采购项目要求

一、项目名称：

全市法院网络安全检查和培训（检查范围涉及全市一个中院、五个基层法院和三十二个人民法庭）

二、本次采购预算：

网络安全检查和培训：6 万元（陆万元整），超过采购预算的报价无效。

三、供应商参加本次采购活动应具备下列条件：

1、具有独立承担民事责任的能力；

2、具有良好的商业信誉和健全的财务会计制度；

3、具有履行合同所必需的设备和专业技术能力；

4、有依法缴纳税收和社会保障资金的良好记录；

5、参加政府采购活动前三年内，在经营活动中没有重大违法记录；

6、法律、行政法规规定的其他条件；

7、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；

8、根据项目特殊要求设置的特定条件；

9、具有《信息安全服务资质认证》证书、《信息安全管理体系认证》证书和《信息技术服务管理体系认证》证书。（投标时需提供证书复印件，加盖单位公章）

四、网络安全检查和培训要求

（一）网络安全检查内容

1、具体内容见附件 1:《网络安全检查内容》;可根据现场环境和实施检查工作公司经验增设检查项目；

（二）网络安全培训内容：

1、网络安全法和行业政策文件解读，信息安全道德规范，安全标准化概述；

2、结合此次网络安全检查，从网络架构、安全技术手段、核心业务等方面解读安全防护体系；

3、现场演示办公电脑、手机、测试服务器的网络安全事件；并结合此次检查发现的安全风险问题，进行演示。

（三）网络安全检查服务报告：

序号	成果名称	说明
1	全市法院网络安全检查报告	1、网络安全检查结果--将服务期间安全检查发现的数据进行汇总、整理与分析，总结存在的安全风险情况。 2、网络安全整改建议--依据总结的各种安全风险问题，逐一提供切实可行的整改建议。

（四）其他要求：

1、付款方式

提供《全市法院网络安全检查报告》并完成培训后，采

购方一次性支付费用。

2、服务期限

合同签订生效后 5 个工作日内提供网络安全检查服务，30 个工作日内完成网络安全检查服务并提供《全市法院网络安全检查报告》；网络安全检查服务完成节点以提供《全市法院网络安全检查报告》并完成培训为准，具体时间亦可跟采购方进行协商。

3、其他说明：

本次的采购预算已经包含了完成此次网络安全检查和培训工作的所有费用。

五、投标提供的材料：

1、需提供“统一社会信用代码营业执照”；未换证的提供 “营业执照、税务登记证、组织机构代码证或三证合一的营业执照”（需提供加盖单位公章的复印件）；

2、需提供《信息安全服务资质认证》证书、《信息安全管理体系认证》证书和《信息技术服务管理体系认证》证书（需提供加盖单位公章的复印件）；

3、加盖单位公章的《法定代表人/单位负责人授权书》、《承诺函》、《报价及承诺书》（《报价及承诺书》单独用信封封存）。

法定代表人/单位负责人授权书

内江市中级人民法院：

本授权声明：_____（单位名称），_____（法定代表人/单位负责人姓名、职务）授权_____（被授权人姓名、职务）为我方参加项目，采购活动的合法代表，以我方名义全权处理该项目有关磋商、报价、签订合同以及执行合同等一切事宜。

特此声明。

法定代表人/单位负责人（委托人）签字或者加盖个人名章：_____

授权代表签字：_____

供应商名称：_____（单位盖章）

日　　期：

注：法定代表人不亲自投标而委托代理人投标适用。

承诺函

内江市中级人民法院：

我公司作为本次采购项目的供应商，根据采购活动要求，现郑重承诺如下：

一、具备《中华人民共和国政府采购法》第二十二条第一款和本项目规定的条件：

（一）具有独立承担民事责任的能力；

（二）具有良好的商业信誉和健全的财务会计制度；

（三）具有履行合同所必需的设备和专业技术能力；

（四）有依法缴纳税收和社会保障资金的良好记录；

（五）参加政府采购活动前三年内，在经营活动中没有重大违法记录；

（六）法律、行政法规规定的其他条件；

（七）根据采购项目提出的特殊条件；

（八）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。

二、完全接受和满足本项目采购活动要求中规定的实质性要求，如对本次采购活动要求有异议，已经在递交响应文件截止时间届满前依法进行维权救济，不存在对采购活动要求文件有异议的同时又参加采购活动以求侥幸成交或者为实现其他非法目的的行为。

三、在参加本次采购活动中，不存在与单位负责人为同一人或者存在直接控股、管理关系的其他供应商参与同一合同项下的政府采购活动的行为。

四、在参加本次采购活动中，不存在和其他供应商在同一合同项下的采购项目中，同时委托同一个自然人、同一家庭的人员、同一单位的人员作为代理人的行为。

五、如果有《四川省政府采购当事人诚信管理办法》（川财采[2015]33 号）规定的记入诚信档案的失信行为，将在递交的文件中全面如实反映。

六、提供的任何资料和技术、服务、商务等响应承诺情况都是真实的、有效的、合法的。

本公司对上述承诺的内容事项真实性负责。如经查实上述承诺的内容事项存在虚假，我公司愿意接受以提供虚假材料谋取成交的法律责任。

供应商名称：（盖单位公章）

法定代表人/单位负责人或授权代表（签字或加盖个人名章）：

日　期：　　年　　月　　日

报价及承诺书

项目名称：_____

供应商名称：_____

报价（小写）：_____元

（大写）：_____元

其他承诺：_____

_____

_____

_____

_____。

供应商名称：（盖单位公章）

法定代表人/单位负责人或授权代表（签字或加盖个人名章）：

日　期：　　年　　月　　日

附件 1：

网络安全检查内容

一、物理环境检查：

序号	检查内容	检查结果	相关要求
1	机房出入专人随同，并鉴别和记录进入的人员；		查看进入登记记录 人民法庭是否登记技术人员维护记录
2	需进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围；		查看审批流程
3	应将主要设备放置在机房内		查看服务器是否都至于机房
4	应将设备或主要部件进行固定，并设置明显的不易除去的标记；		查看是否有设备固定和上机架规范情况
5	机房应设置灭火设备和火灾自动报警系统。		查看灭火类装置是否过期、是否通电
6	机房应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内。		查看机房温度、湿度是否控制得当
7	应提供短期的备用电力供应，至少满足主要设备在断电情况下的正常运行要求；		查看 UPS 负荷、备用电力系统是否有保障
8	机房的门禁系统类型，以及完备程度		记录门锁、门禁情况
9	内、外网设备是否做到一定的空间隔离		内、外网设备不能混合放置
10	设备是否都已做好标识		以设备的功用来划分和标识

二、网络架构检查：

序号	检查内容	检查结果	相关要求
1	网络架构合理性		是否满足网络高可用、可靠性要求
2	网络拓扑合理性		是否将重要网段部署在网络边界处且直接连接外部信息系统？重要网段与其他网段是否有可靠的技术隔离手段
3	网络设备性能和可管理性		网络设备性能是否满足业务要求？是否具备管理能力？

三、核心网络交换检查：

序号	检查内容	检查结果	相关要求
1	网络设备管理员密码强度		是否满足密码强度要求
2	网络设备密码所有人		谁掌握密码？
3	交换机的审计日志		查看本地日志 日志外发，查看外发日志情况以及留存时间
4	登陆源是否限制		查看是否有授信源限制，通过不同源 IP 尝试登陆或核验 ACL
5	交换机的密码强度，是否为默认密码或弱口令		核验密码强度
6	检查核心网络设备，查看是否有 vlan 划分配置，vlan 是否有命名以及互联对接描述		规范性

四、安全防御设备检查：

序号	检查内容	检查结果	相关要求
1	设备使用情况，是否加载有安全防护规则		防护规则颗粒度、防护规则细化程度、生效与否
2	安全设备的使用管理权限		谁掌握、谁有权限
3	安全设备的登陆维护密码是否为默认密码或弱口令		登陆核查
4	安全设备日志		是否有审计日志
5	安全设备设备接口流量与业务吻合度		安全设备是否在用，是否在合适的边界进行防护

五、安全审计设备检查：

序号	检查内容	检查结果	相关要求
1	审计内容		审计内容进行区分
2	审计策略		是否定期产生日志和报告
3	多权限分离		是否将配置管理员、系统管理员和审计员权限进行分离
4	审计记录留存		查看审计期限
5	审计告警		是否进行审计告警，对搞风险日志进行告警
6	审计颗粒度		审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

六、核心业务服务器安全检查（抽查三个核心业务服务器）

序号	检查内容	抽查三个核心业务服务器			检查要求
1	是否为弱口令				密码复杂度要求
2	是否安装有最新的补丁				linux 不在此列
3	是否定期修改密码				如果定期修改，上次修改时间
4	日志审计情况				外部审计或自身留存日志查看
5	是否有主机的防病毒能力				是否更新较新病毒库
6	远程维护情况				确认远程登录方式，远程桌面是否进行强化、SSH 登录是否进行源限制
7	账户审计				是否存在多个账户，账户状态和使用人情况，是否清理无用账户。
8	资源监控				是否对服务器资源进行定期巡检，或采用软件对资源进行实时监控
9	资源变更记录				资源环境变更记录

七、核心业务主机安全检查（抽查五个核心业务主机）

序号	检查内容	抽查五个核心业务主机					检查要求
1	是否开启共享功能						违规开启网络共享、打印机共享等功能
2	是否安装有最新的补丁						linux 不在此列
3	是否安装杀毒软件						是否更新较升级病毒库，电脑使用人员是否可自行关闭杀毒软件
4	是否有设备管理台账						对设备进行台账登记，设备分配到人
5	是否有违规外联情况						内网电脑违规连接互联网
6	是否有涉密文件						非涉密电脑禁止处理涉密文件
7	是否对移动介质进行管控						是否能使用移动介质，对移动介质是否授权使用

八、业务检查：

序号	检查内容	检查结果	相关要求
1	备份技术手段必须包含在线备份和离线备份		需要确认备份,抽查备份文件
2	对执行系统外挂小程序立即停用，并记录		记录是否使用，及细节

3	近期业务系统升级记录		查看电子或纸质记录材料
4	业务日志审计		业务系统自身用户日志留存情况检查，确认留存方式以及日志留存时间。

九、人民法庭其他检查项目（人民法庭增加的检查项目，人民法庭电脑抽检不少于 3 台）

序号	检查内容	检查结果	相关要求
1	网络布局的合理性		内、外网布局合理，设备放置分隔
2	法庭的设备维护记录		设备故障、处理结果、维护人员等相关信息的登记
3	办公电脑安全使用措施		外来人员是否可随意进出，使用到内网
4	是否开启共享功能		违规开启网络共享、打印机共享等功能
5	是否安装有最新的补丁		linux 不在此列
6	是否安装杀毒软件		是否更新较升级病毒库，电脑使用人员是否可自行关闭杀毒软件
7	是否有设备管理台账		对设备进行台账登记，设备分配到人（如果有基层法院统一建立，需在基层法院查看设备台账是否记录）
8	是否有违规外联情况		内网电脑违规连接互联网
9	是否有涉密文件		非涉密电脑禁止处理涉密文件
10	是否对移动介质进行管控		是否能使用移动介质，对移动介质是否授权使用

十、安全管理制度检查（访谈、核验）

检查问答内容	检查结果	备注
是否有专人负责信息安全？		什么科室、谁？
必须立即展开对内网业务系统及相关组件的密码修改		现场要求进行密码修改，并控制密码扩散范围
应将安全管理制度以某种方式发布到相关人员手中		以何种方式发放，过程记录
安全专职人员能否对安全状况有基本掌握，包括网络架、安全审计追溯手段是否了解。		如果有，回答简单的安全问题
信息负责部门，是否完全掌握最高权限		现场点，登陆核心系统
外聘运维人员及信息安全人员变动以及人员管理是否有管理方法和流程		现场问答
外聘人员管理制度和规范		查看相关制度和规范
应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训；		查看培训记录
应建立网络安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面作出规定；		查看相关规定
应提高所有用户的防病毒意识，告知及时升级防病毒软件，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查；		查看相关规范
应确认系统中要发生的重要变更，并制定相应的变更方案；		查看相关变更文档
应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、		查看应急预案

事后教育和培训等内容；		
应制定安全事件报告和处置管理制度，明确安全事件类型，规定安全事件的现场处理、事件报告和后期恢复的管理职责；		相关安全事件处置管理规定
单位人事管理岗位，负责人员录用、调岗、离岗等各环节审核。		
第三方运维人员管理，是否有合同、保密协议等相关规范对三方人员进行约束。		查看服务合同及保密协议