采 购 文 件

第

二

分

册

采购方式：公 开 招 标

采购编号：SJC2014120371

项目名称 :江苏省公安交管数据库安全审计监管平台

江苏省省级行政机关政府采购中心

二〇一五年五月

目 录

（第二分册）

第三章 招标书

我中心受江苏省公安厅的委托，拟对该单位委托的江苏省公安交管数据库安全审计监管平台项目进行政府采购，欢迎你单位参加，并提请注意以下事项：

一、招标主要内容

序号	项目	具 体 内 容
1	项目名称	江苏省公安交管数据库安全审计监管平台
2	采购方式	公开招标
3	采购编号	SJC2014120371
4	分包	无
5	集中采购机构	江苏省省级行政机关政府采购中心 项目负责人：王建浩 电话：025-83286909
6	采购人	江苏省公安厅 联系人：康蓬海 电话：025-83527089
7	采购预算	人民币贰佰捌拾陆万圆整
8	投标保证金	本项目免收投标保证金。本采购文件中，涉及保证金的条款均按免收保证金的情况执行。
9	采购文件获取	采购文件在"江苏政府采购网www.ccgp-jiangsu.gov.cn"及"江苏省省级行政机关政府采购中心网站www.jszfcg.gov.cn"发布，供应商如确定参加投标，可自行下载招标文件。须在投标截止时间前通过我中心“供应商信息服务平台”系统中的[投标未确认项目]页面完成投标确认。
10	答疑	时间：2015年5月19日 10:00 地点：江苏省南京市中央路42号江苏省省级行政机关政府采购中心四楼408开标大厅
11	勘察现场	本项目不安排现场勘察

12	投标	截止时间：2015 年 6 月 3 日 9:30 地点：江苏省南京市中央路 42 号江苏省省级行政机关政府采购中心四楼 408 开标大厅
13	投标文件数量	正本份数：1 份 副本份数：4 份
14	开标	时间：2015 年 6 月 3 日 9:30 后 地点：江苏省南京市中央路 42 号江苏省省级行政机关政府采购中心四楼 408 开标大厅
15	投标文件有效期	投标截止时间后九十天
16	政策功能	本项目面向各种规模企业采购
17	关于联合体投标	本项目不接受联合体投标

二、投标供应商资质要求

参加政府采购活动的供应商应当具备政府采购法第二十二条第一款规定的条件，提供下列材料：

（一）法人或者其他组织的营业执照等证明文件，自然人的身份证明；

（二）开标前六个月内（2014 年 11 月至今）中任一月份的财务状况报告复印件（至少包括资产负债表和利润表）（自然人可以不提供，法人或者其他组织成立未满三个月的可以不提供）；近六个月（2014 年 11 月至今）中任一月份的依法缴纳税收和社会保障资金的相关材料（提供相关主管部门证明或银行代扣证明的复印件，根据国家相关政策免缴或迟缴的需提供相关证明材料）；

（三）具备履行合同所必需的设备和专业技术能力的证明材料，须包含：

1、投标人具备涉及国家秘密的计算机信息系统集成乙级（适用地域为江苏省）及以上资质；

2、投标人具备不少于 6 名 CISP 认证的服务人员，（提供证书复印件及上述人员近三个月内的缴纳社保证明材料）。本项目开发管理团队中，必须有服务人员具有 CISE、CISO、CISA 证书。（提供证书复印件及上述人员近三个月内的缴纳社保证明材料）

3、投标人须提供针对本建设项目单独核算管理和接受建设单位延伸审计的承诺书原件（格式见附表 2）。

（四）参加政府采购活动前 3 年内在经营活动中没有重大违法记录的书面声明（格式见附表 3）。

三、评标办法和定标原则

本项目采用综合评分法，总分为 100 分，按评审后得分由高到低顺序排列，得分相同的，按投标报价由低到高顺序排列，得分且投标报价相同的，按技术指标优劣顺序排列，由评标委员会推荐 1 个中标候选人。具体打分办法如下：

3.1 价格分（40 分）。价格分采用低价优先法计算，即满足招标文件要求且报价最低的供应商报价为评标基准价，其价格分为满分 40 分，其它投标人的价格分统一按照以下公式计算：投标报价得分=(最低报价/该投标人的投标报价)×40 分。

注：本项目非专门面向中小企业采购，根据财政部发布的《政府采购促进中小企业发展暂行办法》规定，对小型和微型企业产品的价格

给予 6%的扣除，用扣除后的价格参与评审。以上所述投标报价，均为对小、微企业产品进行价格扣除后的报价。(提供中小企业声明函，格式附后）

3.2 技术方案（38 分)。

3.2.1 投标产品技术性能响应情况（25 分)。投标产品技术性能响应情况 （ 25 分)。具体由评委根据投标文件中设备参数响应程度打分。所投产品技术指标全部响应招标文件要求的得满分 25 分;打“★”指标为必须满足项，如有负偏离，则作为无效投标；非打“★”指标每有一项负偏离，评委根据其重要程度酌情扣减 1 分，该项减分最多不超过 5 分，否则按无效投标。

3.2.2 项目开发及实施方案可行性（8 分)。投标人需对用户环境和当前系统架构熟悉，对用户需求及发函要求清晰明确,投标人所提方案，必须承诺予以实施，且实施过程所涉费用全部由投标人承担。 对用户环境和当前系统架构描述，得 4 分。 设计思路清晰，实现简单，功能有效，得 4 分

3.2.3 项目开发及实施方案匹配性（5 分)。具体由评委根据投标人的对所投产品的实施方案打分。优得 5 分；良得 3-4 分；一般得 1-2 分，差不得分。

3.3 服务方案 （8 分)。

3.3.1 售后服务方案（4 分)。投标人提供详细的售后服务方案（如服务体系、服务内容、响应次数、响应时间），由评委根据投标人提供方案的合理程度酌情打分。

3.3.2 培训方案（2 分)。由评委根据投标人提供培训方案的合理程度酌情打分。

3.3.3 项目实施方案（2 分)。

3.4 经营业绩（2 分)。 投标人提供自 2011 年（含）以来的类似安全管理平台系统建设案例证明，每个 100 万及其以上金额的项目得 1 分，满分为 2 分；（提供合同复印件）

3.5 企业实力（8 分)。1、投标人提供信用评级机构出具的信用评级报告为 AAA 级以上的得 1 分，其他不得分。 2、投标人提供信息技术产品安全测评证书 EAL3 级（中国信息安全测评中心）得 1 分，没有不得分。 3、投标人提供 IT 产品信息安全认证证书（中国信息安全认证中心）得 2 分，没有不得分。 4、投标人为国家级网络安全应急服务支撑单位（国家计算机网络应急技术处理协调中心）得 2 分，没有不得分。5、投标人提供国家信息安全测评信息安全服务资质证书（中国信息安全测评中心）得 2 分，没有不得分。 以上材料请提供资质证书复印件或相关证明材料，没有不得分。

3.6 现场演示（4 分)。 介绍现有产品已实现功能、针对本项目所要求的安全管理平台的开发思路、技术路线和实施计划，评委根据演示情况酌情给分。

四、关于现场陈述

各投标单位按照签到顺序进行现场讲解及演示，演示需按照招标文件和评委要求，时间不超过 5 分钟。招标方提供投影机及幕布，其他所需设备投标人自备。

评委根据讲解演示情况进行评审，若评委一致认为某投标单位的现场讲解演示的内容与标书要求差距较大，不符合建设要求，可以按照重大负偏离处理。

演示内容：

投标人可以在评标现场进行 5 分钟的 PPT 讲解或现场功能演示，介绍现有产品已实现功能、针对本项目所要求的安全管理平台的开发思路、技术路线和实施计划。

五、关于样品

无

六、有关开标当日流程

6.1 投标供应商授权代表在投标截止时间前到达开标地点。

6.2 投标供应商授权代表持《法人授权委托书》原件和身份证原件到公证员处验证合格后办理签到手续，并递交投标文件。

6.3 采购中心开标、唱标。

6.4 评审委员会对各投标供应商的投标文件进行现场评审，如有需要，评审委员会将请供应商授权代表进行现场澄清或解释说明，必要时应以书面说明情况，授权代表不要远离开标会场，并保持通讯工具畅通。

6.5 评审委员会主任宣布评标结果，未中标供应商退回投标保证金及样品（如有），所有投标文件（含电子投标文件）不予退还。

七、其他相关说明

7.1 本项目仅采购非进口产品（注：本文件所称进口产品是指通过中国海关报关验放进入中国境内且产自关境外的产品）。

7.2 有关本项目的更正公告敬请关注本中心网站发布的信息(网址：www.jszfcg.gov.cn)，也可以与我中心综合科联系，联系电话：025-83286900，传真：025-83286920。

7.3 采购中心开户行信息

单位名称：江苏省省级行政机关政府采购中心

开 户 行：建行江苏省分行湖北路支行

账　　号：

八、政府采购中标（成交）项目融资工作相关信息

为落实政府采购的政策功能，加大对中小型企业的扶持力度，进一步促进中小企业可持续发展，根据有关政策，在我中心中标（成交）的供应商，在合同履约过程中如遇到资金困难，凭中标（成交） 通知书可在相关银行办理授信申请。江苏省省级行政机关政府采购中心联系人：李亭，联系电话：025-83286912。

第四章 政府采购合同专用条款部分（货物）

甲方： 江苏省公安厅

乙方:

甲乙双方根据2015年6月3日政府采购编号SJC2014120371的江苏省公安交管数据库安全审计监管平台项目公开招标采购结果及采购文件的要求,经协商一致,达成如下货物购销合同:

一、货物及其数量、金额等

序号	采购货物名称	规格型号	数量	单价	总价	免费质保期	交货时间
合同总金额：人民币（大写） ￥：					元整。 元整		
甲方	联系人： 固定电话： 移动电话：						
乙方	联系人： 固定电话： 移动电话：						

二、交货地点：

三、交货方式：招标文件有要求的按相关要求执行。招标文件无具体要求的，采取的_____方式交货。

四、验收：甲方按采购文件相关要求及乙方响应文件的承诺进行。如需委托第三方验收，第三方是指：_____，验收费用由甲方承担。因乙方交付的货物不符合标准导致甲方重复支出的验收费用，由乙方承担。

五、履约保证金：本次采购项目未收取投标保证金，采购人如需收取履约保证金，双方在签订合同时由采购人按不超过采购预算金额（如有分包的，按分包预算金额）的1%向供应商收取。

六、付款：由甲方按下列程序付款。每次付款在___个工作日内完成。

1、预付款：签订合同后，支付合同总价的 40%。

2、设备安装调试结束，试运行 6 个月正常，提交全部报告材料，并通过正式验收、审计决算后，支付至决算金额的 90%，同时无息退还乙方的合同履约保证金。

3、尾款：免费质保期结束，经甲方确认在此期间使用正常;工作成果交付甲方并经甲方验收合格或经甲方确认乙方已在合同期间全面履行约定义务，并且乙方已全面履行后合同义务，完成与甲方或甲方指定第三方的交接后，付清余款。

七、保密条款：乙方不得将在履行本合同中知悉的甲方任何信息随意泄露、擅自使用。

如违反本条款规定，乙方应当承担如下责任：_____

八、合同纠纷处理：本合同执行过程中发生纠纷，由甲乙双方协商处理，若协商不成，双方一致同意作如下___处理：

1. 申请仲裁。选定仲裁机构为南京仲裁委员会。

2. 提起诉讼。约定由采购人所在地法院管辖。

九、合同生效：本合同由甲乙双方签字盖章后生效。

十、合同鉴证：集中采购机构应当在本合同上（签字或盖章），以证明本合同条款与采购文件、投标文件的相关要求相符并且未对采购服务和技术参数进行实质性修改。

十一、组成本合同的文件包括：

1. 合同通用条款和专用条款；

2. 中标通知书；

3. 采购文件和乙方的投标文件；

4. 甲乙双方商定的其他必要文件。

上述合同文件内容互为补充，如有不明确，由甲方负责解释。

十二、合同备案

本合同一式四份，中文书写。甲乙双方、集中采购机构各执一份，另外一份由甲方报省财政厅政府采购管理处备案。

甲方：江苏省公安厅 （盖章）

地址：

法定（授权）代表人：

二〇一__年__月__日

乙方： （盖章）

地址：

法定（授权）代表人：

二〇一__年__月__日

户名：

开户银行：

账号：

政府集中采购机构声明：本合同标的经政府集中采购机构依法定程序采购，合同主要条款内容与招投标文件的内容一致。

政府集中采购机构：江苏省省级行政机关政府采购中心（盖章）

地 址：南京中央路 42 号

经办人：王建浩

二〇一___年___月___日

第五章 项目采购需求

招标技术规格及要求

（一） 建设背景

伴随着信息系统的快速发展，信息系统所面临的安全威胁日益复杂，用户对信息安全系统的需求与日俱增。特别对于全省的交通管理信息系统，涵括机动车、驾驶人及交通违法等各项核心业务系统，涉及包括个人隐私、经济利益等关系，该类核心业务数据更受到社会各种人员的关注，也在全国不少地市出现了安全事故，甚至是经济违法犯罪。

从各级领导对交通管理信息系统数据的安全工作非常重视，从建设初始逐年加大在安全建设方面的投资，进行了一系列的组织、制度、管理和技术方面的安全建设工作，提高交通管理数据的安全。

众所周知，绝大部分应用系统都是基于浏览器、Web 服务器、数据库典型的三层部署架构。其中，数据库中存储着大量的核心业务信息。然而数据库在使用过程中缺乏必要技术防护手段，使得存储在数据库里的大量敏感信息的安全性无法得到有效的保障，主要体现在以下几方面：

- 内部用户可以很方便的利用内部网络通过各种通讯协议进行刺探，获取、删除或者篡改重要的数据和信息。
- 内部授权用户对于系统不熟悉而导致误操作也时常给业务系统造成难以恢复的损失。
- 外部非授权人员对数据库进行恶意入侵，获取或者删除数据库里的数据。
- 所有针对数据库的安全事件发生后，无法进行有效的追溯和审计。

（二） 建设目标

以风险管控为主线、以安全效益为导向、以风险相关法律、法规和理论方法为依据、以网络安全风险体系和风险管理体系建立为前提，以网络安全规范建立

为基础、以安全信息化、自动化技术为手段，通过建立安全防御、管理一体化的安全管理平台来满足安全日常工作有序、有效的开展，努力实现管理的自动化，构建江苏省交警信息系统的安全管理体系。

本期建设主要是通过全方位、多途径采集针对数据库的操作行为数据，进行格式化、过滤、归并后，汇总至安全管理平台进行统一分析、处理和展示，从而发现潜在风险和事实风险；同时，预留针对网络、主机、应用等其他管理对象的采集和分析接口，以便后期可以方便的扩展功能。

（三） 建设范围

1、建设范围

本项目覆盖省总队和 13 个地市交警支队。

序号	单位	数据审计监管分析平台（套）	数据采集平台（套）	网络探针（台）	堡垒探针（台）	主机探针（套）
1	省总队	1	1	1	1	1
2	南京	0	1	1	1	1
3	无锡	0	1	1	1	1
4	徐州	0	1	1	1	1
5	常州	0	1	1	1	1
6	苏州	0	1	1	1	1
7	南通	0	1	1	1	1
8	连云港	0	1	1	1	1
9	淮安	0	1	1	1	1
10	盐城	0	1	1	1	1
11	扬州	0	1	1	1	1
12	镇江	0	1	1	1	1
13	泰州	0	1	1	1	1
14	宿迁	0	1	1	1	1
	总计	**1**	**14**	**14**	**14**	**14**

2、采购清单

公安交管数据库安全审计监管平台设备、软件清单

（一）硬件设备和安全平台软件

设备	详细配置	数量
安全平台软件	厂家订制硬件平台安全监测及分析软件，部署在省总队，提供统一的界面，可供统一查询	1
省厅审计设备	部署在省厅的安全审计设备，对省总队的数据库系统访问进行探测	1
省厅堡垒机	部署在省厅的堡垒机设备，对省总队的数据库的各类访问进行控制和记录，主要指非数据库类	1
地市审计设备	部署在地市支队的安全审计设备，对地市支队的数据库系统访问进行探测	13
地市堡垒机	部署在地市支队的堡垒机设备，对地市支队的数据库的各类访问进行控制和记录，主要指非数据库类	13

（二）数据库安全审计监管分析软件

审计监管分析系统	地市审计软件开发，实现审计记录集中上传。 地市数据库审计的状态跟踪。 实现审计数据对外统一服务，提供简洁实用的人机界面，提供审计记录的查询跟踪、提供可疑操作的监控及审计数据分析功能。 可整合安全审计设备的审计数据，提供统一访问界面。 三年维护期间补丁修改及其他小功能完善。	1
集成实施	全省 13 个地市及省厅审计软件开通，针对各地市系统环境不同进行不同的审计配置;，三年免费升级维护	

（三）软件运行的硬件平台

高性能服务器	利用现有刀片服务器，配置 8 核 CPU，64G 内存，2 块本地硬盘，千兆网卡，HBA 卡	0
刀片机箱	利用现有刀片机箱	0
磁盘阵列	利用现有的磁盘阵列	0
移动维护终端	安装数据库审计的客户端，对全省交管综合应用平台数据库的审计情况进行实时监控	2

（四） 平台技术需求

本项目为交钥匙工程，中标人总集成新购和现有设备，建设一套涵括全省交通管理信息系统的数据安全管理平台（包括省总队和 13 个地市），从而提高全省交通管理信息系统的安全度，确保核心业务数据的安全，预防不必要的安全事件，甚至是经济违法事件。

通过在省总队和 13 个地市交警支队部署一套数据安全管理平台，分别对省总队及 13 个地市支队的交通管理综合应用平台的数据库系统进行安全访问防护及数据库审计，并将地市的分析结果汇总到省总队，从而提供统一的数据安全管理平台，提供给省总队及各地市的领导、系统管理员来查看，及时发现并防止可能存在的数据安全隐患。并做到事后可查，从而起到警示和警告作用，提高交通综合管理业务系统的数据安全。

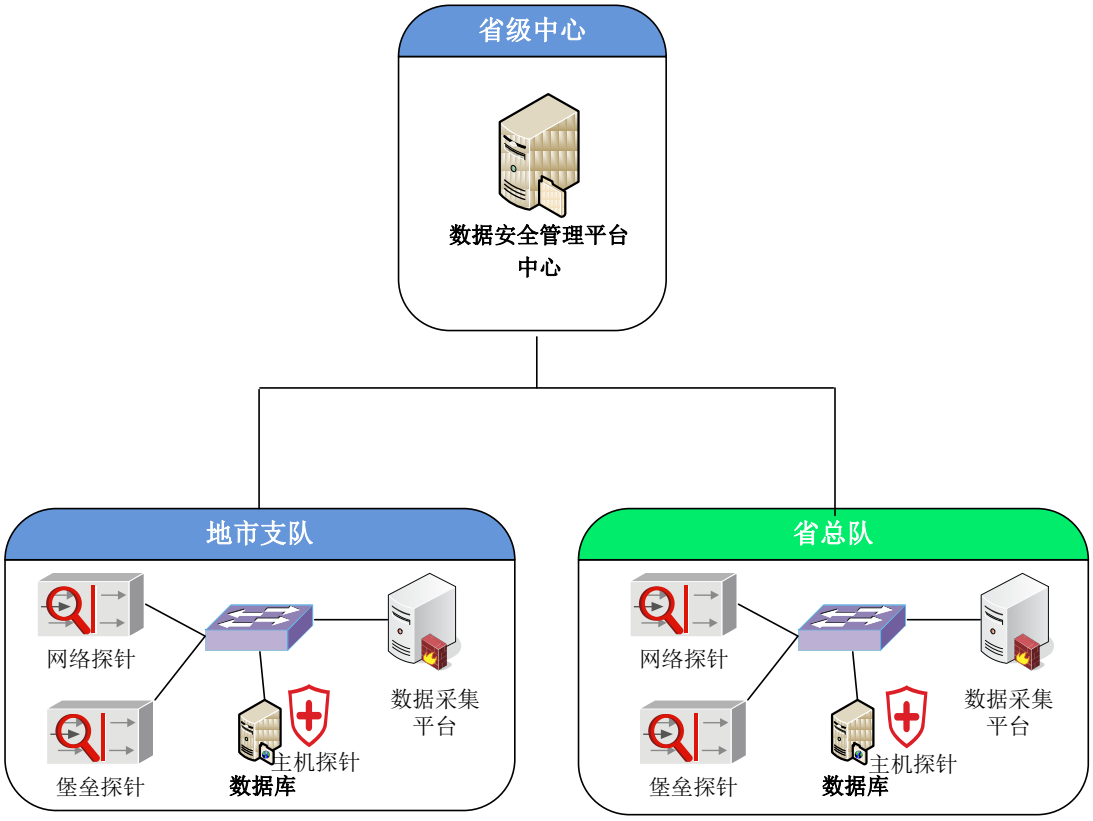
考虑交警业务系统的复杂性，因此采用硬件采集设备和开发基于数据库审计功能的采集软件相结合的方式来实现对全省交通管理业务系统全方位采集和分析。

1、单纯的硬件旁路采集设备不能完全记录所有的数据库操作事件，特别是登录到数据库服务器上后进行的数据库操作，无法完全记录。因此本次系统在使用数据库安全审计设备的同时，还利用数据库自身的审计功能开发一套数据库审计软件，做为硬件采集系统的有效补充，尽可能全的记录数据库操作事件，特别是 DML 和 DDL 事件。

2、单纯使用数据库本身的审计功能作为全省数据库安全审计手段的话，能够进行审计的内容将会很少，因为过多的审计内容将会严重降低交通综合管理数据库系统的性能，从而对业务系统照成一定影响。

（1） 平台系统架构

整个数据安全管理平台采用集中式部署模式，在省厅数据中心部署一套安全管理平台，全省汇集的数据都保存于省厅，部署架构如下：



在省总队数据中心部署 1 套数据安全管理平台软件系统，负责分析全省各地数据安全审计信息；在省总队和 13 个地市支队的数据库服务器前端分别部署 1 套数据采集系统，同时配合部署 1 台硬件网络探针、1 台硬件堡垒探针和 1 套主机探针软件，从网络访问数据库和登录服务器访问数据库等多方面进行安全审计；二级中心探针探测到的数据发给数据采集平台，数据采集平台实时将数据发至省总队一级安全分析平台进行统一分析和汇总。

1、在全省 13 个地市及省总队各部署 1 台网络探针，通过网络端口镜像的方式，对各地市的交管综合平台的业务生产数据库系统进行监控，对所有通过网络客户端方式访问数据库的访问进行追踪并审计，并将所有针对数据库的访问记录在安全设备本地硬盘。提供地市信息系统管理员通过 Web 界面统一查看及管理对数据库的非法访问。

2、在全省 13 个地市及省总队各部署 1 台堡垒探针，对所有通过网络访问数据库主机的会话进行记录和控制。方便地市信息系统管理员对数据库主机的远程访问进行控制并记录远程网络访问。

3、在全省 13 个地市及省总队数据库服务器上各部署 1 套主机探针，对数据库审计记录进行采集和报送。

4、在全省 13 个地市及省总队各部署 1 套采集代理平台，将本地的网络探针、堡垒探针和主机探针采集的数据汇集后，实时转发至省总队安全管理平台。

5、在省厅数据中心部署 1 套数据库安全监测及分析平台中心软件，将全省 13 个地市及省总队的所有数据库访问和操作行为记录进行统一集中到省总队，并对这些访问记录进行统计和分析。提供给省总队信息安全管理员及总队领导统一的报表及界面，方便省总队及时掌握各地市交管综合平台信息系统的安全情况，并对各地市信息系统安全提供指导意见和建议。

通过以上部署，针对省总队及 13 个地市支队的核心交警业务数据库服务器存在的诸多安全风险以及业务审计需求，数据安全管理平台能为用户数据库提供全方位、实时的、细粒度的安全防护与审计，对所有操作进行记录（包括 Select、Update、Insert、Delete）等。

（2） 平台功能要求

1）安全管理平台

(1)事件管理

安全事件管理是一种实时的、动态的管理模型，通过关联分析来自于不同地点、不同层次、不同类型的信息事件，帮助我们发现真正关注的安全风险，且提高安全报警的信噪比，从而可以准确的、实时的评估当前的安全态势和风险，并根据预先制定策略做出快速的响应，因此它是安全管理体系中人工智能的主要体现。

(2)关联分析

安全管理系统采用关联分析引擎来进行事件分析，该引擎实现对来自不同应用、设备、系统等产生的不同类型的事件的实时关联，在海量事件中准确定位安全问题。可以有效的发现在长时间内产生的少量事件的慢速攻击，根据实际业务系统以及流程制定的场景进行关联和分析。

(3)风险管理

风险管理模块基于资产管理、事件管理和评估管理模块中所提供的各项原始数据，分析风险的三要素（资产、威胁、弱点），从单个资产、业务系统、安全域、物理地域等多个维度获取信息系统的安全风险状况。

(4)脆弱性管理

各种重要信息资产存在的脆弱性是影响信息系统网络安全的重要潜在风险，为了了解其安全脆弱性状况，在安全管理平台中将建设脆弱性管理模块，实现对重要信息资产安全脆弱性的收集和管理。该模块收集和管理的脆弱性信息主要包括两类：通过远程安全扫描可以获得的安全脆弱性信息和通过人工评估的方式收集的脆弱性信息。在定期收集到这些脆弱性信息后可以利用脆弱性管理系统进行导入和处理，以利于安全管理员对脆弱性信息的查询、呈现并采取相应的措施进行处理。

(5)安全响应管理

安全管理平台的安全响应管理模块的主要功能是根据当前的网络安全状态，及时调动有关资源做出响应，降低风险对网络的负面影响。网络安全响应模块负责利用安全管理中心提供的采集和统计功能，科学合理的评价网络安全的状态指标，并根据安全的状态指标，结合安全风险控制的需要，及时通过工单系统发布工作指令，调动有关资源做出相应的响应，将剩余风险控制在可以接受的范围内。

(6)工单管理

安全管理平台提供了工单管理的功能。工单系统基于组织架构的安全事件处理流程创建，基于安全事件响应规则运作，实现了事件自动处理与人工参与的有机结合，贯彻于安全事件预警、响应、修补、防护的全过程。

(7)安全策略管理

安全管理平台所提供的安全策略管理模块可协助用户制定各种级别，针对不同对象（人员、设备、应用）的安全策略，实现企业安全策略的快速导入以及安全策略的集中分级管理。同时支持安全策略的不同格式的数据导出、安全策略的数据统计、安全策略的定时发布、安全策略评估等功能，实现企业内所有安全策略的全流程管理。

(8)知识管理

安全知识库实现安全信息的共享和利用，提供了一个集中存放、管理、查询安全知识的环境。其主要功能是将处理的安全事件方法和方案，标准漏洞信息和标准事件信息收集起来，形成安全共享知识库。

(9)辅助决策

对于大部分用户在处理威胁发生时，缺乏足够的知识积累，因此可能造成错误的安全响应。而辅助决策系统恰恰利用安全专家知识库为用户提供具体威胁的辅助决策建议和安全响应脚本来处理和响应事件。

(10)预警管理

预警管理模块管理并实时呈现风险评估中心所提供各类安全威胁、安全风险、安全态势、安全隐患等信息，该模块提供规则设定功能，以便准确定位用户所关心的安全问题，以便有针对性的进行响应处理。

(11)统计分析

对最新的动态安全数据进行深层次统计分析并生成易于理解、结果明确的图形报表，为相关人员提供及时准确的决策依据，通过更加灵活的、方便的、丰富的统计分析内容，使各级人员可以迅速方便的查到决策所需的信息。提供多种的报表内容和形式，为下一步的信息化安全建设规划和资金合理利用提供科学的依据。

(12)典型安全事件监控

安全管理平台通过实时采集各种设备（如防火墙、IDS、防病毒、防篡改设备、服务器、网络设备等）上的安全事件，而后进行关联分析（包括场景匹配和关联计数）来发现入侵攻击行为。监控内容包括：获取权限攻击事件类监控、信息收集攻击事件类监控、可疑网络活动事件类监控、拒绝服务攻击事件类监控、分布式拒绝服务攻击事件类监控、利用漏洞攻击事件类监控、密码猜测攻击事件类监控、病毒/蠕虫传播事件类监控、木马攻击事件类监控、非授权访问事件类监控、CGI 攻击事件类监控、缓冲区溢出事件类监控。

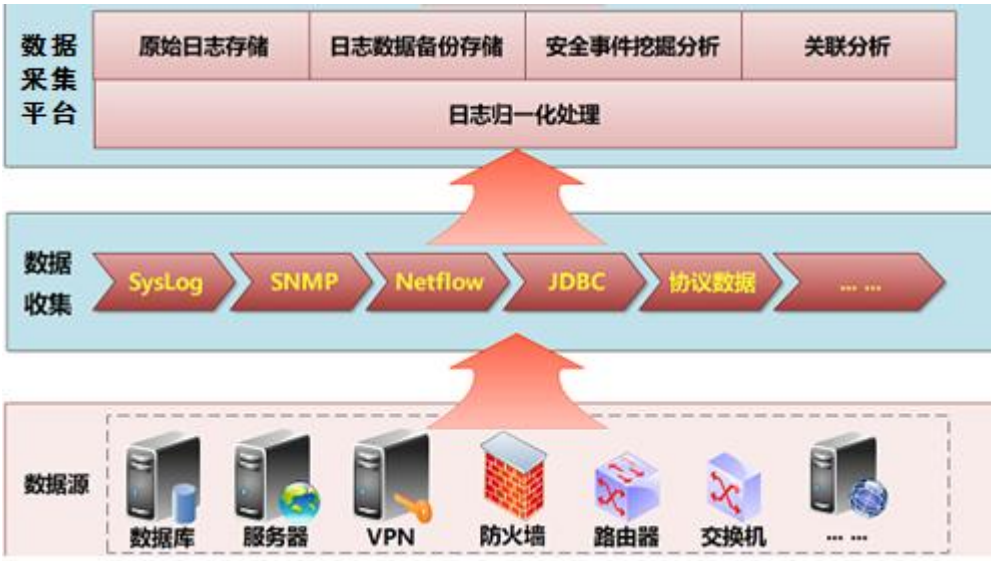
(13)数据库安全监控

全分析管理平台提供多维度的统计分析，系统内置的统计分析引擎能从多维度统计分析业务系统与数据库系统的压力。分析 SQL 语句以及网络带宽上的性能瓶颈，为保障系统持续稳定运行打下基础，为网络扩容提供依据。

2）数据采集平台

数据采集平台将分散的、格式不一的数据，进行统一“格式化“后集中存放，实时或定时传输到安全管理平台，为数据管理平台提供数据支撑。平台基于

SOA 架构设计，采用 B/S 管理模式。系统由日志采集、日志处理、日志管理、事件监测、日志存储等子系统构成。



3）网络探针

网络探针支持 SQL 操作响应时间的审计，支持 Update、Insert、Delete 操作返回行数的审计，支持数据库操作成功、失败的审计；支持数据库绑定变量审计，支持访问数据库的源主机名、源主机用户的审计；可审计 SQL 操作的客户端名称；可对 SQL 进行语法解析，分析 SQL 语句的操作类型，操作对象等信息。数据库审计系统内置有 SQL 语法解析器，能实现此功能；此外，用户还可以自定义 SQL 语法解析规则，分析用户特有 SQL 操作等；

网络探针可以通过对浏览器与 Web 服务器、Web 服务器与数据库服务器之间所产生的 HTTP 事件、SQL 事件进行业务关联分析，管理者可以快速、方便的查询到某个数据库访问是由哪个 HTTP 访问触发，定位追查到真正的访问者，从而将访问 Web 的资源账号和相关的数据库操作关联起来。包括访问者用户名、源 IP 地址、SQL 语句、业务用户 IP、业务用户主机等信息。

网络探针可根据解析的 SQL，对用户数据库服务器进行安全判断、攻击检测。数据库审计系统内置了多种攻击检测场景，能有效地对攻击行为作出告警等处理。并且能够通过审计记录发现生产数据库一些潜在的安全威胁，比如 SQL 注入，密码猜解，执行操作系统级的命令等，同时内置了丰富的数据库入侵检测规则库，及时发现并阻止生产数据库安全威胁，保证交警数据库更加安全运行。

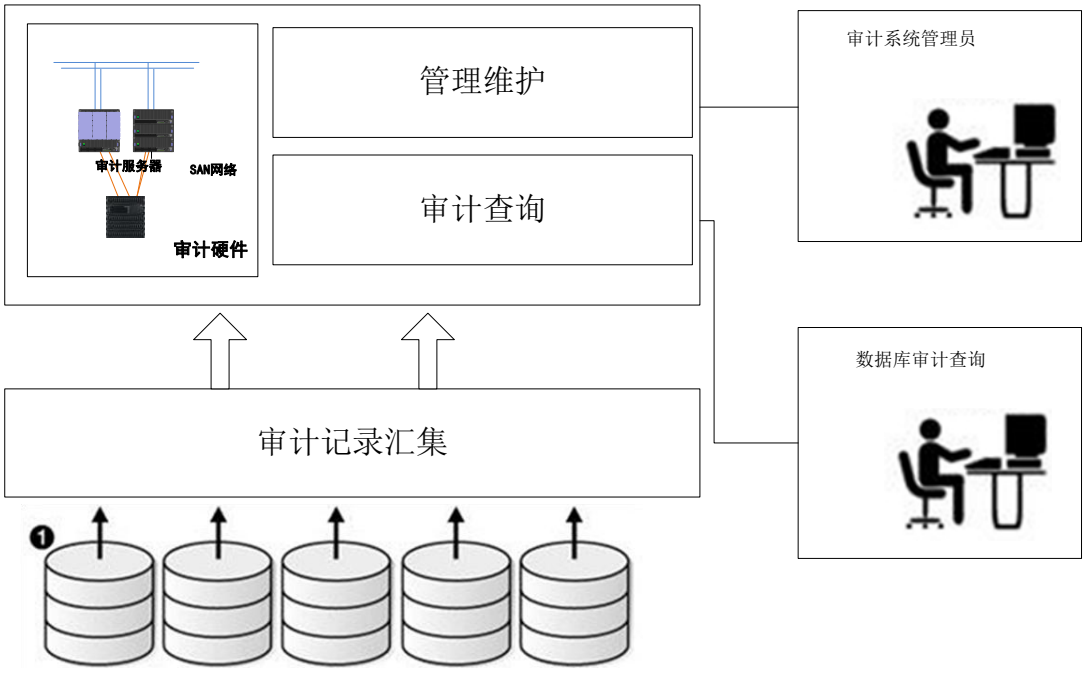
4）堡垒探针

堡垒探针应用了目前先进的技术作为支持，针对内部的网络设备和服务器进行保护，对此类资产的常用访问方式进行监控和审计。例如对字符终端、图形终端等访问方式进行监控和审计，实现对用户运维过程的标准化管理，满足交警内部网络对数据库核心资源的访问安全的要求。

堡垒探针应至少支持如下协议进行审计：SQL、Telnet、FTP、SSH、RDP（Windows Terminal）、X windows、VNC 等，从而加强系统运维层面的安全管理。

5）主机探针

省交管审计系统



1）系统说明：

省总队部署一套硬件设备，采用 2 台数据库服务器，配置一台大容量磁盘阵列，用于全省审计数据的集中存放和管理服务，并对全省统一提供审计记录跟踪分析服务。

各地市开启数据库审计功能，对数据库 DML 操作、DDL 操作、及会话登陆

等重要数据库行为进行数据库审计，并将审计记录存放到数据库表中。定期将本地审计记录传输到省交管服务器中，传输后删除本地审计记录，以减轻对生产数据库的影响。

开发一套全省审计管理系统，在地市端实现审计记录定时传输到省交管局，并在确认传输完成后，对本地审计表数据进行清理；在省交管局实现审计数据对外统一服务，提供简洁实用的人机界面，提供审计记录的查询跟踪、提供可疑操作的监控及审计数据分析功能。

2）系统功能

1、通过利用各地市交通管理数据库本身的审计功能，可以针对核心表进行全面审计和监控，可以对包括直接在数据库主机上操作进行审计和记录，提供信息系统的安全。

2、通过自研软件，将全省各地市的数据库审计日志汇总到省总队，并依据省总队要求进行相关审计信息分析，提高信息系统安全预警。

3、对地市的安全审计状态进行监控和告警，一旦有地市的审计停止及时发出预警。

4、对地市的数据库安全审计记录汇总到省总队，并及时清理各地市的审计记录，减少由于审计记录过多而对地市业务系统造成的影响。

5、可以对其他相关的硬件审计设备的审计记录进行收集和联动，从而为省总队和地市提供更为全面的安全审计记录，做到全方位非法访问的跟踪和分析，找出信息系统可能存在的安全隐患。

投标方应在充分理解本项目的基础上，结合实际情况，遵循相关安全法律法规和安全标准，按照合规性、完整性、系统性的原则，**对本章节的技术要求进行逐项应答，给出“实质性响应描述”，同时还可以自行进行补充，所有技术要求的实质性响应描述和自行补充内容均有投标方承担相应责任。**

对于本项目中风险管理体系建设而言，应自始至终按照风险管理体系的技术要求进行，按照相应的系统开发流程和软件开发项目管理流程，最终开发出符合初始设计要求的**数据风险防护平台和数据风险管理平台。**

江苏省交警数据库安全审计监管平台的的设计是依照“结构化”体系设计方

法，首先把构建风险管理体系的基础部分，为风险防护平台和风险管理平台奠定基础。其次通过防护平台发现风险、定位风险、解决风险，并且对风险的持续、有效的管理。管理平台的核心是把风险管理与工作对应起来。根据风险指标体系进行风险识别、监视和评估，通过预警告警体系进行风险通告，通过防护平台、工作平台完成风险的自动化处置。信息安全各岗有责，各个岗位安全负责人员根据策略体系、知识库体系指导，基于风险支撑体系完成相关风险管控工作。

（3） 现有产品要求

指标项	指标规格要求
基本要求	★系统采用 B/S 架构，用户可以在不安装客户端的情况下访问系统；系统采用 J2EE 的架构进行开发，能够跨平台部署，支持的操作系统包括 Windows、Linux、UNIX 等主流操作系统；支持 ORACLE、MS SQL SERVER、MYSQL 等主流数据库；支持 NoSQL
性能要求	★单个事件采集代理信息采集能力：大于 3000 条/秒；单级平台事件处理能力：大于 2000 条/秒；联机事务处理响应时间：对于单步操作，响应时间应小于 5 秒；统计处理响应时间：对于大数据量的统计，应能保证在夜间（3 小时内）完成
安全要求	★系统应具有自检功能，能监视各功能模块的运行情况，随时发现系统自身的问题。产品内部组件之间通信支持加密传输，对采集到的日志进行加密存储，保证数据的完整性和机密性
事件管理模块	安全管理平台应广泛支持华为、H3C、思科、Juniper、微软、天融信、启明等主流厂商设备事件类型，以满足现有或将来部署的设备 支持 SNMP、Syslog、日志文件、ODBC/JDBC 等信息收集方式
脆弱性管理模块	★系统能够实时评估系统资产的脆弱度，支持导入第三方漏洞扫描报告；能够通过扫描报告的导入自动发现新的资产；

指标项	指标规格要求
	支持资产弱点生命周期管理：新发现、确认、已消除、已防护
威胁管理模块	系统应能够收集本项目中所有的安全设备、网络设备日志信息；支持任意字段作为条件查询安全事件 支持在事件存储阶段对事件进行过滤
关联分模块	★系统应支持基于攻击状态机模型的关联检测技术，支持图形化方式表示攻击回放，提供图形化的编辑方式，支持用户自定义关联分析场景，对于关联分析确认的攻击事件，采取预设规则进行响应处理（提供功能截图证明）
场景管理模块	★支持多种场景库，并对以下所列主要场景进行描述：对输错口令、越权访问、配置更改等可疑或违规行为的次数进行统计分析，并根据设定的阀值报警；支持对 ARP 病毒的监测和溯源。（提供功能截图证明）
知识库管理模块	系统应支持以分组的方式对系统中的知识文章信息进行管理 知识库分组包括：安全专家库，事故案例库，漏洞库，补丁库，病毒库，安全基本要求库，应急预案库，文档管理库 厂商应提供知识库的基本内容并定期更新，同时支持用户后期自行管理，包括：增加，删除，查询，移动，导入，导出，发布等操作
工单管理模块	系统应支持将需要处理的安全事件以工单的形式下发给负责人，并按照流程化管理工单。提供图像化界面，可自定义工单处理流程
风险管理模块	系统支持按照《信息安全风险评估规范 GB/T 20984—2007》和 ISO27001 标准的要求，实时分析重要资产和安全域的各类风险，风险级别按照等级进行划分 ★系统支持根据资产的安全需求、资产面临的威胁、存在的脆弱性三要素进行综合评估，给出当前资产的风险状况，并

指标项	指标规格要求
	且从保密性、可用性、完整性三个方面进行详细的风险展示能根据资产风险的状况进行资产评级、能根据安全域的风险状况进行安全域评级
预警管理模块	支持接收来自平台内部、第三方服务商和上级主管单位提供的安全预警信息，并将预警信息转发给相应的管理责任人
响应管理模块	★系统应支持对指定事件的响应，响应方式至少支持以下几种：防火墙阻断， SNMP Trap 告警， WinPop 告警，短消息告警，工单告警处理等。（提供功能截图证明）
等保管理模块	★系统支持等保定级、备案、现状调研、评估、差距分析、测评等日常管理功能，支持按照等级保护三级标准要求进行体系建设和日常运维管理；统支持按问卷任务和技术检查任务对测评项进行分类显示及统计的功能（提供功能截图证明）
数据采集模块	支持远程自动、代理两种数据采集模式。支持 Syslog、SNMP Trap、Netflow、JDBC 等协议数据收集。
产品资质	安全管理平台产品 IT 产品信息安全认证证书（中国信息安全认证中心）
	安全管理平台产品涉密信息系统产品检测证书（国家保密局涉密信息系统安全保密测评中心）；
	安全管理平台产品军用信息安全产品认证证书（军 C+级）（中国人民解放军信息安全测评认证中心）；
	安全管理平台产品计算机软件著作权登记证书（中华人民共和国国家版权局）；
	安全管理平台产品信息技术产品安全测评证书 EAL3 级（中国信息安全测评中心）
	安全管理平台计算机信息系统安全专用产品销售许可证(公安部公共信息网络安全监督局颁发，类别为安全管理平台)；
	数据库审计系统计算机信息系统安全专用产品销售许可证

指标项	指标规格要求
	(公安部公共信息网络安全监督局颁发)；
	堡垒机运维审计系统计算机信息系统安全专用产品销售许可证(公安部公共信息网络安全监督局颁发)；

（4） 平台技术参数

主要技术参数要求		
平台总体要求	设计要求	★符合公安部《公安信息通信网综合安全管理平台技术规范（试行）》（公科信[2011]114 号）相关要求
	架构设计	应支持多层体系结构，至少包含交互对象层、接入交换层、核心处理层、集中展示层。
		技术架构应支持面向服务体系结构(Service-Oriented Architecture，SOA)，具备跨平台、可伸缩和高可靠的特性。支持 B/S 模式管理安全管理系统。
		★初始配置不少于 100 个管理对象的授权许可
	总体业务流程	能够支持信息获取、信息预处理、业务处理、业务分析等多个业务流程阶段，支持各流程阶段策略配置。
		能够支持多种类型业务流程集中处理和按业务流程类型处理。
		应遵循业务流程处理和流程内容保密相结合的原则。
		能够支持平台内置主流的业务流程引擎，支持业务流程定制。
平台功能	集中展示	应提供集中化的运行数据呈现。提供相应权限的查阅与工作界面。
		能够提供安全首页集中展示平台重点安全信息，重点安全信息至少应包括：值班工作信息、个人工作信息、待办工作信息、最新安全事件、最先安全预警、最新安全通报、专项系统状态、下级平台状态、签到时间。
		能够提供运行监控、业务处理、安全分析、知识库等集中展示和用户交互界面。

	运行监控	能够提供平台自身状态信息监控，自身状态信息至少应包括：平台资源状态、平台模块状态、平台在线人数、平台当前用户、平台级联状态、平台当前时间
		★能够提供拓扑图方式进行专项系统状态信息监控，专项系统状态信息至少应包括：专项系统名称、在线状态、系统资源使用状态，支持通过配置增加更多专项系统状态信息
		★能够提供事件信息实时监控，支持对所监控的事件进行选择过滤、支持对所监控的事件字段进行展示配置、支持事件字段展示配置和过滤相关联、支持通过事件 IP 字段查看资产信息、支持事件信息实时刷新间隔设置和刷新启动停止
		★能够提供监视仪表盘对被监控安全对象运行信息实时监控,支持的安全对象类型至少包括：网络类、应用类、安全类、主机服务器类等，支持的运行信息类型至少包括：安全对象状态、安全对象事件，支持仪表盘展示方式至少包括：幻灯片、相框、饼图、柱图、折线图、表格、树状表格、指示灯等展示方式，支持多种页面布局，支持内容实时刷新
	业务处理	★能够提供签到、巡检、签收、通知、通报、预警、响应处置、审核等业务流程，支持流程多级平台级联流转，支持级联流程和本级流程关联，支持流程按处理状态分类管理
		★能够提供可视化流程图，支持流转过程展示、支持流程当前流转节点展示
		能够提供流程处理过程记录，支持记录流程处理节点、处理时间、处理人员、处理方法、处理结果
		能够提供流程处理催办功能，支持催办记录包括被催办的流程处理节点、催办时间、催办人员、催办内容
	业务统计分析	★能够提供对事件、业务流程、系统运行信息、安全考核指标等数据的业务统计分析，支持查询统计分析、报表统计分析、仪表统计分析等分析方式

		支持依据事件时间、事件类别、事件级别、IP 地址、区域、资产、处理状态、响应级别、报警等级等对安全事件、事件等进行统计分析
		支持依据人员、部门、区域、事件类别、流程名称、完成率、超时率等组合统计和分析
		支持依据专项系统的名称、服务名称、时间、系统提供商、区域、性能指标、连续工作周期等组合统计和分析
		支持定期（如周、月、季度、年）自动和人工方式统计与分析。支持 word、excel、html、pdf 报表格式。支持图形化的报表呈现模式如柱形图、饼形图等。支持统计分析与考核数据的修订。支持通过图表查询、展示、打印、存储分析结果。支持变化趋势图表、TOP N 数量图表、详细信息图表等，支持自动将报表发送到负责人的邮箱中。
		能够提供报表管理支持强大的定制功能，用户可以自定义报表的 logo、大标题、小标题、统计内容、统计条件以及统计图形样式等。支持预置报表至少包括：资产风险走向报表、资产风险统计报表、资产风险等级统计报表、资产漏洞统计报表、漏洞级别统计报表、漏洞资产统计报表、资产补丁统计报表、资产类型统计报表、资产硬件信息统计报表、资产软件信息统计报表、资产脆弱性统计报表和脆弱性收集过程报表
	关联分析	★能够提供关联分析功能，对各类信息资源进行综合分析、挖掘和归并，发现隐藏在独立事件与业务背后的规律与事实
		★能够支持基于状态机的关联分析，支持图形化方式展示攻击过程，支持出场预置关联分析规则，规则条数不少于 50 条
		能够通过关联分析确认的攻击事件，采取响应处理
	业务配置	能够提供监控报警功能监控安全问题产生报警事件、触发报警响应，支持多种安全问题监控方式至少包括：字段匹配方式、关联分析方式，支持安全问题监控规则策略配置，支持多种报警响应方式至少包括：邮件、短信、消息、声光、命令行等

		能够提供信息预处理功能，支持信息解析预处理、信息补全预处理、信息分级预处理、信息过滤预处理、安全事件确认和分配预处理。
		能够提供业务流程配置功能，支持流程流转节点处理用户和处理角色的配置，支持用户个性化流程定制
		能够提供模板配置功能，支持应急预案模板配置，支持统计分析模板配置，支持仪表分析模型配置
	平台管理	能够提供用户与授权管理功能，支持提供多用户、分权限的管理，支持多用户在系统平台上同时协同工作，支持用户按所分配权限访问系统功能和防止用户越权使用系统，支持系统菜单访问权限细致划分功能，支持控制用户的登陆 IP、登陆次数、有效时间等，支持角色增删改查管理，支持用户增删改查管理，支持包含公安数字证书在内的双因子认证，支持三权分立
		能够提供系统自审计功能，支持记录每个用户进入、退出平台的时间以及在平台中的所有操作的内容且审计内容至少包括：事件名、用户、时间、重要级别、操作详细内容、操作结果，支持系统自身运行日志信息记录，支持日志记录的查询、格式化导出分析，支持审计角色才有权限查看审计内容
		★能够提供数据管理功能，支持法律法规库、分类事件库、案例库、各种模板库、安全漏洞库、安全补丁库、病毒库、资产安全对象库、人员库等，支持查看数据库版本名称、型号、版本信息，支持查看数据库的数据分区信息，支持查看数据库分区恢复、数据库数据同步，支持数据库磁盘不足产生事件提醒，支持数据库自动备份或人工备份，支持数据导入导出
		能够提供系统配置功能，支持安全交互对象的日志源配置，支持邮件服务器配置，支持系统组件模块启停及状态查看，支持数据库状态查看，支持安全事件自动确认规则配置
		能够提供备份与恢复功能，支持系统备份恢复和数据库备份恢复，支持冷备份和热备份

		能够提供安全策略管理功能，支持安全策略文档的上传、下载、在线阅读、审批、发布等管理操作，支持安全策略数据导入、导出、归档、版本控制等功能，支持多种安全策略发布方式至少包括：Email 方式、页面方式、终端管理联动方式
	接入管理	能够提供平台级联功能，支持事件数据信息级联传递，支持业务流程级联交互，支持策略数据信息级联下发，支持下级自动向上级注册和联通性检测
		支持集中化管理、分布式采集的业务模式，所有采集的数据只保存于省级中心
		能够提供安全对象数据采集功能，支持多厂家多种类型设备至少100 种以上，支持新设备采集扩展接口且可现场通过配置完成新设备支持，支持多种采集方式至少包括 Syslog、SNMP(V1、V2、V3)、SNMP Trap、XML、JDBC/ODBC、Flatfile、HTTP、TELNET、NETFLOW、WMI、Opsec 等
		支持的数据库对象包括：Oracle、SQL-Server、DB2、Informix、Sybase、PostgreSQL、人大金仓 kingbase、Cache、南大通用 Gbase、达梦、MySQL 等
		能够导入第三方漏洞扫描报告，至少支持：Nessus 扫描报告、McAfee FoundStone 扫描报告、绿盟极光扫描报告、榕基扫描报告。
		能够提供问卷调查功能，支持在线、离线调查方式，支持问卷项和问卷模板配置，支持问卷结果、资产、脆弱性相关联
	合规管理	★系统支持等保定级、备案、现状调研、评估、差距分析、测评等日常管理功能，支持按照等级保护三级标准要求进行体系建设和日常运维管理。系统支持按问卷任务和技术检查任务对测评项进行分类显示及统计的功能
	网络探针	★硬件（14 台），2U 机架式，2 个 10/100/1000BASE-TX 管理口，4 个 SFP 插槽，4 个 1000BASE 电口采集口，1T 存储空间；记录事件数>40000 条/秒，总记录时间>10 亿条，可审计并发数据库用户数>1000，三年质保

	堡垒探针	★硬件（14 台），1U 机架式结构型；4 个 10/100/1000BASE 自适应电口，可扩展至 12 个千兆接口，1T 存储空间；50 个主机/设备许可，无用户数限制，三年质保
	主机探针	★软件，可以部署于 windows、linux 和 unix 操作系统，实时采集数据库本身的审计记录，针对核心表进行全面审计和监控，可以对包括直接在数据库主机上操作进行审计和记录
	移动维护终端	★硬件（2 台），国际知名品牌，Intel i7 处理器，内存 8G 以上，256G 固态硬盘+1TB 机械硬盘，独立显卡，显存 2GB 以上，14 吋屏，五年质保。
	采集平台	★软件，支持采集网络探针、堡垒探针、主机探针的数据，转发至省级统一安全管理平台，支持采集数据的过滤和归并，支持接收省级安全管理平台的安全策略
	系统环境	支持多种操作系统平台部署，至少包括 Windows、Linux、Unix 等主流操作系统；支持多种浏览器，至少包括 IE 等主流浏览器。
	部署方式	支持多级分布式部署，支持单级多模块分布式部署。支持系统运行中增删模块组件不影响系统的正常运行，支持模块组件运行错误在自有进程中隔离不影响其他模块组件运行。
	数据库	平台自身部署支持多种主流数据库，至少支持一种主流国产数据库
平台性能	稳定性	支持系统主要功能组件 7*24 运行； 系统年运行率单机不低于 99.99%，双机不低于 99.99%； 对被采集对象的内存资源占用不超过 3%，对网络带宽占用不超过 10%； 事件采集器对于所在主机和服务器的 CPU 利用率占用<2% 。
	实时性能	代理模块实时收集能力>180,000 条/分 服务器模块实时分析处理能力>120,000 条/分 数据入库模块实时处理能力>60,000 条/分 系统具备分布式计算能力，能够适应复杂的应用环境的高负载处理。

	安全性	支持与第三方数字证书认证技术相结合。
		可配置帐号口令的强度，可以设定登录尝试次数，超过阈值自动锁定系统。能够指定可访问的 IP 地址范围，支持通过 HTTPS 协议进行 WEB 访问
		支持和第三方系统的 Web Service 接口可以使用 HTTPS 协议传输，支持 WebService-Security 规范。
		系统用户密码数据存储进行加密处理，确保私密性、防止篡改。
		平台各个模块组件之间的网络通信应采用加密协议，确保数据流和控制流的传输私密性。
	存储性能	事件存储能力：具备海量存储能力，能够将原始事件存放至少 3 个月，以备审计查询，具备 10Tb 的数据管理和分析能力；
平台易用性	使用	全部功能提供联机帮助文档
		支持显示界面菜单隐藏
平台扩展功能	脆弱性管理	支持导入第三方漏洞扫描报告，至少支持：天融信扫描报告、Nessus 扫描报告、McAfee FoundStone 扫描报告、绿盟极光扫描报告、榕基扫描报告、Xscan 报告。 支持将漏洞扫描报告和资产关联。支持资产弱点生命周期管理：新发现、确认、已消除、已防护。支持图形化方式表现资产脆弱性统计报表。
	风险管理	支持以仪表盘的形式显示当前风险值和历史风险平均值。 支持显示资产或安全域在最近一段时间内的风险走势 支持把当前资产或安全域的威胁以列表的形式展示。 支持把当前资产或安全域的漏洞以列表的形式展示。 支持自动对超过既定阀值的风险进行报警。 依据风险级别以不同颜色显示在图标中。
	溯源分析	★支持按照不同的数据库操作行为进行实时监控和分类展示； 支持根据违规结果信息进行溯源，至少能追溯至业务应用系统的用户账号这一级别

	辅助决策	支持处理国内知名厂家（如：天融信、绿盟等）上传的 IDS 事件时，将入侵时间的处理方案作为辅助决策，并关联到对应事件中。
开发要求	定制开发	★按照招标需求在投标人原有安全管理平台成熟产品基础上开发符合我单位要求的数据库综合安全管理平台，同时应具备成熟的数据库审计产品和堡垒机产品，以便将此 2 款产品功能以模块的方式集成进安全分析平台。 定制开发内容主要包括平台扩展功能、探针互动，其他功能和要求应为现有产品必须具备。 开发方式在用户现场或用户指定地点开发,开发人员不少于 10 人。

（五）研发、实施及服务要求

（1） 研发要求

1）项目研发方式要求

- 研发方式：要求在现有安全管理平台基础上二次开发。中标供应商应按照总体目标和具体目标要求，负责项目需求的设计、编写和完善，确保需求的可用性、完整性、系统性和有效针对性。
- 需求完善、需求分析、功能设计、总体设计、技术设计和界面设计等各阶段，中标供应商均须将相关文档提交采购人确认。
- 研发地点：在用户现场进行开发和测试。

2）项目计划安排要求

项目时间总体要求：从中标之日起 60 个工作日内完成系统上线并运行。

3）项目研发团队和人员要求

研发人员要求：参加本系统研发的人员必须具备相关经验和能力，投标方必须安排对现有系统熟悉、对相关领域熟悉的人员参与本项目。

（2） 项目开发和组织规范要求

1) 开发要求

项目团队中开发人员不少于 10 人，应保证四到位原则（人员到位、时间到位、团队能力到位、项目质量到位），确保本系统与总队系统顺利对接。

2) 项目组织管理要求

- 要求投标人成立专门的项目开发实施小组，并提供项目经理和项目成员的人员名单以及具体职责安排。
- 项目经理应具有代表中标方全权负责本项目的权力，如项目管理、协调和沟通等工作；
- 中标方必须保证项目组织成员的稳定性，中标方不得随意抽调项目组成员。如需更换实施人员必须取得采购人同意，并提供合适的可选择的后备人员。
- 要求投标人必须明确合理的开发地点、组织方式。项目开发地点和组织方式，采购人有权提出合理变更。
- 投标人必须提供具体的与项目试点单位和项目其他单位的沟通协调方式，项目沟通流程、沟通计划，确保项目实施能够按部就班地进行；
- 投标人必须提供到货验收计划、工程实施策略、与现有系统的联动结合等问题，共同讨论制定并确认详细设计方案；
- 投标人必须提供详细的工程开发实施方案，工程进度计划，制定工程进度计划书、划分工程实施阶段、确定阶段性目标以及双方技术人员的安排等内容，其内容提供电子文档，并必须由采购人进行论证确认方可实施；
- 投标人必须针对本项目提供完善的风险管理与控制计划，便于项目实施能够按时完成；
- 投标人必须针对本项目提供切实可行的质量管理与控制计划，便于项目实施能够按质完成；
- 投标人自身项目实施所需人员工作生活费用、机器设备、场地和开发环境等一切相关费用自理。

3) 项目试点和推广应用要求

- 项目实施范围：江苏省公安厅交警总队、地市支队。
- ★时间要求：2 个月内成功运行。

投标人必须提供实施方案（最终方案由采购人确定），实施单位准备工作要求、实施的策略、实施计划安排、双方参与人员及职责、与项目单位和项目其他单位的沟通协调方式和方案、上线风险防范和应急预案、验收内容及标准、验收组织及流程等内容。

（3） 项目质量控制要求

1) 系统设计及开发质量控制要求

在需求分析基础上，应严格按照 CMM 标准流程，进行系统功能设计。开发小组至少包含系统架构师、软件工程师、数据库开发工程师、安全顾问等角色。系统交付应提交所有文档，主要包括：

- 需求设计说明书
- 功能设计说明书
- 技术设计说明书
- 其他分析设计文档
- 用户操作说明书

2) 系统测试要求

系统开发完毕及实施过程中，需要进行严格测试，并出具详细的测试报告，包括：

- 功能测试
- 用户界面测试
- 性能测试
- 安全性测试
- 兼容性测试
- 回归测试

- 联调测试
- 现场模拟测试

（4） 项目研发地点要求

项目人员工作地点：在用户现场（或用户指定地点）封闭式开发。

（5） 实施要求

1) 项目实施要求

- 根据用户实际需求编写和提交项目实施方案，合理组织实施人员进行现场实施。提前告知用户单位实施环境和配合事项，制定实施管理制度，按照实施进度计划有序进行。
- 实施不能影响业务正常运行，同时制定备份和恢复计划和应急响应流程。
- 全省实施分成 4 个小组同时进行，实施人员不少于 8 人。

2) 项目验收要求

- 投标人必须提供可行的系统测试方案，及时发现并解决系统试运行期间的出现各种问题；
- 投标人必须提供针收对本项目的工程验收方案，包括：验收的时间、验收的项目、项目符合度自验报告（含合法合规性承诺）、验内容、验收方法、验收文档、验收通过的条件、验收组织方式建议等；
- 项目单位可根据合同及招标文件规定对现场验收内容和具体基数指标进行修改和补充，经双方确认后形成现场验收文件并作为现场初步验收依据；
- 系统测试中如发现产品性能指标或功能与产品技术文档或投标技术文件上所描述不符，将被视为性能或功能不合格，项目单位有权拒绝验收；
- 投标人必须将系统符合的要求全部有关技术文件、资料、安装、测试、验收报告等文档汇集成册交付项目单位；
- 从实施单位现场初步验收报告签署之日起系统进入试运行期，整个系统试运行期为两个月。2 个月内没有出现技术问题，由投标人提交终验单，由省交

警总队组织终验，相关费用由中标供应商负责，系统终验收合格后签署系统终验报告，进入质保期。

（6） 质保要求

★投标人必须提供至少三年的升级和质保服务，产品必须保证采购人长期的、合法的正常使用权，确保产品长期正常可用。质保期自项目终验报告签署之日起计算；

- 在质保期内，如果产品软件有更高的版本推出，投标人应主动告知项目单位，并根据投标人要求及时进行免费升级，同时提交“升级报告”、升级避险及应急方案和升级版本相关文档；
- 所有质保方式均为上门保修，即由原厂商派员到项目单位现场维护；
- 在质保期内，投标人必须组织有能力和熟悉项目单位应用情况的人员成立质保服务队伍，负责全省质保期内多种方式（电话、邮件、现场等）服务。项目单位系统应用出现重大问题或风险事件，必须由有能力人员提供现场服务，直到解决问题为止。服务响应时间要求：一般服务：7×24 小时；现场服务时间：1 小时。
- 在设备扩容及软件（包括数据库等第三方软件）安装和升级时，投标人应及时派技术人员到场指导和协助；
- 在质保期间内，分别为每个地市支队及省总队提供不少于每季度一次的巡检、故障处理或软件 bug 修订服务。
- 投标人必须根据系统应用情况，及时协助项目单位修改、调整配置，使系统在最优状态下运行，最大限度地利用各种系统资源；

（7） 应急响应服务要求

- 接到项目单位系统故障处理请求后，要求投标人在 30 分钟内给予响应，及时解决系统运行故障，保证系统正常运行；
- 在故障处理过程中，要求投标人保证每天向用户通报一次处理情况，特殊情况随时通报；

- 若 8 小时内仍无法解决系统故障，投标人必须更换同等或更高性能的设备，提出应急处理方案，以保证项目单位的系统稳定运行和整体安全；
- 原厂商必须在故障处理结束后 24 小时内向项目单位提供书面故障处理报告；
- 对于不能明确是否是该项目产品出现故障时，投标人应在上述响应时间内到达现场，协助项目单位进行检查，排除问题。

（8） 培训要求

投标人必须提供针对本项目的现场培训计划，包括：培训目标、培训时间、培训地点、培训人员，以及具体培训课程和内容。

- 投标人必须提供针对本项目的用户现场培训，免费对项目单位相关技术人员进行相应的培训；
- 现场培训必须由原厂商工程师主持进行，使之能够满足日常运行操作及维护的要求。

（9） 项目安全和保密要求

1、中标供应商及所有参与项目研发和实施所有人员必须签署安全保密协议，并承担相关法律责任；

2、中标供应商项目完成后，所有涉及采购方的信息系统的资料及数据不得留存和对外泄密，若发生违规事件并产生严重后果，采购方有权追究其相关法律责任；

3、安全性和合法性要求

A、 要求投标人提供的产品不得存在漏洞和后门；

B、若产品发现软件缺陷，投标人必须在 30 日内发布补丁程序，并于 10 天内向项目单位提供补丁程序并负责相关技术实施。

C、投标人必须确保项目产品和技术平台在本项目实施中不得有版权纠纷和法律问题。

D、项目研发期间应充分考虑平台性能与硬件服务器的配比关系，不可无理由增加。如需增加提供详细方案。

E、采购人项目运行不需再买第三方任何软硬件产品（项目系统运行所需服务器除外），产品在使用过程中不能有版权纠纷。

F、投标人不得把列入国家范围内的涉密信息和涉密技术放进投标文件中。

第六章 投标文件格式

注：请投标人按照以下文件的要求格式、内容，顺序制作投标文件，并请编制目录及页码，否则可能将影响对投标文件的评价。

投标文件

【正/副本】

项目编号：

项目名称：

分 包 号：

投标单位（全称）：

授权代表：

联系电话：

日　　期：

目 录

请投标单位编制目录及页码，否则可能将影响对投标文件的评价。

一、投标函、投标报价及项目相关文件

1.投标函

江苏省省级行政机关政府采购中心：

你们江苏省公安交管数据库安全审计监管平台（采购编号为：SJC2014120371）招标文件（包括更正公告，如果有的话）收悉，我们经详细审阅和研究，现决定参加投标。

1、我们郑重承诺：我们是符合《政府采购法》第 22 条规定的供应商，并严格遵守《政府采购法》第 77 条的规定，本投标文件中提供的所有材料均是真实有效的。

2、我们接受采购文件的所有的条款和规定。

3、我们同意按照本采购文件第一章“投标（响应）供应商须知”第 3.6 条的规定，本投标文件的有效期为从开标之日起计算的九十天，在此期间，本投标文件将始终对我们具有约束力，并可随时被接受。如果我们中标，本投标文件在此期间之后将继续保持有效。

4、我们同意提供采购中心要求的有关本次采购的所有资料。

5、我们理解，你们无义务必须接受投标报价最低的投标，并有权拒绝所有的投标。同时也理解你们不承担我们本次投标的费用。

6、如果我们中标，为执行合同，我们将按投标供应商须知有关要求提供必要的履约保证。

投标供应商名称：_____（公章）

地址：_____邮编：_____

电话：_____传真：_____

法定代表人（授权代表）（签字或盖章）：

职务：_____

日期：_____

2.开标一览表

分包号	_____
投标报价合计	￥____圆整 人民币（大写）____
投标供应商企业标准	_____（请填写：大、中、小、微型）企业
投标报价总计中，小、微型企业产品报价合计	￥____圆整 人民币（大写）____
交付时间	签订合同后_____日历天内

投标供应商全称（公章）：

法定代表人（授权代表）（签字或盖章）：

注：

（1）投标报价应包括采购文件所规定的采购范围的全部内容。

（2）投标供应商不得实质性改动开标一览表格式及内容。

（3）企业标准请参照《关于印发中小企业划型标准规定的通知》（工信部联企业【2011】300 号）文件规定自行填写。

（4）投标供应商如使用小、微型企业产品投标，请如实填写小、微企业产品报价合计，并按要求提供相应的《中小企业声明函》。

（5）投标供应商使用小、微型企业产品投标，小、微型企业产品可给予 6%的价格扣除，用扣除后的价格参与评审。

3.投标报价明细表（货物类）

分包号：_____

序号	物品名称	详细部件名称	数量	单位	品牌	单价	总价	生产厂商	产地	质保期	备注
1	（请勿缺项）其 他										
2											
3											
4	安装调试、培训、售后服务等其他所有费用（请列明细）										
非小、微型企业产品报价总计			人民币（大写）：_____圆整 ￥：_____								
序号	物品名称	详细部件名称	数量	单位	品牌	单价	总价	生产厂商	产地	质保期	备注
1	（请勿缺项）										
小、微型企业产品报价总计			人民币（大写）：_____圆整 ￥：_____								
投标报价总计			人民币（大写）：_____圆整 ￥：_____								

投标供应商全称（公章）：____ 法定代表人（授权代表）（签字或盖章）：_____

注： （1）此表为表样，行数可自行添加，但表式不变。

（2）相关安装调试费用、质保及人员培训、后续服务及其他所有费用由供应商自行计算填列。

（3）总价=单价*数量，数量由投标供应商自行计算并填列。

（4）上表中的“投标报价总计=非小、微企业产品报价合计+

小、微企业产品报价合计”，此总计数应当等于“开标一览表”中“投标报价总计”数。

（5）上表中的“小、微型企业产品报价合计”数应当等于“开标一览表”中“小、微型企业产品报价合计”数。参与价格评审的价格=（非小、微型企业产品报价合计）+小、微型企业产品报价合计*（1-6%）。

（6）投标供应商必须保证承诺使用小、微型企业产品参加投标的真实性，如出现虚假响应，一经查实，将按照采购文件第一章第6.1.3条规定进行处理。

（7）若本项目有多个分包的，则每个分包须分别填写此表，并注明分包号。

（8）评审委员会将就此表中小微企业产品明细内容对照供应商提供的《中小企业申明函》进行审核，如产品未提供相应的《中小企业申明函》，将不做价格扣除。

4.技术要求响应表（货物类）

分包号：_____(如果有分包)

序号	品名	采购需求 主要技术条款描述	所投产品 相应技术指标描述	偏离情况
1				
2				
3				
4				
5				
	……			

投标供应商全称（公章）：_____

法定代表人（授权代表）（签字或盖章）：_____

注：（1）此表为表样，行数可自行添加，但表式不变。

（2）投标供应商根据系统方案添加的设备、材料等也请列出。

（3）是否偏离用符号“+、=、-”分别表示正偏离、完全响应、负偏离。

（4）投标供应商必须仔细阅读本采购文件“第五章”中所有技术规范条款和相关功能要求，并将响应情况及偏离情况逐项填入上表，响应时不得对原有技术规范进行直接复制粘贴及简单表述为完全响应，否则将影响该项得分。**采购文件中标注必须满足的核心技术要求响应情况必须在上表中予以明确描述，缺项、漏项及描述不清将按重大负偏离处理。**投标供应商必须根据所投货物实际情况如实填写，评审委员会如发现有虚假描述的，该投标文件视为无效，并按照相关法律法规规定对供应商进行处罚。

（5）若本项目有多个分包的，则每个分包须分别填写此表，并注明分包号。

5.商务需求响应表（货物类）

分包号：_____(如果有分包)

序号	项目	采购需求 主要商务条款 描述	投标供应商 相应承诺 描述	偏离 情况
1	免费质保期			
2	售后服务要求			
3	项目完成时间(投入			

	工作时间、交货时间等）			
4	交货方式			
5	培训要求			
6	付款方式			
7	备品备件及耗材等要求			
8	人员安排			
	……			

投标供应商全称（公章）：_____

法定代表人（授权代表）（签字或盖章）：_____

注：（1）此表为表样，行数可自行添加，但表式不变。

（2）投标供应商根据项目添加的服务承诺、培训等也请列出。

（3）是否偏离用符号“+、=、-”分别表示正偏离、完全响应、负偏离。

（4）投标供应商必须仔细阅读本采购文件“第五章”中所有商务条款和相关服务要求，并将响应情况及偏离情况逐项填入上表，响应时不得对原有商务条款和服务要求进行直接复制粘贴及简单表述为完全响应，否则将影响该项得分。**采购文件中标注必须满足的核心商务要求响应情况必须在上表中予以明确描述，缺项、漏项及描述不清将按重大负偏离处理。**投标供应商必须根据所将提供服务的实际情况如实填写，评审委员会如发现有虚假描述的，该投标文件视为无效，并按照相关法律法规规定对供应商进行处罚。

（5）若本项目有多个分包的且服务相同的，则只需填写一份此表，并注明“所有分包”。否则每个分包须分别填写此表，并注明分包号。

6.技术支持性文件

分包号：_____(如果有分包)

序号	产品	技术支持文件名称及类型 （如彩页、说明书、官方网站资料等）	证明材料 （第几页—第几页）
1			
2			
3			
4			
5			
6			
7			
	……		

投标供应商全称（公章）：_____

法定代表人（授权代表）(签字或盖章)：_____

注：(1）此表为表样，行数可自行添加，但表式不变。

（2）若本项目有多个分包的，则每个分包须分别填写此表，并注明分包号。

7.技术方案

8.实施方案

本项包括供货方案、安装方案、验收方案、培训方案、售后服务

方案等，应包含且不限于下列内容：

项目实施进度、人员安排、运输安装方案、质量保证措施、与其他单位交接配合方案、验收方案、培训计划（包括时间、地点、人员数量、授课师资、授课效果等内容）、售后服务方案（包括服务时间、响应时间、服务人员水平和能力、重大活动保障方案）等内容。

（如果需要）附表：项目人员安排一览表

序号	姓名	在本项目中担任的职务	职称	身份证号码	主要资历、经验及承担过的管理项目
1	……	项目经理（请列明细）			
2	……	主要管理和技术人员（请列明细）			
3	……	其他人员（请列明细）			

投标供应商全称（公章）：___

法定代表人（授权代表）（签字或盖章）：_____

注：（1）此表为表样，行数可自行添加，但表式不变。

（2）项目人员资质、管理经验证明文件、本单位员工证明文件等另附。

（3）若本项目有多个分包的且人员安排相同的，则只需填写一份此表，并注明“所有分包”。否则每个分包须分别填写此表，并注明分包号。

9.经营业绩

分包号：_____(如果有分包)

序号	业绩名称	采购单位	签订时间	合同金额（万元）	证明材料（第几页—第几页）

投标供应商全称（公章）：_____

法定代表人（授权代表）(签字或盖章)：_____

注：(1) 此表为表样，须填写完整，行数可自行添加，但表式不变。

(2) 投标供应商所提供的经营业绩须列入上表，评审委员会将依据每个经营业绩所附证明材料的有效性判断该业绩有效性。

(3) 若本项目有多个分包的且经营业绩相同的，则只需填写一份此表，并注明“所有分包”。否则每个分包须分别填写此表，并注明分包号。

10.其他材料

序号	其他材料名称	发证或出具日期	发证或出具部门	证明材料（第几页—第几页）
1	财务审计报告			

2	认证、奖励证书			
3	……			

投标供应商全称（公章）：

法定代表人（授权代表）（签字或盖章）：

注：（1）此表为表样，须填写完整，行数可自行添加，但表式不变。

（2）投标供应商所提供的财务报告、经营信誉及其他荣誉等材料须列入上表。评审委员会将依据每个品目所附证明材料的有效性判断该项的有效性。

11. 中小企业声明函

中小企业声明函 1

本公司郑重声明，根据《政府采购促进中小企业发展暂行办法》(财库[2011]181 号)的规定，本公司为_____(请填写：大型、中型、小型、微型)企业。

一、根据《工业和信息化部、国家统计局、国家发展和改革委员会、财政部关于印发中小企业划型标准规定的通知》(工信部联企业[2011]300 号)规定的划分标准，本公司为_____(请填写：大型、中型、小型、微型)企业。

二、本公司参加采购编号为 SJC2014120371 的江苏省公安交管数据库安全审计监管平台项目采购活动提供本企业制造的货物，由本企业承担工程、提供服务，或者提供其他____(请填写：中型、小型、微型)企业制造的货物。本条所称货物不包括使用大型企业注册商标的货物。

本公司对上述声明的真实性负责。如有虚假，将依法承担相应

责任。

企业名称(盖章)：

日　期：

注：(1) 投标供应商必须同时满足此声明函中两个条件对中小微型企业的划型标准，才可称为中小微型企业。

（2）投标供应商为中小微型企业或大型企业使用中小微型企业制造的货物参加本次政府采购项目需提供此声明函。

（3）投标供应商如不提供此声明函，价格将不做相应扣除。

中小企业声明函 2

本公司郑重声明，根据《政府采购促进中小企业发展暂行办法》(财库[2011]181 号)的规定，本公司为_____ (请填写：中型、小型、微型)企业。

一、根据《工业和信息化部、国家统计局、国家发展和改革委员会、财政部关于印发中小企业划型标准规定的通知》(工信部联企业[2011]300 号)规定的划分标准，本公司为_____(请填写：中型、小型、微型)企业。

二、_____（投标单位名称）参加采购编号为 SJC2014120371 的江苏省公安交管数据库安全审计监管平台项目采购活动提供的（投标货物名称、型号）为本企业制造的货物。

本公司对上述声明的真实性负责。如有虚假，将依法承担相应责任。

货物制造企业名称(盖章)：

日　期：

注：（1）投标供应商使用其他中小微型企业制造的货物参加本次政府采购项目，需由货物制造企业提供此声明函。

（2）货物制造企业如不提供此声明函，价格将不做相应扣除。

注：（1）1—2 项均须法定代表人（授权代表）（签字或盖章）并加盖投标供应商单位公章

未提供或未按要求提供将不能通过符合性审查。

二、资格证明文件

序号	采购文件要求的 资格证明文件	供应商提供的资格证明文件 （须标明名称及对应页码）	是否 响应
1	企业法人营业执照或事业单位、科研机构等法人证书（在有效期限内，提供复印件，原件备查） 注：如本项目允许联合体投标（响应），则联合体中各单位均须提供有效的营业执照或法人证书复印件。		
2	法人授权委托书原件（格式见附件 1）		
3	采购文件第三章第二条所规定条件、 （一）法人或者其他组织的营业执照等证明文件，自然人的身份证明；（二）开标前六个月内（2014 年 11 月至今）中任一月份的财务状况报告复印件（至少包括资产负债表和利润表）（自然人可以不提供，法人或者其他组织成立未满三个月的可以不提供）；近六个月（2014 年 11 月至今）中任一月份的依法缴纳税收和社会保障资金的相关材料（提供相关主管部门证明或银行代扣证明的复印件，根据国家相关政策免缴或迟缴的需提供相关证明材料）；（三）具备履行合同所		

	必需的设备和专业技术能力的证明材料，须包含： 1、投标人具备涉及国家秘密的计算机信息系统集成乙级（适用地域为江苏省）及以上资质； 2、投标人具备不少于6名CISP认证的服务人员,(提供证书复印件及上述人员近三个月内的缴纳社保证明材料)。本项目开发管理团队中,必须有服务人员具有CISE、CISO、CISA证书。（提供证书复印件及上述人员近三个月内的缴纳社保证明材料） 3、投标人须提供针对本建设项目单独核算管理和接受建设单位延伸审计的承诺书原件(格式见附表2)。 (四)参加政府采购活动前3年内在经营活动中没有重大违法记录的书面声明（格式见附表3)。		
4	……		

说明：上述所列资格证明文件为必须提供内容，未提供或未提供有效材料的，将不能通过符合性审查。

三、相关附表格式

1.法人授权委托书

江苏省省级行政机关政府采购中心：

本授权书宣告：

委托人：_____

地　　址：_____ 法定代表人：_____

受托人：姓名_____ 性别：____ 出生日期：____年__月__日

所在单位：_____职务：_____

身 份 证：_____联系方式:_____

兹委托受托人_____合法地代表我单位参加江苏省省级机关政府采购中心组织的（采购编号为：SJC2014120371）江苏省公安交管数据库安全审计监管平台项目的政府采购活动，受托人有权在该投标活动中，以我单位的名义签署投标书和投标文件，与集中采购机构协商、澄清、解释，质疑，签订合同书并执行一切与此有关的事项。

受托人在办理上述事宜过程中以其自己的名义所签署的所有文件我均予以承认。受托人无转委托权。

委托期限：至上述事宜处理完毕止。

委托单位　（公章）

法定代表人（负责人）　（签字或盖章）

____年____月____日

备注：

（1）本授权书一式两份，供应商授权代表须在开标前持一份授权书原件及本人身份证件办理签名报到，另一份授权书原件放置在投标文件正本中。**非授权代表办理上述事宜，采购中心将拒绝。**

（2）供应商法定代表人直接参加投标的，无须提供法人授权委托书，但须持本人身份证件及营业执照复印件办理相关手续。

2.总公司授权委托书

江苏省省级行政机关政府采购中心：

本授权书宣告：

委托单位：_____

地　　址：_____ 法定代表人：_____

受托单位：_____

地　　址：_____ 负责人：_____

兹委托我下属公司_____合法地代表我单位参加江苏省省级机关政府采购中心组织的（采购编号为SJC2014120371）江苏省公安交管数据库安全审计监管平台项目的政府采购活动，并授权其以自己的名义独立办理以下事宜：

（1）参加投标活动；

（2）出席开标会议；

（3）签订与中标事宜有关的合同；

（4）负责合同的履行、服务及在合同履行过程中有关事宜的洽谈和处理；

（5）由受托单位以自己的名义另行出具授权委托书授权其受托人具体承办上述事宜。

受托单位在办理上述事宜过程中以其自己的名义所签署的所有文件我均予以承认。

委托期限：至上述事宜处理完毕止。

委托单位　（公章）

法定代表人　（签字或盖章）

二〇一*年_____月_____日

备注：本授权书适用于具有法人资格的母公司授权无法人资格的分公司的情况，分公司参加投标必须提供本授权委托书，否则将不能

通过符合性筛选。

3.生产厂商授权书（参考格式）

江苏省省级行政机关政府采购中心：

作为设在_____（生产厂商地址）的制造/生产_____（产品名称）的 _____（生商厂商名称）在此以制造厂的名义授权_____（投标供应商名称和地址）用我厂制造的上述产品参加江苏省省级行政机关政府采购中心组织的采购编号为江苏省公安交管数据库安全审计监管平台项目的政府采购活动及后续的合同谈判和签署合同。

我们在此保证以投标（响应）合作人来约束自己，并为上述供应商就此次政府采购活动而提交的货物承担全部质量保证责任及按采购文件要求提供安装调试等售后服务。

我方于_____年____月____日签署本文，以此为证。

投标（响应）供应商名称：_____

出具授权书的生商厂商名称：_____

姓　　名：_____（生产厂商授权代表（签字或盖章））

职　　务：_____

公　　章：_____

日　　期：_____

备注：

（1）该授权书可由供应商所投产品的生产厂商或生产厂商直接授权的国内总经销商出具。

（2）如果供应商所投产品为进口产品，可由该产品在国内的有权经

销商出具授权，有权经销商包括该进口产品的国内经销商、地区总经销商及获得他们直接授权的经销商（该有权经销商须提供获得授权的证明材料）。

（3）授权出具单位如有内部格式授权书，可以按其格式出具，但必须包含上述格式文件的意思表达，特别是质量保证和提供售后服务。

（4）《生产厂商授权书》盖章必须为公章（见采购文件第一章第 3.7.2 条规定）。

（5） 如果为外文授权书须提供中文译文，同时提供中文译文和外文授权书内容相符的书面承诺。中标单位还须在签订合同前向采购人提供中文译文和外文授权书内容相符的公证文书。

4.资质要求材料格式

附表 1

声　明

我公司郑重声明：参加本次政府采购活动前 3 年（2012 年 5 月---2015 年 5 月）内，我公司在经营活动中没有因违法经营受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚。

投标供应商全称（公章）：

法定代表人（授权代表）签章：

日期：