终端安全管理软件采购比选文件

第一章 投标邀请

一、项目基本情况

（一）项目名称：中国保险行业协会终端安全管理软件项目

（二）项目预算金额：人民币 18 万元（壹拾捌万元整）

（三）采购内容：

序号	名称	数量	采购需求
1	终端安全管理软件	1 项	具体详见采购文件

（四）合同交货期限：合同签订后 30 天完成货物交付。

（五）本项目是否接受联合体投标：□是 ■否。

二、参加比选的资格要求（须同时满足）

（一）满足《中华人民共和国政府采购法》第二十二条规定；

（二）投标人不得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；

（三）供应商必须具有网络安全服务项目相关的技术服务能力；

（四）法律、行政法规规定的其他条件。

三、获取比选文件

详见比选公告。

四、比选单位递交比选文件时，必须提供如下证明资料：

（一）有效的营业执照或法人证书（复印件）；

（二）公司简介；

（三）法人授权委托书（原件）；

（四）被授权人身份证（原件及复印件）；

（五）供应商的资信证明：会计师事务所出具的最近一年度财务审计报告；

（六）依法缴纳税收的记录：最近半年内任意一个月的纳税有效凭据或相关部门出具的依法纳税有效证明文件，依法免税的，应提供依法免税的相关证明文件（复印件）；

（七）依法缴纳社会保障资金的记录：最近三个月内缴纳社会保障资金的有效票据凭证或由社保中心出具的缴纳社会保障资金的有效证明文件，依法免缴的，应提供依法免缴的相关证明文件（复印件）；

（八）参加本次采购活动前三年内，在经营活动中没有重大违法记录的声明（格式，原件，授权代表签字并加盖供应商公章）；

（九）原厂授权函及服务承诺函（原件及复印件）；

（十）比选文件要求或供应商认为必要的其他资格证明文件（复印件，加盖供应商公章）。

五、比选时间及地点：

（一）提交比选方案文件截止时间：2024 年 1 月 16 日 14 时 00 分（北京时间），逾期或不符合规定的比选文件恕不接受。

请供应商将密封好的有效比选书（正本一份、副本四份）、比选书电子版（一份）邮寄至：北京市丰台区金泽西路 2 号院 1 号楼（丽泽平安金融中心 A 座）501 室中国保险行业协会，联系人：王超，联系电话：010-66290204。

（二）比选文件开启时间：2024 年 1 月 17 日 15 时 00 分（北京时间）

（三）比选文件开启地点：北京市丰台区金泽西路 2 号院 1 号楼（丽泽平安金融中心 A 座）501 室，届时请参选单位派授权人参加比选。

（四）评标方法和标准：综合评分法。

六、公告期限

自本公告发布之日起 15 天。

七、联系方式

联系人：王超、刘坤

联系方式：010-66290204、66290493

地址：北京市西城区金融大街 15 号鑫茂大厦北楼 7 层

第二章 采购需求

一、项目概况

本项目为加强中国保险行业协会的终端安全管理能力，通过采购终端安全管理系统软件，保护协会的终端系统免受恶意威胁和网络攻击，保证协会信息安全。

二、总体要求

本项目需根据国家网络安全等级保护的相关管理与技术要求，结合中国保险行业协会终端现状，制定终端软件实施部署方案，并按照相关要求完成全部终端软件安装部署，安全策略调整，安全加固等工作。

三、项目主要商务要求

标的提供的时间	合同签订后 30 天内完成货物交付
标的提供的地点	中国保险行业协会
投标有效期	从提交投标（响应）文件的截止之日起 90 天
付款方式	合同签订后支付 50%，验收合格后支付 50%。
验收要求	满足招标参数要求，按期提供项目验收报告，按期完成所有服务。
履约保证金	不收取

四、项目具体技术要求（★为废标项）

（一）采购需求（以最终报价单选型为准）

项目	终端需求	数量
终端安全管理软件	办公终端（Windows 台式计算机、笔记本计算机）包含但不限于防病毒、补丁管理、软件管理、终端管控、移动存储管理、水印管理、终端审计等功能。	160
	主机终端（其中 Win Server 数量 20，Linux 数量 170），	190

	主要功能包含但不限于病毒防护、补丁管理、终端安全检测与响应（EDR）等功能。	
服务要求	三年原厂 7×24 软件支持服务。	

（二）功能要求

类型	技术指标项	指标要求
通用要求	基本要求	管理中心操作系统支持 Windows Server 2012 R2/2016/2019/2022 的 64 位版本；支持 CentOS 7 系统；
		支持 WinPC 客户端、WinServer 客户端和 Linux 客户端，需同台管理。
		★客户端主程序、病毒库版本支持按分组和多批次进行灰度更新，支持设置观察时长【提供功能截图】
		★支持终端“防退出”、“防卸载”密码保护、防安装密码保护。
WinPC	病毒防护	支持手动导入、导出黑白名单，添加黑白名单。
		扫描到病毒时，支持自动进入深度查模式，扫描时不允许终端用户暂停或停止扫描任务。
		支持对压缩包内的病毒扫描，可自定义配置压缩包的扫描层数，至少 10 层模式下的扫描。
		支持对进程防护、注册表防护、驱动防护、U 盘安全防护、邮件防护、下载防护、IM 防护、局域网文件防护、网页安全防护、勒索软件防护。
		支持僵尸网络攻击防护，对流出本机的网络包数据和行为进行检测，根据策略在网络层拦截后门攻击、C2 连接等威胁。
		★支持不少于三个杀毒引擎混合使用，提高病毒检出率。【提供功能截图】
	补丁管理	支持对 Windows 操作系统、IE、.NET Framework、Office、Adobe Flash Player、Adobe Acrobat 和 Adobe Acrobat Reader DC 等软件进行补丁修复。
		★支持管理员预先设置好灰度发布批次和漏洞修复策略，逐步验证并推送补丁到用户组，自动化编排完成漏洞修复。【提供功能截图】
		支持按照补丁的维度统计补丁安装情况，包括补丁号、系统类型、补丁类型、补丁级别、补丁名称、补丁描述、发布日期、漏洞 CVE 编号、漏洞 CNNVD 编号、未安装、已安装、已安装未生效、已排除、未更新补丁库。并支持导出统计报表。
	软件管理	★支持内置软件库，需包含 1000 款以上应用软件，类别包括：办公软件、图形图像、视频软件、压缩刻录、输入法、远程工具、浏览器、下载工具、编程开发、教育学习、阅读翻译、系统工具、主题壁纸、音乐软件、网络应

		用、聊天工具、安全杀毒等，以保证软件安装包无捆绑和病毒。【提供功能截图】
		支持软件分发功能，支持一次分发多款有依赖的软件。
		可统计本地软件统计时段内的打开次数和使用时长，用于统计高成本的软件的使用活跃度，为企业管理者提供采购参考。
	终端管控	支持外设库管理，可统计终端外接的各种设备，可禁止使用大容量 USB 存储设备（大容量设备自持自定义大小阈值）。
		★支持对外设进行多维度的放行，包括设备名称、PID/VID、实例路径，通过添加实现例外或加黑。【提供功能截图】
		支持终端进程红名单、黑名单、白名单功能。可保护核心进程不被结束。
		支持对互联网出口地址探测，支持对违规的互联网出口进行发现、断开网络、终端锁屏、断网+锁屏处理。支持例外白名单添加。
		★支持对终端节能管理，支持对长时间运行、定时关机、空闲节能、工作时间外开机等节能类型设定策略，并支持提示倒计时弹窗间。【提供功能截图】
		支持对网卡进行防护，支持阻止终端修改 IP 地址、使用动态 IP 地址、热点创建等。
	移动存储管理	支持对移动存储介质进行注册，支持授权、启用、停用、删除、取消注册等
		支持 U 盘与终端进行点对点的授权，可以灵活控制使用权限
		支持自动审批客户端注册请求；不同分组可设置不同审批规则
		★支持外出管理，并可以设置外出使用权限与有效时间【提供功能截图】
	水印管理	支持屏幕水印，支持自定义水印信息，可调整水印密度、大小。
		支持打印水印，支持打印结果附带图片背景水印，支持以二维码的方式展示水印信息。
		支持截屏暗水印，屏幕上无任何输出，截屏后的图片可溯源用户、终端等信息。
	终端审计	支持 HTTP/HTTPS/FTP/SMTP/共享目录/移动存储/光盘刻录/QQ/微信/企业微信/钉钉文件流转行为审计
		通过审计日志，通过文件唯一 ID 还原文件内部流转轨迹。
		支持对终端打印行为的日志审计。并可对打印文件进行归档。
		支持邮件审计；支持对 QQ、微信、企业微信和钉钉的即时通讯消息进行审计；支持网站访问审计。
WinServer	病毒防护	支持手动导入、导出黑白名单，添加黑白名单。

		扫描到病毒时，支持自动进入深度查模式，扫描时不允许终端用户暂停或停止扫描任务。
		支持对压缩包内的病毒扫描，可自定义配置压缩包的扫描层数，至少 10 层模式下的扫描。
		支持不少于三个杀毒引擎混合使用，提高病毒检出率。
	补丁管理	支持管理员预先设置好灰度发布批次和漏洞修复策略，逐步验证并推送补丁到用户组，自动化编排完成漏洞修复。
		支持开启自动修复漏洞，包括开机时修复，并支持随机延迟执行、间隔修复和按时间段修复，可设置延迟时间、间隔修复时间和修复时间段。
		允许终端用户手动修复漏洞，如果发现“修复内容”中设置的需要修复的漏洞和功能缺陷没有修复成功则提醒终端用户修复。
		支持展示终端信息、补丁号、补丁级别、补丁类型、安装日期、事件上报时间、事件类型、结果、详细描述。
		支持按终端统计补丁安装和生效情况，支持按照终端维度统计，统计每台终端的各个级别的补丁未安装数量，以及已安装、已安装未生效、已排除的总数量，并支持导出统计报表。
		支持按照补丁的维度统计补丁安装情况，包括补丁号、系统类型、补丁类型、补丁级别、补丁名称、补丁描述、发布日期、漏洞 CVE 编号、漏洞 CNNVD 编号、未安装、已安装、已安装未生效、已排除、未更新补丁库。并支持导出统计报表。
	EDR 能力	★支持采集的终端进程行为数据类型包括进程事件、IP 访问、DNS 访问、进程注入、注册表变更、文件操作、账户变更、邮件附件传输、U 盘文件传输、IM 文件传输、下载工具文件传输、浏览器文件传输、PowerShell 命令执行、命名管道事件、进程权限信息、WMI 事件、驱动文件加载、映像文件加载、无文件脚本执行、内网横向渗透、内存执行事件、账户登录登出、病毒防护事件。【提供功能截图】
		支持以树形结构展示威胁事件中文件的调用过程，包括进程上下文关系，进程网络访问、文件变更情况等。
		★可视化展示威胁告警在 MITRE ATT&CK 攻击模型中的覆盖情况，方便用户直观了解攻击者所应用攻击战术点和技术点，进而评估出攻击所处阶段和影响范围。【提供功能截图】
		对恶意文件进行处置，保证文件不能再次运行和执行，处置动作包括终止进程、终止进程并隔离、终止进程并删除、恢复隔离进程文件。
		★对全网终端进行威胁事件风险性评估。并支持一键响应处置能力。【提供功能截图】
		★用户可以通过可视化页面自定义创建规则、编辑规则、发布规则、删除规则，规则实体编写支持以进程、文件、注册表、网络连接等行为作为检测特征，对内置规则未覆盖的场景进行补充检测。

		支持将告警和日志通过 syslog 和 kafka 发送给第三方平台
Linux	病毒防护	支持手动导入、导出黑白名单，添加黑白名单。支持通过文件导入添加黑白名单。
		支持对压缩包内的病毒扫描，支持多层压缩包的扫描，可自定义配置压缩包的扫描层数，至少大约 10 层模式下的扫描。
		支持对进程防护、U 盘安全防护
		支持不少于两个杀毒引擎混合使用，提高病毒检出率。
	EDR 能力	支持采集操作系统的进程事件、IP 访问、DNS 访问、账户登录登出、文件操作、账户变更、U 盘文件传输、U 盘挂载/卸载、浏览器文件传输、驱动文件加载、映像文件加载。
		可视化展示威胁告警在 MITRE ATT&CK 攻击模型中的覆盖情况，方便用户直观了解攻击者所应用攻击战术点和技术点，进而评估出攻击所处阶段和影响范围。
		对终端进行断网操作，只允许与控制中心进行通讯，以避免影响其他终端，进而扩大安全事件影响范围。
		对恶意文件进行处置，保证文件不能再次运行和执行，处置动作包括终止进程、终止进程并隔离、终止进程并删除、恢复隔离进程文件。
		对指定终端当下的状态进行深入调查，包括终端登录日志、启动项、计划任务、正在运行的服务等，以及最近一段时间内终端的行为数据信息。
		对全网终端进行威胁事件风险性评估。并支持一键响应处置能力。
		用户可以通过可视化页面自定义创建规则、编辑规则、发布规则、删除规则，规则实体编写支持以进程、文件、注册表、网络连接等行为作为检测特征，对内置规则未覆盖的场景进行补充检测。
		支持将告警和日志通过 syslog 和 kafka 发送给第三方平台

（三）资质要求

产品资质	具备《计算机软件著作权登记证书》资质证书
	提供公安部颁发的《计算机信息系统安全专用产品销售许可证》
	连续通过国际权威杀毒软件评测机构 Virus Bulleti 测评认证（VB100）
	近三年 IDC 终端安全市场排名前三。
	IT 产品信息安全产品认证证书
	EAL3+国家信息安全测评信息技术产品安全测评证书

（四）服务要求

1．中选供应商所提供的软件符合信息产业部、国家版权局认可的正版软

件，产品包装应属于封装或安全未启用的状态。

2．中选供应商需承诺能够在中标通知之日起20个工作日内将所列软件产品（含产品规格说明、产品安装部署、日常管理、运行操作、版本更新等手册）送达甲方指定交货地点，双方确认软件清单或功能模块，确认软件产品符合项目建设需求。

3．在采购方能够提供软件更新升级的环境下，中选供应商保证软件产品到货后10个工作日内完成合同软件产品的安装或更新升级工作，并稳定运行，期间承担更新升级的一切费用。

4．中选供应商更新升级应用时必须以不影响局域网内其他软件或系统的运行为前提，并对有可能影响到的软件或系统采取良好的保护措施，以消除影响。

5．中选供应商对采购的软件产品提供包含全包式免费上门维护、免费巡检调优及其他技术支持等服务，并为采购方购买三年的原厂服务（中选供应商应于收到《验收合格报告》之日起三日内向甲方交付相关原厂纸质及电子证明文件），该原厂服务自采购方收到相关原厂证明文件之日起开始计算。

终端安全管理系统软件原厂服务具体如下：

（1）有效期内提供产品的大、小版本的免费升级；

（2）有效期内提供产品病毒库、各功能特征码等更新；

（3）远程诊断、电话及现场技术支持；

（4）解答客户有关产品使用中出现的问题；

（5）7×24原厂技术支持服务响应；

（6）经过注册获得原厂网站支持。

6．中选供应商在采购方提出技术支持要求后30分钟内响应；2小时内给出技术建议；若出现重大安全威胁（由采购方认定），则应在8个小时内到达

现场，24 小时内排除风险。

7．软件产品供货合同签订后付款 50%，产品到货后安装验收一个月后付款 50%。如报价中含有服务费，该项费用按年支付，最终以合同约定为准。

8．签署合同时中选供应商必须提供产品原厂商授权书，否则视为违约。

五、项目管理及服务要求

1．服务保证

应严格执行项目管理规定，从项目组织管理、项目进度管理、项目质量保障和安全保密等方面加强项目管理，确保服务质量。

2．质量保证

应建立严格的质量保证体系，制定项目建设的质量控制方案和实施措施，并督促落实各环节质量控制内容和目标；保证项目各个阶段工作满足招标方对质量的要求。

应根据项目的工作计划，对阶段性工作成果进行审核，并向项目单位提交里程碑式工作成果。通过保证各阶段性成果的质量，最终保证整个项目的质量。

3．工期保证

（1）在本项目合同签订之后，按合同约定完成相关工作

（2）项目进度管理应该遵循以下原则：

项目进度管理的依据是项目合同所约定的工期目标；

在确保项目质量和安全的原则下，控制项目进度。

（3）项目进度管理应该至少包含以下内容：

在了解项目详细情况后，按照合同约定工期制定具体实施计划，明确各阶段工作任务。

按照具体实施计划，定期跟踪检查，对可能发生的延误提出相应对策；定期或不定期地召开或参加项目例会、协调会议等，向招标方通报项目进展情况，提

交进度报告，及时解决相关问题。

4．售后服务

应建立统一的售后技术支撑服务体系，能够提供 5×8 小时售后技术及保障服务，必要时 4 小时内应到达现场。

5．服务期：自合同签订之日起 3 个月内完成相关工作内容并出具报告。

六、保密要求

1．组织保密要求

（1）成交供应商有责任对采购人提供的各种技术文件（软件、咨询报告、服务内容）与工作业务信息进行保密，未经采购人书面批准不得提供给第三方。如有违反，成交供应商应承担相应的法律责任。此保密义务不因合同的终止而免除。

（2）供应商必须与采购人签订《安全保密协议》。如有违反，成交供应商必须承担全部责任并赔偿采购人的一切损失，采购人有权追究成交供应商的法律责任并终止合同。

（3）成交供应商必须遵守采购人的各项规章制度，严格按照工作规范组织进行运维工作，制定切实可行的措施保障人员安全，设备安全，生产安全。

（4）成交供应商必须制定合理的措施对服务进行管理和思想教育，加强保密意识，安全生产意识。

2．人员保密要求

成交供应商应负责所有参与本次项目的员工严格遵守保密协议，如有违反，成交供应商必须承担全部责任并赔偿采购人的一切损失，采购人有权追究成交供应商的法律责任并终止合同。

七、其他要求

1．基本要求

（1）供应商应该提供满足本技术条款中要求的全部服务支持。

（2）本技术条款提出了最低限度的要求，供应商应保证提供符合本技术条款和行业标准的优质服务。

（3）本次采购项目建设成果的**所有权归采购人所有**。

2．服务承诺要求

（1）响应文件中提交项目成员名单，明确服务团队人员，且成交后未经采购人同意不得更换。

项目团队的总体要求，中标方按照用户要求开展服务，并在投标文件中建立合理的项目进度计划，详细阐述项目过程中各项服务如何开展、具体实施步骤、要求有标准化交付安全服务的效果评价方法。中标方需要派出强有力的人员组建成项目组，项目经理、技术负责人至少需要 3 年以上的相关项目工作经验。

项目团队需保持稳定，中标方应承诺项目经理、技术负责人等核心人员必须专职承担本项目工作，未经用户单位许可不得更换。中标方应明确项目经理和技术负责人在本项目中的岗位职责、任职资格及管理权限，并明确项目经理和技术负责人调动相关资源的权力，确保项目顺利实施。

（2）供应商应严格执行保密的有关规定，非经采购人书面同意，不得将本项目所有信息、资料向任何第三方披露、泄露。

（3）应保证提供的所有服务完全满足本技术条款要求。

（4）其他满足本次采购要求的承诺。

第三章 评分标准

序号	评分内容	明细内容	分值	评分标准
1	商务部分（16 分）	服务能力相关证书	8	1、供应商具有有效的信息技术服务管理体系认证证书得 2 分； 2、供应商具有有效的信息安全管理体系认证证书得 2 分； 3、供应商具有有效的质量管理体系认证证书得 2 分； 4、具有有效的厂商项目授权和服务承诺函（原件）得 2 分。 以上需提供复印件加盖公章，未提供不得分。
		近三年业绩	8	近三年（2020 年 12 月 1 日至今）承担的类似项目业绩，每提供一项业绩得 2 分，本项最高得 8 分。 注：以上业绩需提供合同复印件，合同复印件需至少包括合同的甲乙双方、主要内容、双方签章及生效时间。未按上述要求提供不得分。
2	技术部分（54 分）	对技术规范的响应程度	14	综合依据响应文件对项目需求书的理解和阐述，在满足比选文件要求且结合项目实际情况的前提下，综合判定供应商产品选型配置方案的科学性、合理性和可操作性。 1、方案的科学性、合理性和可操作性强得 14 分； 2、方案的科学性、合理性和可操作性一般得 10 分； 3、方案的科学性、合理性和可操作性欠佳得 7 分； 4、方案的科学性、合理性和可操作性差得 3 分； 5、无方案得 0 分。
		技术方案合理性	10	1、整体方案先进、能提供风险计算方法，方案合理可行，得 10 分；

				2、整体方案描述较完善，方案较合理较可行，得 8 分； 3、整体方案描述基本完善，方案基本合理基本可行，得 5 分； 4、整体方案描述不够完善，方案不够合理不够可行，得 3 分； 5、整体方案描述不完善，方案不合理不可行，得 1 分； 本项未提供，得 0 分。
		项目组人员配备	10	综合考虑响应文件中人员配备情况： 拟投入本项目的团队成员组织机构配置合理、清晰，人员具有丰富的同类项目方面的实施经验：10 分； 拟投入本项目团队成员组织机构配置较合理、较清晰，人员具有较丰富的同类项目方面的实施经验：8 分； 拟投入本项目团队成员组织机构配置有欠缺，同类项目方面的实施经验一般，但不影响本项目实施：5 分； 拟投入本项目团队成员组织机构配置不够合理、较混乱，人员欠缺同类项目方面的实施经验：2 分； 拟投入本项目团队成员组织机构配置不合理、混乱，人员无同类项目方面的实施经验：1 分； 未提供该方案：0 分。
		实施计划安排方案	10	综合考虑响应终端安全软件产品的安装、调试、系统数据迁移实施方案的细致程度等。 方案的科学性、合理性和可操作性强得 10 分； 方案的科学性、合理性和可操作性一般得 8 分； 方案的科学性、合理性和可操作性欠佳得 5 分； 方案的科学性、合理性和可操作性差得 2 分； 无方案得 0 分。

		培训方案	5 分	综合考虑培训计划安排、开展技术培训的相关承诺等能否满足或优于比选文件要求。 方案的科学性、合理性和可操作性强得 5 分； 方案的科学性、合理性和可操作性一般得 3 分； 方案的科学性、合理性和可操作性欠佳得 2 分； 方案的科学性、合理性和可操作性差得 1 分； 无方案得 0 分。
		售后服务方案及承诺	5	综合考虑售后服务内容、质保期、售后服务响应时间、反应迅速等。 方案的科学性、合理性和可操作性强得 5 分； 方案的科学性、合理性和可操作性一般得 3 分； 方案的科学性、合理性和可操作性欠佳得 2 分； 方案的科学性、合理性和可操作性差得 1 分； 无方案得 0 分。
3	价格部分（30 分）	投标报价	30	（1）评标基准价：满足招标文件要求且投标价格最低的有效投标报价为评标基准价。 （2）投标报价得分=（评标基准价/投标报价）×100×30%。