品牌：华为，国产品牌；通用2U智能服务器；	台	3

				2、处理器:2 颗 2.3GHz 主频 16Core 处理器; 3、内存：128GB，工作频率 2933MHz; 4、硬盘：2 块 1.92T NVMe；后置 4*2.5 寸硬盘背板 1 块; 5、配置独立 RAID 卡，支持 RAID 0/1/5/6/50/60(2GB 缓存，超级电容）; 6、网卡：2 个 10GE 光口（含 10GE 多模光模块），2 个 GE 接口; 7、电源：2 个 2000W 热插拔电源，并提供配套的电源连接线;		
10	数据服务器	华为	Atlas 800	1、品牌：华为，国产品牌；通用 2U 智能服务器; 2、处理器:2 颗 2.3GHz 主频 16Core 处理器; 3、内存：128GB，工作频率 2933MHz; 4、硬盘：2 块 1.92T NVMe；后置 4*2.5 寸硬盘背板 1 块; 5、配置独立 RAID 卡，支持 RAID 0/1/5/6/50/60(2GB 缓存，超级电容）; 6、网卡：2 个 10GE 光口（含 10GE 多模光模块），2 个 GE 接口; 7、电源：2 个 2000W 热插拔电源，并提供配套的电源连接线;	台	1
11	时钟服务器	宝瑞丰	FC-1006-PRO	1、网口 6 个; 2、串口 2 个; 3、卫星信号跟踪支持 GPS L1, BeiDou B1, GLONASS L1, Galileo E1, SBAS 等; 4、首次定位时间：热启动 < 2s；温启动 < 40s；冷启动 < 60s; 5、支持协议 NTPv2, NTPv3, NTPv4, SNTP;	台	1
12	数据交换机	华为	S6720-30C-EI-24S-AC	1、交换容量 2.5Tbps，包转发率包转发率 700Mpps。 2、端口配置 24 个万兆 SFP+端口，2 个 40G QSFP+端口，支持业务扩展插槽数 1，扩展后最大可支持 6 个 40G QSFP+端口。 3、支持 MAC 地址 288K，支持 ARP 表项 44K。 4、为了提高设备可靠性，支持可插拔的双电源。 5、为了保障业务稳定性，要求 10GE 端口转发时延<1μs。 6、配置双电源，10 个万兆多模光模块，4 个万兆单模光模块。	台	1
13	域名服务	华为	定制	1、我公司负责衡水市全员核酸检测信息系统的域名申请（最终域名名称由采购方确定）。 2、我公司负责协调对接好系统开发厂家相关域名服务的所有工作，并承担三年内所产生的所有相关包括申请、服务等费用。 3、我公司所选择的域名注册商是华为。	项	1
14	系统集成	定制	定制	我司所投产品含上述所有设备的系统集成、安装调试以及相关配件、辅材等。	项	1