数据库审计系统招标公告

安信农业保险股份有限公司（以下简称“征集人”）现邀请合格的供应商（以下简称“应征人”）就征集人所需项目进行项目征集，征集人偿付能力符合监管规定,具体可上征集人官网查询[www.aaic.com.cn](http://www.aaic.com.cn)，征集人将择优选定中选人，欢迎符合条件的应征人前来参与方案比选，现将有关事项公告如下。

1. 征集项目内容
2. 设备数量

数据库审计系统1套

1. 设备要求

设备及设备附属配件均为原厂提供。

1. 应征人必须具备的条件：
2. 应征人须为原厂商或授权代理商，所投产品品牌为国内外知名品牌，所投服务器产品性能可靠，不少于三年市场应用案例。
3. 应征人必须具有独立法人资格，具有独立承担民事责任的能力，具备相应的经营范围且其注册资金或净资产（所有者权益）必须不小于 1000（含）万元人民币（或等值外币）。须提供有效《企业法人营业执照》副本复印件。
4. 应征人必须具有专业团队，具有较强的售前、售中和售后服务支持能力，提供7\*24报修服务电话及固定的客户服务经理，省会城市、一类城市、直辖市均需要有办事处及备件库。提供全国性服务网点的证明材料。提供人员素质和技术能力资质证明。
5. 投标人未被“信用中国”网站（www.creditchina.gov.cn）、“中国政府采购网”（www.ccgp.gov.cn）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;并提供截图证明；
6. 财务状况：投标人应具备良好的财务状况，具有足够的流动资金来承担招标范围各事项,提供近两年的财务状况报告复印件（至少包括资产负债表和利润表）。
7. 近六个月中任一月份的依法缴纳税收和社会保障资金的相关材料。
8. 法定代表人为同一个人的两个及两个以上法人，母公司与全资子公司/由其控股的子公司，不得同时参加本项目。
9. 法律、行政法规规定的其他条件。
10. 应证人需提供厂商对本项目的授权书。
11. 应征人所需提交材料
12. 有效《企业法人营业执照》副本复印件
13. 全国性服务网点的证明材料
14. 人员素质和技术能力资质证明
15. 企业征信证明
16. 近两年的财务状况报告复印件（至少包括资产负债表和利润表）
17. 近六个月中任一月份的依法缴纳税收和社会保障资金的相关材料
18. 以上所有资质证明都需加盖应征人公司公章
19. 售后服务要求
20. 应证人应为征集人提供及时周到的系统技术支持。
21. 应证人应确保为甲方提供7\*24小时技术支持服务，响应时间不应该超过1小时，现场响应支持不应超过4小时。
22. 应证人所提供设备保质期(维保)均为三年，集成商所提供的设备在保质期内因硬件、软件本身质量问题所造成的损坏或无法正常运行，由此产生的维修、更换硬件和软件故障排除等所需一切费用（包括工程师差旅费用等支出）由集成商负责。
23. 应证人应提供相应的备件支持，以便及时更换损坏硬件。
24. 应证人应在质保期后设备生命周期内有义务继续对系统设备提供维保服务，甲方将支付相应费用。
25. 针对以上要求，应证人可提供具体可行的有吸引力的合作方案。
26. 验收
27. 所有设备均需提供安装服务，所采购设备（包括软件）安装都必须由生产厂商授权集成商执行。
28. 安装前由征集人信息技术部协同征集人行政办公室对货物的品牌、数量、包装等方面进行实物验收。征集人提供的所有包装的货物均应完好无损。如遇交付前已拆封的货物，征集人有权拒绝或要求更换。应证人交货时，必需提供所有产品原厂或总代理出具的供货相关证明。
29. 应证人根据征集人技术要求在征集人信息技术部指导下进行设备安装、调试，并由征集人信息技术部进行使用性能方面的验收。
30. 报名方式

有意者请于2019年9月23日之前将标书及相关材料送至以下地址：上海市静安区共和新路3651号 顾晓磊收

商务联系人：顾晓磊

联系方式：021-66988356 [guxl@aaic.com.cn](mailto:guxl@aaic.com.cn)

技术联系人：卫金凯

联系方式：021-66988391 [weijk@aaic.com.cn](mailto:weijk@aaic.com.cn)

1. 投诉邮箱：kehufuwu@aaic.com.cn
2. 设备技术指标

**硬件及性能部分**

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 硬件指标 | 1、系统：产品采用专用工控机硬件架构，非普通PC服务器， MTBF(平均故障间隔时间)≥65000小时；  ★2、系统启动采用CF卡加硬盘方式，保证稳定可靠不可篡改。（提供产品图片并盖原厂公章）；  3、处理器：采用当前Intel E3 或 E3以上CPU，至少4核4线程，主频至少3.1G；  4、内存：≥8GB DDR3 1600Mhz；  5、电源模块：具备冗余热插拔双电源；  6、硬盘可用容量：≥1TB，1T\*2，支持RAID1，最大支持扩展到4T\*2硬盘。  ★7、网络端口**：**支持监听接口扩展；配备至少2个千兆电口管理口  支持千兆网络环境下的监听能力，标配至少2个千兆电口和2个千兆光口  支持最大扩展至4电4光或8电或8光共8个千兆以太网口。 |
| 处理能力 | 1、审计性能：能够稳定、流畅地同时支持8数据库数审计能力，不会产生漏审；  ★2、峰值处理能力：≥20000条/秒；提供国家权威检测机构（公安部三所或国家保密科技测评中心）检测报告  3、审计日志检索能力：≥1500万条/秒； |

**功能及资质部分**

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 部署方式 | 为适应各种复杂的部署环境，产品部署模式上应满足以下的要求：  1、旁路部署模式下无须在被审计数据库系统上安装任何代理即可实现审计；  ★2、支持在目标数据库安装agent解决云环境、虚拟化环境内部流量无法镜像场景下数据库的审计；提供国家权威检测机构（公安部三所或国家保密科技测评中心）检测报告  3、支持分布式部署，管理中心可实现统一配置、统一报表生成、统一查询；  4、管理中心和探测器都可存储审计数据，实现大数据环境下磁盘空间的有效利用和扩展；  5、管理中心和探测器直接的数据传输速率、时间、端口都可自定义；(提供功能截图证明)  ★6、支持大数据平台部署，具有成熟的大数据hadoop平台处理，支持后期无缝扩展大数据版本，支持审计数据外送至大数据平台，检索性能高达100亿数据仅需6-8秒，存储数据量高达3000亿以上；（需提供大数据合同关键页面复印件） |
| 协议支持 | 为审计和防护不同类型、不同版本的数据库，产品在协议支持应具备以下的要求：  1、支持Oracle、SQL-Server、DB2、Informix、Sybase、MySQL六种主流数据库审计；  2、支持PostgreSQL、HANA、Teradata、Cache、人大金仓、达梦、南大通用数据库审计；(提供功能截图)；  ★3、支持MongoDB、Hbase非关系型数据库审计；  4、支持主流业务协议 HTTP、Telnet、FTP、SMTP、POP3、DCOM；  ★5、支持对SQL server（2005及以上版本）数据库采用加密协议通讯，可以通过导入证书的方式实现审计和防护；（需提供功能截图，并提供国家权威检测机构（公安部三所或国家保密科技测评中心）检测报告）  6、支持对各种协议自动识别编码及在web界面手工配置特定编码 |
| 审计功能 | 为满足对数据库操作行为审计，满足业务、安全等方面的需求，产品需要满足以下的要求：  1、支持数据库操作类、表、视图、索引、存储过程等[各种对象的所有SQL操作审计](#_支持各种对象的SQL审计_1)  ★2、支持数据库请求和返回的双向审计，特别是返回字段和结果集、执行状态、返回行数、执行时长等内容，支持通过返回行数和内容大小控制返回结果集大小； (提供功能截图，并提供国家权威检测机构（公安部三所或国家保密科技测评中心）检测报告)  3、支持跨语句、跨多包的绑定变量名及绑定变量值的审计[（提供功能截图并盖原厂公章）](#_绑定变量)  ★4、支持与堡垒主机自动关联审计通过ssh、rdp等加密协议操作数据库行为（需提供功能截图，并提供国家权威检测机构（公安部三所或国家保密科技测评中心）检测报告）； |
| 智能发现 | 为更加便捷使用数据库审计，数据库审计需具备以下功能：  1、自动识别流量中存在的数据库  ★2、支持定期[自动扫描数据库漏洞](#_支持定期扫描数据库漏洞)和不安全配置，提供漏洞扫描报告；(需提供功能截图并提供国家权威检测机构（公安部三所或国家保密科技测评中心）检测报告) |
| 应用关联 | 为了更好的完成追踪溯源，数据库审计产品需要具体三层关联功能，要求如下：  ★1、支持B/S业务系统三层关联审计； （需提供功能截图，并提供国家权威检测机构（公安部三所或国家保密科技测评中心）检测报告）  2、支持通过[部署agent](#_Agent三层关联)实现java web环境100%准确关联（提供功能截图）  3、支持[旁路自动学习三层审计](#_旁路自学习三层关联)关联功能（提供功能截图） |
| 安全审计 | 为发现数据库中不安全访问行为及审计数据二次泄露等问题，数据库审计需满足以下功能：  1、支持审计记录中敏感数据的模糊化处理，内置常见敏感数据掩码规则，支持自定义（提供功能截图）  2、内置安全特征库不少于300条，如SQL注入、缓冲区溢出、弱口令等；  3、可自定义审计规则，审计规则至少支持18个条件；（提供功能截图）；  4、规则各条件之间支持[与或非逻辑](#_支持与或非逻辑关联)关系；（提供功能截图）；  5、告警数量需[支持最大告警数量限制](#_最大告警数限制)，超过告警阈值之后便不告警；（提供功能截图）；  6、告警查询应支持根据登陆用户、客户端工具名、客户端IP、规则进行归并分析，能详细展示每类告警占总告警数量百分比，便于告警分析处理（提供截图证明）； |
| 审计查询 | 为满足审计追踪溯源、分析安全问题等需求，数据库审计应满足以下的查询需求：  1、具有高效的查询性能，后台采用[SPHINX](#_SPHINX全文索引)全文检索引擎检索（提供产品功能截图）；  2、查询条件易于使用，[审计查询条件](#_查询条件)均为非正则表达式形式进行  3、支持采用部分[匹配模糊](#_支持模糊查询)查询方式检索审计日志  4、支持基于数据库[访问日期、时间、源/目的IP、来源](#_多维度查询)、数据库名、数据库表名、字段值、数据库登陆账号、SQL关键词、数据库返回码、SQL响应时间、数据库操作类型、影响行数等条件的审计查询； |
| 统计报表 | 为满足事后分析需求，数据库审计应满足以下的需求：  ★1、系统提供内置[多种报表模板库](#_内置多种报表模板)，内置的报表不少于35种；（提供功能截图）  2、报表支持严格按照[塞班斯（SOX）法案、等级保护标准](#_SOX、等级保护合规多维度)要求生成多维度综合报告；  3、支持按照数据库[访问行为](#_按行为分析)生成报表，智能识别帐号的增删、权限变更、密码修改、特权操作等行为；  4、支持按照[时间曲线统计流量](#_时间曲线等报表)、在线用户数、并发会话、DDL操作数、DML操作数、执行量最多的SQL语句等报表；（提供功能截图）  5、支持[性能分析](#_按性能分析)，准确提炼出SQL语句执行频率和执行时间异常的报表；  6、支持[Word、PDF、ppt](#_导出格式)等格式的报表导出；  7、支持[报表自定义](#_报表自定义)，自定义的条件不少于20个；（提供功能截图） |
| 模型分析 | 为了更加智能发现数据库安全问题，产品需要具备以下功能：  ★1、支持对数据库[自动建模及智能对异常行为告警功能](#_自动建模告警)；（提供产品功能截图，并提供国家权威检测机构（公安部三所或国家保密科技测评中心）检测报告证明）；  2、可通过行为[轨迹图方式](#_轨迹图方式展示)展示数据库访问行为；（提供产品功能截图）；  ★3、可基于账号、IP地址、访问权限、客户端工具等维度对行为模型做钻取分析、变更分析，对学习的安全基线以外的行为自动智能的进行告警；（提供产品功能截图）；  4、可以自动[对比不同时期的行为模型](#_不同时期对比)，以区分其审计日志数趋势、用户、IP地址、工具、访问权限的差异情况； |
| 数据管理 | 为满足数据备份保留的需求，产品需要具备以下功能：  1、支持根据保留天数和占用百分比[自动清理](#_自动清理)最早的数据；  2、提供审计策略和[系统配置信息的单独导入、导出](#_系统配置单独导入导出)功能； |
| 系统管理 | 为增加系统管理的安全性、适应性、可维护性，产品需要具备以下的功能：  1、支持用户界面告警、Syslog、SNMP、邮件、短信、ftp六种方式告警；  2、采用B/S架构管理，[支持中英文两种管理界面](#_中英文切换)  3、支持[系统安全配置](#_系统安全配置)（会话锁定、超时退出、IP地址访问控制、密码复杂性管理、验证码登陆等措施）  4、支持[NTP时间同步、SNMP](#_NTP、SNMP)(v1、V2、V3)网络管理协议 |
| 故障排错 | ★系统内置独立的故障排错系统，支持一键导出系统调试日志，一键检测服务、许可证、流量等常见故障；支持流量分析功能，包括抓包、包内容查看、[自动探测sql语句](#_流量分析)等； |
| 产品资质 | ★所有资质必须为数据库审计产品专有的资质，不能是网络审计产品或者综合审计的产品资质。 |
| ★具备公安部颁发的《[计算机信息系统安全专用产品销售许可证](#_销售许可)》，数据库安全审计国标-增强级 |
| ★具备国家信息安全测评中心颁发的《[信息技术产品安全测评证书](#_国家信息安全测评EAL3+)》，级别EAL3+，提供证书复印件； |
| ★产品通过国家信息安全认证中心[3C](#_3C_认证)认证检测，级别增强级以上，提供证书复印件； |
| ★具备国家保密局涉密信息系统安全保密测评中心颁发的《[涉密信息系统产品检测证书](#_涉密信息系统产品检测证书)》 |
| ★具有军用信息安全产品认证证书，[军B+](#_军工认证_B+)级 |
| 具有[自主知识产权和著作权](#_自主知识产权和著作权)，需提供相应证明文件 |
| ★要求内置的数据库扫描系统也通过国家相关部门的认证和检测，并获得独立的销售许可、涉密资质 |

**其他**

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 公司资质 | ★原厂商具有国家安全应急服务支撑单位证书（国家级）  ★原厂商具有信息安全等级保护安全建设服务机构能力评估合格证书  ★原厂商应具备ISCCC信息安全服务风险评估资质一级  ★原厂商应具备国家信息安全测评信息安全服务资质证书（安全工程类二级）  ★原厂商注册资金不少于3000万，需提供经年检合格的营业执照副本 |
| 售后支持 | ★提供不少于三年产品原厂商质保服务，提供原厂质保函；  ★提供不少于三年的原厂商7\*24小时上门现场服务支持；  ★原厂商工程师实施及提供设备相关的培训，提供原厂产品培训1天。 |