国家税务总局贵州省税务局数据中心基础资源设备（网络与安全设备）更新项目需求公示

一、投标人资格要求：

1.基本条件：

（1）满足《中华人民共和国政府采购法》第二十二条规定，并按照《政府采购法实施条例》第十七条要求提供下列材料：

①具有独立承担民事责任的能力：提供法人（企业法人、机关法人、事业单位法人和社会团体法人）或其他组织的营业执照或统一社会信用代码证书副本或复印件等证明文件，或自然人身份证明复印件。

②财务状况报告：具有良好的商业信誉和健全的财务会计制度：提供2020年度或2021年度经有资质的审计机构出具的审计报告（如为合并报表审计报告的，投标人须由并表单位出具的合并报表是否已包含投标人财务数据的证明或说明）；成立不足一年的公司须提供银行出具的资信证明。如果投标供应商提供财政部门认可的政府采购专业担保机构出具的投标担保函的，可不提供前述要求的审计报告。

③具有依法缴纳税收和社会保障资金的良好记录：提供有效的税款所属期及社会保障资金所属期分别为2022年任意一个月的税收和社会保障资金缴纳凭证（所属期税款为“0”而无缴纳凭证的，应有经税务机关盖章认可的零申报说明等证明）。

④具有履行合同所必须的设备和专业技术能力：投标人自行书面承诺或提供有关证明材料。

⑤参加本次政府采购活动前三年内，在经营活动中没有重大违法记录：提供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。

（2）法律、行政法规规定的其他条件：根据《财政部关于在政府采购活动中查询及使用信用记录有关问题的通知》（财库〔2016〕125号）规定，本项目投标人的信用记录作为供应商资格审查的重要依据。信用记录查询渠道由采购人通过‘信用中国’网站。（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）查询、记录和证据留存，与其他采购文件一并保存。查询截止时点为开标当天评审前。信用信息使用规则：由代理机构对供应商信用记录

进行甄别，对列入失信被执行人、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及其他不符合《中华人民共和国政府采购法》第二十二条规定条件的供应商，应当拒绝其参与政府采购活动。前述内容在采购文件明确。

⑥特殊条件：

本项目根据《财政部 工业和信息化部关于印发<政府采购促进中小企业发展管理办法>的通知》（财库〔2020〕46 号）第八条第一款第三项“要求获得采购合同的供应商将采购项目中的一定比例分包给一家或者多家中小企业”的规定，投标人须提供单独的承诺函承诺，如果投标人为大型企业，中标后必将本项目合同金额的 30%分包给一家或者多家中小企业，其中，分包给一家或者多家小微企业的比例不得少于前述 30%的 60%。

本项目采购标的对应的中小企业划分标准所属行业为软件与信息技术服务业。

二、本项目预算金额及采购方式：

1、总预算金额（万元）：859 万元；其中包括：基础资源设备 198.37 万元；网络运行设备 205.61 万元；信息安全设备 455.02 万元；

2、采购方式：公开招标；

三、实质性响应要求条款：

除法律、法规和规章规定外，招标文件中用“拒绝”“不接受”“无效”“不得”“必须”“应当”等文字规定或标注“★”符号的 条款为实质性要求条款(即重要条款)，对其中任何一条的偏离，在评标时将其视为无效投标。

四、无效投标的情形：

1、未在投标人须知前附表规定的提交时间、地点提交的；

2、有下列情形之一的，应在资格审查时按照无效投标处理：

(1)投标人未按照招标文件规定提交投标保证金的；

(2)投标人不具备招标文件规定的投标人资格条件的；

(3)报价超过招标文件中规定的预算金额或者最高限价的；

(4)投标人存在失信记录的。失信记录是指，通过“信用中国”网站(www.creditchina.gov.cn)、中国政府采购网(www.ccgp.gov.cn) 查询相关主体信用记录，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及其他不符合《政府采购法》第二十二条规定条件的情况。两个以上的自然人、法人或者其他组织组成一个联合体，以一个供应商的身份共同参加政府采购活动的，应当对所有联合体成员进行信用记录查询，联合体成员存在不良信用记录的，视同联合体存在不良信用记录。失信情况查询方式详见投招标文件。

3、有下列情形之一的，应在符合性审查时按照无效投标处理：

(1)投标文件未按照招标文件规定要求密封、签署、盖章的；

(2)不满足本招标文件中标注“★”的实质性条款要求的；

(3)投标有效期不足的；

(4)投标文件含有采购人不能接受的附加条件的；

(5)不符合法律、法规和招标文件规定的其他无效标情形的

五、采购标的

一、采购标的

（一）项目目标

当前，网络安全已经上升为国家战略，成为国家安全的重要组成部分。习近平总书记指出，没有网络安全就没有国家安全。2016 年 4 月 19 日，习近平总书记在网信工作座谈会上提出，要全面加强网络安全检查，摸清家底，认清风险，找出漏洞，通报结果，督促整改；要建立统一高效的网络安全风险报告机制、情报共享机制、研判处置机制，准确把握网络安全风险发生的规律、动向、趋势。2017 年 6 月 1 日，我国的网络安全法正式实施，《网络安全法》第二十一条规定，网络运营者应当按照网络安全等级保护制度的要求，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

根据《网络安全法》、等级保护 2.0 相关标准、《国家网络安全事件应急预案》等政策标准要求，贵州省税务局应配套建立常态化、长效化的新型安全技术运营和管理体系：通过技术、人员、流程三种手段，基于日常管理、隐患发现、应急指挥机制，以科学合理的方法实现最短时间内协调设备资源、人力资源、管理资源，对安全事件进行有效处置。实现统一的网络安全协同运营，保障省局网络安全防护持续有效，促进网络安全体系建设和队伍建设，在重保时期切实做好网络安全保障。

因此，根据《网络安全法》、等级保护 2.0 相关标准等法律法规和标准规范的要求，结合省局数据中心现状，通过本项目的建设，应能实现以下目标：

一、消除基础环境隐患，杜绝信息系统“带病”工作；

二、建立省局应急保障资源储备体系；

三、筑牢税收数据物理安全底线；

四、降低数据中心网络故障风险隐患，提升网络通信能力，提高网络稳定性、可靠性和

冗余性；

五、实现数据交互能力的提升，保障业务平稳运行。

（二）项目标的

序号	产品名称	数量	说明
1.	外联网接入 WEB 应用防护系统	2 台	开启 WEB 应用防护等功能。
2.	核心骨干防火墙	2 台	同时开启访问控制、WAF、IPS、防病毒、黑白名单等功能。
3.	业务隔离防火墙	4 台	同时开启访问控制、WAF、IPS、防病毒、黑白名单等功能。
4.	数据库防火墙	2 台	
5.	数据库脱敏系统	1 台	
6.	应用负载均衡	4 台	
7.	带外管理网核心交换机	2 台	主控引擎≥2 块。
8.	业务专网接入交换机	57 台	提供千兆电口 48 个、万兆光口 4 个。
9.	48 口全光万兆交换机	4 台	10GE 光口≥48 个，100GE 光口≥6 个。
10.	96 口存储交换机	4 台	配置 96 个 16Gb FC 端口，96 端口激活,提供不受限制的端口聚合功能，全光纤支持级联。
11.	存储交换机端光模块	120 个	支持 16GB（SFP+）接口传输速率。
12.			
13.			

二、需要满足的技术要求(实现本项目目标的所有技术要求，包括但不限于采购标的的功能和质量要求)

本项目采购的数据中心网络与安全设备及存储交换机设备主要包括外联网接入 WEB 应用防护系统、核心骨干防火墙、业务隔离防火墙、数据库防火墙、数据库脱敏系统、应用负载均衡、带外管理网核心交换机、业务专网接入交换机、48 口全光万兆交换机、96 口存储交换机及存储交换机端光模块等 11 项核心功能。其中，标记“★”号的为必备指标，无标识的为一般指标。证明材料需加盖公章，包括但不限于**有资质（行政主管部门认可，或者行业标准认可，或者国际标准认可）的第三方证明，或者所投产品制造商参数确认函，或者**官网截图等，证明材料需加盖投标人公章。详细需求如下

1. **外联网接入 WEB 应用防护系统（数量：2 台）**

序号	指标种类	指标名称	指标内容	是否需要证明材料
1	★	接口配置	配置不少于 8 个 10/100/1000M 以太网电口，不少于 8 个千兆光口 SFP，不少于 8 个万兆光口 SFP+，配置不少于 1 个 USB 口和 1 个 RJ45 串口，配置交流冗余电源。（均包括万兆多模光模块）	是
2	★	性能要求	网络层吞吐量≥70Gbps，应用层吞吐量≥35Gbps，并发连接数≥850 万，每秒新建连接数≥60 万。（提供厂商参数确认函）	是
3		流量检测	为解决数据非对称转发中出现的网络不通和安全检测失效问题，需支持主-主、主-备模式部署，需要支持在透明双主部署场景下，同一条流的所有数据包都能在同一台设备进行安全检测。	是
4		网络接口	为提高链路带宽和链路可靠性，需要支持链路聚合功能，可以将多条物理链路接口进行组合，成为一个性能更高的逻辑链路接口。	否
5		协议检测	内置对 SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP 等协议进行病毒防御的功能。	否
6		未知威胁检测	为解决未知威胁感知问题，产品需要支持未知威胁检测能力。	是
7	★	WEB 基础防护	为解决 WEB 应用防护问题，产品需要具备对常见 WEB 应用攻击防御功能：支持 SQL 注入攻击防护、XSS 攻击防护、WEB 应用扫描防护、爬虫防护、非法上传防护、非法下载防护、HTTP Flood 防护；对利用 WEB 服务器漏洞进行攻击的行为，能识别攻击行为并拒绝访问；提供相匹配的安全防护特征库，并能进行自动或手动升级。	是
8		WEB 防护拓展	为拓展 WEB 防护的能力，支持自定义 WEB 应用防护规则，通过基于正则表达式自定义规则匹配方向、动作、字符串、危险等级、攻击影响、描述等。	是
9		WEB 防护口令	为提高 WEB 口令防护能力，支持 WEB 弱口令检测、WEB 登录明文传输检测、WEB 口令爆破防护。	否
10		X-Forward-For 字段检测	针对攻击溯源场景，产品需要具备对报文头部的 X-Forward-For 字段检测功能，以方便防火墙对非法源 IP 进行溯源。	否
11		抗 CC 攻击	具备 CC 攻击防护功能。	否
12		预定义漏洞特征库	针对主机的异常外联行为，产品需要支持预定义漏洞特征库和自定义 IPS 规则。	否
13		态势感知联动	具备与态势感知平台联动功能，将防火墙产生的安全日志等数据上报至态势感知平台，并在态势感知平台进行威胁展示。	是

14	★	异构	为提升整体安全防护能力，外联网接入 WEB 应用防护系统应相对业务隔离防火墙采用异构厂商设备。	是
15		销售许可证	所投产品具备计算机信息系统安全专用产品销售许可证，提供有效证书复印件。	是

2. 核心骨干防火墙（数量：2 台）

序号	指标种类	指标名称	指标内容	是否需要证明材料
1	★	接口配置	配置不少于 6 个 10/100/1000M 以太网电口，不少于 8 个万兆光口 SFP+，配置不少于 1 个 USB 口和 1 个 RJ45 串口，配置交流冗余电源。（均包括万兆多模光模块）	是
2	★	性能要求	网络层吞吐量≥100Gbps，应用层吞吐量≥40Gbps，FW 吞吐量≥40Gbps，防病毒吞吐量≥20Gbps，IPS 吞吐量≥23Gbps，并发连接数≥3500 万，每秒新建连接数≥80 万。（提供厂商参数确认函）	是
3		流量检测	为解决数据非对称转发中出现的网络不通和安全检测失效问题，需支持主-主、主-备模式部署，需要支持在透明双主部署场景下，同一条流的所有数据包都能在同一台设备进行安全检测。	是
4	★	IPS 防护	具备入侵防护功能，支持规则库的分类组织和管理，包括：攻击手段/技术/流行度/危险度/服务类型；支持远程扫描、暴力破解、缓存区溢出、蠕虫病毒、木马后门、SQL 注入、跨站脚本等等检测和防护。	是
5		网络接口	为提高链路带宽和链路可靠性，需要支持链路聚合功能，可以将多条物理链路接口进行组合，成为一个性能更高的逻辑链路接口。	否
6	★	病毒检测与防护	产品支持病毒检测与防御功能，可以对多层压缩文件病毒进行检测与处置。	是
7		病毒库	支持不小于 500 万级的病毒库。	否
8		协议检测	产品内置对 SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP 等协议进行病毒防御的功能。	否
9		未知威胁检测	为解决未知威胁感知问题，产品需要支持未知威胁检测能力。	是
10	★	WEB 防护	为解决 web 应用防护问题,产品需要具备对常见 Web 应用攻击防御功能，如 XSS 跨站脚本、SQL 注入等类型。	是
11		X-Forward-For 字段检测	针对攻击溯源场景，产品需要具备对报文头部的 X-Forward-For 字段检测功能，以方便防火墙对非法源 IP 进行溯源。	否
12		抗 CC 攻击	具备 CC 攻击防护功能。	否

13		预定义漏洞特征库	针对主机的异常外联行为，产品需要支持预定义漏洞特征库和自定义 IPS 规则。	否
14		态势感知联动	具备与态势感知平台联动功能，将防火墙产生的安全日志等数据上报至态势感知平台，并在态势感知平台进行威胁展示。	是
15	★	异构	为提升整体安全防护能力，核心骨干防火墙应相对业务隔离防火墙采用异构厂商设备。	是
16		销售许可证	所投产品具备计算机信息系统安全专用产品销售许可证，提供有效证书复印件。	是

3. **业务隔离防火墙（数量：4 台）**

序号	指标种类	指标名称	指标内容	是否需要证明材料
1	★	接口配置	配置不少于 6 个 10/100/1000M 以太网电口，不少于 4 个万兆光口 SFP+，配置不少于 1 个 USB 口和 1 个 RJ45 串口，配置交流冗余电源。（均包括万兆多模光模块）	是
2	★	性能要求	网络层吞吐量≥70Gbps，应用层吞吐量≥35Gbps，FW 吞吐量 ≥30Gbps,防病毒吞吐量 ≥12Gbps，IPS 吞吐量≥12Gbps 并发连接数≥850 万，每秒新建连接数≥60 万。	是
3		流量检测	为解决数据非对称转发中出现的网络不通和安全检测失效问题，需支持主-主、主-备模式部署，需要支持在透明双主部署场景下，同一条流的所有数据包都能在同一台设备进行安全检测。	是
4		网络接口	为提高链路带宽和链路可靠性，需要支持链路聚合功能，可以将多条物理链路接口进行组合，成为一个性能更高的逻辑链路接口。	否
5	★	病毒检测与防护	产品支持病毒检测与防御功能，可以对多层压缩文件病毒进行检测与处置。	是
6		病毒库	支持不小于 500 万级的病毒库。	否
7		协议检测	产品内置对 SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP 等协议进行病毒防御的功能。	否
8		未知威胁检测	为解决未知威胁感知问题，产品需要支持未知威胁检测能力。	是
9	★	WEB 防护	为解决 web 应用防护问题,产品需要具备对常见 Web 应用攻击防御功能，如 XSS 跨站脚本、SQL 注入等类型。	是
10		X-Forward-For 字段检测	针对攻击溯源场景，产品需要具备对报文头部的 X-Forward-For 字段检测功能，以方便防火墙对非法源 IP 进行溯源。	否

11		抗 CC 攻击	具备 CC 攻击防护功能。	否
12		预定义漏洞特征库	针对主机的异常外联行为，产品需要支持预定义漏洞特征库和自定义 IPS 规则。	否
13	★	IPS 防护	具备入侵防护功能，支持规则库的分类组织和管理，包括：攻击手段/技术/流行度/危险度/服务类型；支持远程扫描、暴力破解、缓存区溢出、蠕虫病毒、木马后门、SQL 注入、跨站脚本等等检测和防护。	是
14		态势感知联动	具备与态势感知平台联动功能，将防火墙产生的安全日志等数据上报至态势感知平台，并在态势感知平台进行威胁展示。	是
15	★	异构	异构：为提升整体安全防护能力，业务隔离防火墙应相对核心骨干防火墙、外联网接入 WEB 应用防护系统采用异构厂商设备。	是
16		销售许可证	所投产品具备计算机信息系统安全专用产品销售许可证，提供有效证书复印件。	是

4. **数据库防火墙（2 台）**

序号	指标种类	指标名称	指标内容	是否需要证明材料
1		硬件参数	内存≥64G，存储空间≥24T，万兆光口≥4 个（含万兆多模光模块），双电源，机架式设备。	否
2		性能参数	数据库实例：≥300； 峰值 SQL 吞吐 40000 条语句/秒。	是
3		数据库类型	支持 ORACLE、MYSQL、SQLSERVER、RDS-Mysql、RDS-PG、PostgreSQL、GaussDB、DM、MongoDB、oceanbase 等主流数据库。	是
4		部署模式	支持透明代理、透明网桥、旁路模式、HA 主备模式。	是
5			支持当设备不可用时，自动启用 BYPASS 功能，避免因安全设备本身影响业务系统。	是
6		运行模式	支持学习、模拟、运行三种运行模式：学习模式支持 SQL 的自学习，识别安全 SQL。	是
7			支持在学习一定周期后，系统自动转激活运行，减少人工操作。	否
8		防护策略	内置数据库漏洞虚拟补丁不少于 1600 个，可阻止黑客通过这些漏洞进行攻击。	是
9			支持正常 SQL 特征及 SQL 注入特征双重防护，防止 SQL 注入攻击。	是
10			自动学习业务 SQL，捕获 SQL 语法，生成 SQL 白名单，通过 SQL 白名单进行访问控制。	是

11			支持透明代理模式下的可信 IP,将加入到可信 IP 列表中的可信的终端设备 IP 地址，终端设备与数据库通信的流量将会进行 bypass 处理，极大减少了经过数据库防火墙的流量，降低了数据库防火墙压力，保证设备稳定运行，提供更稳定的防护能力。	是
12			支持风险响应策略，针对不同信任度的身份和风险等级设置不同的响应行为（通过、告警、阻断行为、阻断连接）。	是
13			支持设置敏感标签身份，使之具备合法访问指定敏感数据的权限。未明确注册的身份，默认表示为不合法身份，不能访问任何敏感表格。	是
14			支持数据行数(阀值)进行精细管控，超出阀值的行为进行阻断或拦截，避免数据大量泄漏。	是
15			支持多维身份管理，至少支持应用程序名、IP 地址、主机名、操作系统账户、数据库账户、数据库实例名、时间、U 盾等因素的任意组合,形成新的登陆认证规则。	是
16			支持检测和审计密码猜测行为，通过设置密码猜测次数限制进行防护，当达到密码猜测限制时，锁定猜测终端，支持手工解锁。	是
17			支持数据库防漏扫，当特定的漏洞扫描器对数据库进行扫描时，实现防御拦截。	是
18		审计	支持 SQL 命令的细粒度审计和分析，并详细记录管理用户的行为信息，包括该语句执行的时间、机器名、用户名、IP 地址、MAC 地址、客户端程序名以及 SQL 语句等信息，对数据库操作进行审计，可对查询，新增，修改，删除等行为进行监控。	是
19			提供自动审阅，自动审阅过的审计信息，再次出现将不需要再行审阅，依赖于审计信息可以提取访问规则，把规则加入至访问及订阅规则库。	是
20		告警管理	支持多种安全响应措施，包括页面、邮件、短信方式进行告警。	否
21		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、支持双因子认证，支持短信认证、证书认证 2、支持系统安全配置如会话锁定、超时退出、密码复杂性管理等安全措施	是
22		安全运营	支持通过 syslog 的方式进行日志外发，支持审计、告警等日志外发。	是
23			支持以图形、列表等方式查看告警信息，以列表形式展现的告警信息应当包含告警时间、告警内容、告警等级、用户 IP、数据库代理 IP、事件等。	是
24		报表管理	支持登录事件、访问事件、风险事件、告警事件等报表的生成。	是

25			支持按日、周、月等时间周期生成综合报表。	否
26			报表支持以 wrod、PDF 等格式保存到本地。	否
27			支持报表调度，保障报表数据快速展示。	否
28			24 小时监控主流 SQL 注入攻击、数据库漏洞攻击、敏感访问、系统运行、流量等信息。	是
29		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》	是

5. 数据库脱敏系统（1 台）

序号	指标种类	指标名称	指标内容	是否需要证明材料
1		硬件参数	内存≥32G，固态硬盘≥128G SSD，存储硬盘≥3T，电口≥6 个，双电源，机架式设备。	否
2		易用性	系统基于 B/S 架构 web 管理模式，提供中文操作界面，无需安装任何客户端或者代理。支持 Linux、Windows、统信 UOS 等操作系统。	是
3		稳定性	脱敏系统平稳运行，满足高峰交易处理的需要，使用过程中不出现 crash，进行脱敏操作的过程中不需要频繁重启后台服务，脱敏操作对数据库(源库和目标库)影响小。	否
4		性能指标	单次脱敏数据量不小于 2T，且脱敏速度不小于 50M/s	否
5		数据源和目标	系统支持丰富的数据源和目标，数据源、目标配置通过系统界面实现： 1、支持 Oracle、Sql Server、Mysql、PostgreSQL、MariaDB、informix、人大金仓、达梦、Vertica 关系型数据库。 2、支持 MongoDB、南大通用 Gbase 8a/8t/8s 非关系型数据库脱敏； 3、支持 Teradata 等数据仓库脱敏。 4、支持直接读取 txt、csv、excel、xml、json 文件、oracle dump（exp/expdp）、mysql dump（sql 文件）文件进行脱敏。	是
6		脱敏方式	数据脱敏过程不落地，无需额外存储中间数据。	否
7			支持源库到目标库脱敏（包含支持同库脱敏）、数据库到文件脱敏、文件到文件脱敏（包括 FTP 和 SFTP 方式）、文件到数据库脱敏。	否
8			支持主流关系型数据库：Oracle、SQL Server、Mysql 数据库之间的异构脱敏。	是
9			支持增量脱敏方式，支持通过时间戳方式进行增量脱敏。支持数据库、文件的增量脱敏。	是
10			支持 Oracle 等数据库在脱敏时自定义选择目标表空间。	是

11		敏感信息发现	支持通过抽样的方式进行敏感数据发现，可自定义发现规则，系统内置的发现规则包括：中文姓名、英文姓名、姓名拼音、电话号码、邮箱、邮编、金额、日期、企业营业执照、组织机构代码证、银行卡号、军官证、港澳通行证、往来台湾通行证、护照、香港身份证、澳门身份证、税务登记证、身份证、组织机构名称、地址、IP 地址、社会统一信用代码等。	是
12			支持自动检测源数据库 DDL 的变动，识别增量的新数据表的敏感信息。	是
13			支持混合类型的敏感数据发现：一个字段多种敏感类型、一个数据单元内包含多种敏感类型。	是
14			支持针对单个字段手动设置敏感类型。	是
15		脱敏规则管理	可自定义增加脱敏规则，提供 SHA1 加密、MD5 加密、AES 加密、RSA 加密、随机映射、固定映射、替换、截断、截取，以及保留、取整、范围内浮动、比例内浮动等各种脱敏算法。	是
16			支持数据脱敏后保持原有数据特征、关联性、一致性。	否
17			支持依赖脱敏，可根据依赖字段的值对数据进行不同类型的脱敏处理。	否
18			支持对已脱敏的数据进行逆向脱敏查询，得到真实数据，便于用户校验数据的可使用性。。	否
19			支持组合脱敏，选择多个敏感类型形成组合，组合内所有敏感类型都存在时才进行脱敏。	是
20			支持自定义分段脱敏，可以通过配置位数，分隔符，指定位置，百分比位置，正则、脚本分段方式，对所有敏感类型进行自定义分段脱敏。	是
21		脱敏管理	系统自动检测源数据库 DDL 变动，自动同步变化的对象。	是
22			核心敏感数据可通过黑名单过滤，不脱敏或不迁移到目标端，提供独立管理页面。	是
23			支持对已发现敏感类型的数据重复、合并、筛选使用，无需进行敏感数据的再次发现。	否
24			支持表(包含分区表、簇表、索引组织表、队列表、压缩表、嵌套表)、主键、外键、索引（包含分区索引、位图索引、函数索引、压缩索引）、约束、视图、同义词、序列、队列、DBlink、自定义类型、存储过程、函数、触发器、包等数据库对象脱敏后在目标库中自动创建。	是
25			支持在脱敏前对脱敏结果进行预览，确定脱敏效果。	是
26			支持结构化数据库中根据分区表进行筛选脱敏模式。	是
27			快速脱敏：对于“临时性强、新增数量高”的脱敏需求，如数仓建设和数据分析。可通过上传规定的表格文件完成脱敏配置，自动完成敏感数据的发现并进行脱敏作业。	是

28		API 接口调用	支持第三方系统调用 API 脱敏接口对 JSON、XML 文本进行敏感数据脱敏。	否
29			支持作业调度 API，可通过 API 对于作业进行启动和终止操作，可通过该 API 查看作业当前的运行状态、处理的数据量、同步对象数量、处理进度、处理耗时等。	是
30			支持 Token、Accesskey 两种不同的 API 身份安全验证方式	是
31		作业管理	支持脱敏作业定时调度，可在指定时间自动运行；支持作业分段运行管理。	是
32			脱敏作业运行状态可视化展现，包含脱敏作业状态、效率（如：10000 行/s）、容量效率（如 300MB/s）、进度条、当前脱敏操作等监控指标；	是
33			有精细脱敏作业阶段，如对于库到库的脱敏至少包含预处理、数据库对象同步、脱敏数据同步、索引创建、约束启用等不同阶段。	否
34			支持对脱敏任务进行停止、启动、重启、审批，并且支持任务并发，充分利用系统资源，提高脱敏效率。。	是
35			可视化日志，所有日志可视化分类分级展现，方便作业的分析和复盘。	是
36			支持对脱敏作业的预演，在长时间作业前，完成各类检查，包含权限检查，空间检查。字符集检查，硬件性能检查	是
37		授权和审核	完善的授权体系，可对数据源中的库、表或者脱敏作业，进行单独或批量授权给单用户或用户组。	是
38			拥有脱敏作业审核流功能，针对单独脱敏作业，可配置专人审核后方可运行。	是
39		资质要求	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》	是

6. 应用负载均衡（4台）

序号	指标种类	指标名称	指标内容	是否需要证明材料
1		接口配置	配置不少于 4 个 10/100/1000M 以太网电口，不不少于 4 个万兆光口 SFP+，配置不少于 1 个 USB 口和 1 个 RJ45 串口，配置交流冗余电源。（均包括万兆多模光模块）	是
2		性能要求	4 层吞吐量不少于 27.5Gbps，7 层吞吐量不少于 20Gbps，四层并发连接数不少于 3800 万，七层并发连接数不少于 750 万，四层新建连接数 CPS 不少于 100 万，七层新建连接数 RPS 不少于 150 万。（提供厂商参数确认函）	是

3		负载均衡算法	为适应不同业务的调度需求，支持轮询、加权轮询、按主机加权轮询、加权最小连接、最快响应、加权最小流量、加权源 IP 哈希、带宽比例、哈希、优先级等算法。	是
4		可视展示	为观测设备和业务情况，支持展示：新建连接数、并发连接数、吞吐情况、业务的健康状态，上下行流量、每秒请求数，节点池的调度算法、CPU 温度、CPU 和内存占用率等；	是
5		健康检查	支持第 4 层 ARP 到第 7 层应用层协议检测，支持可定制的基于应用层的健康检查方式。	是
6		SSL 卸载	支持 SSL 卸载功能。	否
7		日志记录	支持将日志发送到外部的 Syslog 服务器。支持累积存储和查询 6 个月内日志，方便回溯查询。	否
8		IPv6	需支持 IPv6，支持双栈模式，支持 NAT46、NAT64、NAT66、FTP ALG、DNS64 等协议转换。	是
9		安全加密	为加强连接安全，支持 cookie 加密，提升 cookie 安全性。	是
10		节点保障	支持优先级算法下最少可用节点保障，优先级高的节点故障时会自动进行选举，保证优先级高节点的可用性。	否
11		传输优化	为保障访问体验，支持图片优化技术，提升 web 页面加载速度。	否
12		冗余部署	支持双机热备部署方式，可自动同步配置并提供连接会话的镜像功能，实现无缝故障切换。	是
13		销售许可证	所投产品具备计算机信息系统安全专用产品销售许可证，提供有效证书复印件。	是

7. 带外管理网核心交换机（2台）

序号	指标种类	指标名称	指标内容	是否需要证明材料
1		接口配置	支持千兆电口，千兆光口，万兆光口，25G 端口、40G 端口、100G 端口；	是
2	★	性能要求	1. ★设备采用 CLOS 架构,业务模块插槽数≥10 个，主控引擎槽数≥2 个,交换网板槽位数≥4，主控引擎与交换网板物理分离；	是
3	★		2. ★交换容量≥600Tbps，包转发率≥140000Mpps（提供官网网址与截图作为证明文件并加盖制造厂商鲜章）；	
4			3. 支持 RIP、OSPF、ISIS、BGP 等 IPv4 动态路由协议，支持 RIPng、OSPFv3、ISISv6、BGP4+等 IPv6 动态路由协议；	
5			4. 支持跨设备链路聚合，支持多虚 1 技术；	

6			5. 支持基于硬件信任根的安全启动，防止交换机的主控、线卡、交换网板在启动阶段被入侵（提供官网网址与截图作为证明文件并加盖制造厂商公章）；	
7			6.支持流量可视化功能,提供第三方测试报告并加盖原厂商公章；	
8			7. 支持 HQoS 功能,（提供官网网址与截图作为证明文件并加盖制造厂商公章）；	
9			8.支持 VXLAN，能够实现 VXLAN 二三层互通；	
10			9.支持 IPv4/IPv6 硬件 BFD,最小时间间隔小于 4ms，提供第三方测试报告并加盖原厂商公章；	
11			10.支持命令行接口（CLI），Telnet，Console 口进行配置；支持 SNMPv1/v2/v3；	
12			11.支持基于 ACL 和 UCL 的访问控制，提供权威第三方测试报告；	
13	★		12.★支持内置智能图形化管理功能，能够实现通过图形化界面设备配置及命令一键下发和版本智能升级（提供官网网址与截图作为证明文件并加盖制造厂商公章）；	
14			13.提供工信部入网许可证复印件；	
15	★		14. ★每台配置 2 块主控板、4 电源，4 风扇，2 块独立监控网板，4 块独立交换网板，48 个千兆电口、2*96 个万兆光口（含 2*96 个万兆多模光模块），24*100G 光口（自适应 40G）（含 8 个 100G 多模光模块，8 个 40G 多模光模块）。	

8. 业务专网接入交换机（57台）

序号	指标种类	指标名称	指标内容	是否需要证明材料
1		接口配置	整机提供 48 个千兆电口，10GE 光接口 4 个。	是
2	★	性能要求	1.★交换容量≥430Gbps，包转发率≥160Mpps；	是
3			2. 支持 SNMP、Telnet、RMON、SSH；	
4	★		3.★支持基于端口的 VLAN（4K 个），支持基于协议的 VLAN，支持基于 MAC 的 VLAN；	
5			4.支持 VxLAN 功能，支持 BGP EVPN，支持分布式 Anycast 网关，支持 VxLAN 的自动化部署，提供权威第三方测试报告；	
6	★		5.★支持 IPv4 静态路由、RIP V1/V2、OSPF，支持 IPv6 静态路由、RIPng；	
7			6.支持安全启动，通过安全 CPU、一次性可编程存储器等安全措施，从可信硬件锚开始，启动过程中每一步进行验证，确保每一阶段运行程序是可信	

			的，提供权威第三方测试报告。	
8			7.支持通过标准以太端口进行堆叠，单一 IP 管理；	
9			8.支持 CPU 保护功能，能限制非法报文对 CPU 的攻击，保护交换机在各种环境下稳定工作；	
10			9.内置智能管理功能,支持通过 web 图形化界面管理设备；	
11	★		10.★每台配置双电源，双风扇，4 个 10GE 多模光模块；	

9. 48口全光万兆交换机（4台）

序号	指标种类	指标名称	指标内容	是否需要证明材料
1		接口配置	整机提供 10GE 光口端口数量≥48 个，100 GE 光接口≥6 个；	是
2	★	性能要求	1. ★交换容量≥4.8Tbps，包转发率≥2000Mpps；	是
3	★		2. ★支持前后风道、后前风道，支持双电源，≥4 风扇框；	
4			3. 支持基于端口、基于协议、基于 MAC 的 VLAN；	
5			4.支持硬件 BFD，最小时间间隔小于 4ms，提供第三方测试报告并加盖原厂商公章；	
6			5. 支持 RIP、OSPF、ISIS、BGP 等 IPv4 动态路由协议，支持 RIPng、OSPFv3、ISISv6、BGP4+等 IPv6 动态路由协议；	
7			6.支持流量可视化功能,提供第三方测试报告并加盖原厂商公章；	
8	★		7. ★支持 MCE、MPLS、MPLS VPN（提供官网网址与截图作为证明文件并加盖制造厂商公章）；	
9			8.支持 AI ECN：识别流量模型，动态调节 ECN 门限，提供第三方截图证明；	
10			9. 支持二层、三层 Vxlan 网关和 BGP EVPN 特性；	
11			10. 支持 SNMP、Telnet、RMON、SSH，支持端口镜像 ERSPAN；	
12			11. 提供入网许可证复印件；	
13	★		12. ★48 个万兆多模光模块,6 个 100G 多模光模块；	

10. 96口存储交换机（4台）

序号	指标种类	指标项	指标内容	是否需要证明材料
1	★	架构要求	采用无拥塞的背板架构，可在线热插拔 ；能够支持市场主流存储设备，需能与我局现有 SAN 网络在网设备无缝兼容（我局现有设备主要为：中科曙光 6510,H3C 6600B，华为 SNS3096 等）；支持 SNMP 、Telnet、Web 管理 / GUI 界面，双电源；	是
2	★	主板要求	采用最新型号的存储 SAN 交换机主板；	是
3	★	端口配置	每台 SAN 交换机配置 96 个 16Gb FC 端口，96 端口激活,提供不受限制的端口聚合功能，全光纤支持级联；	是
4		强弱电线材	配备连接到 220V 16A 标准 PDU 的电源线材;提供与光纤端口相同类型和数量的多模万兆光纤跳线（LC-LC），长度小于 15 米;电口网络跳线为超 5 类以上成品线；	是
5	★	其他要求	需提供至少 6 年原厂质保服务（包含上门技术支持服务）； 若所投产品若为贴牌生产或定牌生产等委托代工产品，需提供该设备原始设计制造商一致性说明。	是

11. 96口存储交换机端光模块（120个）

序号	指标种类	指标项	指标内容	是否需要证明材料
1	★	传输速率	支持最高 16GB（SFP+）接口传输速率；	是
2	★	其他要求	需适用于我局现有 SAN 存储光纤交换机（我局现有设备主要为：中科曙光 6510,H3C 6600B，华为 SNS3096 等）；	是

（一）采购标的的性能要求（针对货物类项目）：

1.中标供应商所提供的系统、软件，如需经国家有关部门登记、备案、审批或许可的，中标供应商应当保证已经完成上述手续，并准备接受采购人的检查。

2.采购人在验收中如发现中标供应商提供的产品功能、质量、技术参数不符合合同规定的内容，有权全部退换货或部分退换货，拒付不符合合同规定部分的货款。中标供应商须在采购人提出退换货要求后 3 日内向采购人提供符合采购人质量要求的产品，中标供应商应对由退、换货引发的损失承担全部赔偿责任。

（二）采购标的的材料要求（针对货物类项目）：

1.在本项目采购范围内的软、硬件产品，投标人需提供完整的授权，不得存在产权或商业纠纷。如有第三方软件、工具或服务的，其产品和服务价格一并计入投标总价。

2.中标供应商保证对在合同执行中提供、使用的来自第三方的技术、软件等知识产权，

具有合法的所有权或使用权，不会侵犯第三方的合法权利。

3.本项目要求投标人所使用的产品必须基于成熟、适配良好的产品或技术，不得以实验室产品、测试产品等投标。

4.中标供应商交付的产品不能含有任何可以自动终止或者妨碍其他系统正常运行的功能。

（三）采购标的结构要求（针对货物类项目）：/

（四）采购标的外观要求（针对货物类项目）：

中标供应商所提供的软件产品均为正常渠道获取的正版产品，硬件产品必须是原厂发货全新未拆封设备。

（五）采购标的的安全要求

中标人在未经过采购人书面批准的情况下，不得将任何采购人认为涉及数据安全的观点、数据、系统结构信息、测试结论以及测试记录传播、披露和使用。未经采购人同意，中标人不得擅自修改任何程序和数据。

中标供应商所提供的硬件、软件，如需经国家有关部门登记、备案、审批或许可的，中标供应商应当保证已经完成上述手续，并准备接受采购人的检查。

（六）采购标的的服务内容

重点保障服务。中标人应在“两会”、“国庆”等重大活动期间提供重点保障服务，提高响应速度和服务质量。对关键系统中存在的设备、系统软件及应用软件的多厂商问题，在发生系统故障及问题时，协调相关厂商进行分析并加以解决。

（七）采购标的的服务标准

1.人员要求

中标人应为本项目组建一个项目实施团队，至少包括项目经理1 名、多名实施人员，在重大网络安全保障期间提供现场技术支持服务。

2.服务机构要求

本项目的实施范围主要包含贵州省税务局数据中心的关键网络、安全及存储设备等。因此，对于实施产品的安装、维护和技术支持提出了更高的要求，为了更好的满足售后服务和技术支持的要求。本项目的技术支持和服务需要满足以下要求：

（1） 中标供应商保障在保修期内由于产品本身质量原因造成的任何损伤和损坏，中标供应商在接到通知后 2 小时内响应到场，24 小时内完成维修或更换，并承担修理调换的费用。

（2） 中标供应商须在贵州省内具备一定数量的售后服务人员，能提供免费咨询服务和长期技术支持。

（3）中标供应商中标后应每月一次定期巡检，处理相关问题并出巡检报告，协助招标人做好运维工作。

（4）质保期满后系统出现故障，中标供应商应本着对项目负责的态度尽快解决相关问题，费用由双方另行协商解决。

3. 项目验收

项目验收工作由采购方按照相关规定组织开展，中标方配合完成。

（1）验收方式及时间

软、硬件到货安装结束后，验收由采购人现场组织，中标供应商配合进行。

（2）验收标准

执行 ISO20000 运维服务规范、《国家税务总局贵州省税务局信息系统运维规范》，建立可靠的运维保障体系；严格遵守我局安全和保密规定，以及招标文件明确的各项服务质量及具体技术指标要求、中标供应商投标文件及承诺。（属采购人不宜公开的标准、规范等在中标后由采购人提供）

验收争议事项解决：依据采购文件及响应文件及其合同约定解决，采购文件及响应文件及其合同未约定的，双方友好协商解决仍有争议的，提交有资质的第三方鉴定。采购人履约验收部门不得无故拖延验收，超过规定时限未验收或未提交相关书面意见的，视同验收合格；成交供应商不配合验收、或者对采购人的验收异议未积极响应处理的，视同违约，依法承担列入失信人名录等法律责任。

（3）验收内容及提供的资料

包括但不限于以下内容：

*工作记录；

*软件、设备到货单；

*软件、设备安装配置、补丁升级的实施方案、实施报告；

*操作手册；

*系统巡检报告；

*甲方要求的其他与项目相关的资料和文档；

*总体验收报告。

（4）验收时供需双方均须派人参加，必要时可外聘专家，共同完成验收。

（八）采购标的其它技术要求

1. 保密要求

（1）投标人及参与项目的所有人员应严格遵守招标人的保密要求，签订保密协议和保密承诺书，并由投标人担保。

（2）投标人对于招标人提供的资料，以及本项目实施过程中所涉及的所有文档、数据、介质和相关信息保密，未经许可，不得以任何形式向第三方传播。保密期限不受本项目期限的限制，在本项目履行完毕后，保密信息接受方仍应承担保密义务。

（3）投标人应对参与项目的所有人员进行背景调查，并由投标人担保。

（4）如因投标人一方的原因造成泄密，招标人将保留追究其法律责任的权利。

2. 知识转移要求

知识转移的目标是投标人要采取有效方法、途径保证招标人能顺利完成本项目实施过程中各阶段移交物的接收及技术知识的吸收和转移，确保招标人能够掌握该项目的核心技术。

招标人不单独对知识转移支付费用。

中标人应将项目相关的所有报告、材料、过程文件全部交接给国家税务总局贵州省税务

局，不得有所保留。

3.知识产权要求

（1）项目交付过程中所产生的所有技术成果（包括相关技术资料、设备安装配置文档等）归招标人所有。享有永久使用权、复制权和修改权。除本项目工作所需外，未经招标人书面同意，投标人不得擅自使用、复制招标人的数据信息、文档及其他资料。

（2）投标人应保证在本项目中所有预装和为本项目安装的软件为在中国境内具有合法版权或使用权的正版软件且无质量瑕疵。

（3）投标人应保证其所提供的产品及服务不侵犯第三方的知识产权，否则，由此给招标人造成的一切损失由投标人承担。对本项目内由投标人采购的第三方工具软件，投标人需承诺无知识产权纠纷。

4.项目归档要求

项目归档的资料都应为简体中文（专用技术配置除外），且清楚明了，且应按照采购人要求进行编码归档。

5.费用要求

本项目涉及的各项费用，如实施服务、售后技术支持服务等，在项目实施过程中，招标人不再支付项目实施有关的任何费用。涉及项目实施所需的费用，未在投标文件中指明的，投标人必须考虑周全并承担相关费用。

三、、需要满足的商务要求（实现本项目目标的所有技术要求，包括但不限于取得采购标的时间、地点、财务和服务要求）

（一）采购人取得采购标的时间（期限）：

合同签订后30日内软件、设备到货安装。

采购人取得采购标的地点（范围）：

实施地点：国家税务总局贵州省税务局

（二）**本项目的付款进度和方式：**在合同中约定付款进度和方式。

（三）采购标的所需的包装和运输：/

（四）采购标的所需的售后服务：设备及软件安装调试验收合格之日起5年（其中96口存储交换机质保期限为6年，数据库防火墙、数据库脱敏系统硬件质保和特征库升级期限3年）。

（五）采购标的所需的保险：不涉及

（六）采购标的的其它商务要求：无

九、评标办法及定标原则

根据《政府采购货物和服务招标投标管理办法》（财政部 2017 年第 87 号令）规定,本项目采用综合评分法，具体评分表如下：

注：投标人提供的佐证资料模糊不清晰的，视同未提供。

评审因素		分值	考核内容
投标报价（最后报价）（30分）		30	投标报价得分=(评标基准价 / 投标报价)×30 1. 评标基准价，指满足招标文件要求且投标报价最低，其报价分为满分。 2.评标过程中，不得去掉报价中的最高报价和最低报价。因落实政府采购政策进行价格调整的，以调整后的价格计算评标基准价和投标报价。 3.评标委员会只对资格性检查和符合性审查合格的投标文件进行价格评审。超过项目预算的投标报价按无效投标处理。
履约能力（26 分）	相关证书	17	1.投标人同时具有有效的 ISO 9001 质量管理体系、ISO 27000 信息安全管理体系、ISO 20000 服务管理体系、ISO 45001 职业健康安全管理体系、ISO14001 环境管理体系认证证书得 1 分，没有或不提供不得分。 2.投标人具有安全工程类信息安全服务资质证书，得 1 分，没有或不提供不得分，没有或不提供不得分。 3.投标人具有信息系统安全集成服务二级或以上资质证书得 2 分，投标人具有信息系统安全集成服务三级资质证书得 1 分，没有或不提供不得分。 4.投标人具有信息系统安全运维服务二级或以上资质证书得 2 分，投标人具有信息系统安全运维服务三级资质证书得 1 分，没有或不提供不得分。 6.投标人具有信息安全应急处理服务二级或以上资质证书得 2 分，投标人具有信息安全应急处理服务三级资质证书得 1 分，没有或不提供不得分。 7.投标人具有二级或以上信息技术服务运行维护标准符合性证书-ITSS 资质证书得 2 分,资质等级为三级得 1 分,资质等级为四级得 0.5 分,没有或不提供不得分。 8.投标人具有连续 10 年省级“重合同守信用”证书得 2 分，没有或不提供不得分。 9.所投核心交换机的 CPU、网络处理器、交换芯片等关键芯片为自研芯片，并提供第三方测试报告材料并

			加盖原厂商公章得 4 分，不提供不得分。 10.所投业务隔离防火墙具有中国信息安全测评中心颁发的信息技术产品安全测评证书（EAL4+）和《自主原创产品测评证书》，得 1 分，没有或不提供不得分。 （提供上述证书复印件并加盖投标人公章）
	成功案例	4	投标人提供 2019 年 1 月 1 日以来网络设备、存储设备、安全设备类业绩的，每提供一份有效业绩得 0.5 分，最多得 4 分。 （提供上述案例证明材料复印件并加盖投标人公章，提供的证明材料复印件至少包括首页、项目内容、签章页等相关内容，否则不得分）。
	技术力量	5	根据本项目组建实施团队。 1.投标人针对本项目组建的项目团队中，应指定一名固定项目经理，该人员须具备有效的 PMP、信息系统项目管理师证书，每个证书得 0.5 分，最多 1 分，没有或不提供不得分。 2.成员中至少 1 人同时具有中国信息安全测评中心颁发的 CISP 证书、CISAW 证书、NISP 证书，每个证书得 0.5 分，最多得 1 分，没有或不提供不得分。 3.成员中至少 1 人同时具有 Oracle 数据库的 OCM、DM 数据库的 DCA 认证证书，得 1 分，没有或不提供不得分。 4.成员中具有 CCIE、HCIE、H3CIE、网络规划设计师证书，每个证书得 0.5 分，最多得 1 分，没有或不提供不得分。 5.根据本项目售后服务的具体需要，本项目的售后服务管理人员每 1 人具备 ITSS 认证证书得 0.5 分，最多 1 分，没有或不提供不得分。 投标人须提供以上专业人员的资质证书复印件及由投标人为该人员缴纳的 2022 年以来连续近 6 个月的社保证明及劳动合同复印件并加盖投标人公章，未提供不得分。
技术或者服务水平（42 分）	项目服务方案	10	1.项目组织方案 投标人须全面、准确理解项目需求，针对项目技术要求提供有效的组织方案，内容全面、具有较强的可操作性，得 2 分； 组织方案基本合理，对需求的把握基本到位，具有基本的可操作性，得 1 分；组织方案不合理，对需求把握不到位，可操作性较差，得 0 分。

			2.项目实施方案 投标人须提供全面、合理、可行的集成实施方案，方案切实可行、条理清晰的得 2 分；方案基本可行、条理基本清晰的得 1 分；方案不具体、条理不清晰和不提供，得 0 分。 3.运行保障方案 投标人须全面、准确理解项目需求，针对项目运行保障要求提供内容全面的、完整和适用的方案，内容全面、具有较强的保障性，得 2 分；运行方案基本合理，对需求的把握基本到位，具有基本的保障性，得 1 分；方案不完整、不合理，得 0 分。 4.售后服务方案 投标人须提供全面、合理、可行的售后服务方案，方案切实可行、条理清晰的得 2 分；方案基本可行、条理基本清晰的得 1 分；方案不具体、条理不清晰和不提供，得 0 分。 5.应急保障方案 投标人须根据项目要求，针对项目过程中可能出现的紧急情况，提供全面、完整的应急方案。方案具有全面性、合理性、可行性的得 2 分；方案基本全面、合理、可行的得 1 分；方案不可行、不清晰，得 0 分
	产品指标	32	投标人提供的设备、软件功能指标全部满足非“★”项的得共 32 分，不满足一项扣 8 分。扣完为止。
落实政府采购政策（2 分）		2	1.促进中小企业发展：本项目非专门面向符合条件的中小企业采购，对符合条件的中小微企业给予 3%的价格扣除优惠。 2.技术创新：提供行政主管部门颁发的技术创新类有效证书，给予 1 分的加分。 3.少数民族及少数民族地区政策性加分：对原产地在少数民族自治区和享受少数民族自治待遇的省份的投标主产品(不含附带产品)，且投标主产品不得低于本采购项目预算金额 50%的，得 1 分。
总分		100	

注：符合条件的中小企业指依据《财政部 工业和信息化部关于印发<政府采购促进中小企业发展管理办法>的通知》（财库〔2020〕46 号）第十一条规定，在投标文件中出具《中小企业声明函》；符合条件的监狱企业指依据《财政部 司法部关于政府采购支持监狱企业发展有关问题的通知》（财库〔2014〕68 号）规定，在投标文件中出具由省级以上监狱管理局、戒毒管理局（含新疆建设兵团）出具的属于监狱企业的证明文件；符合条件的残疾人福利企

业指依据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购 政策的通知》（财库〔2017〕141 号）规定，在投标文件中出具《残疾人福利性单位声明函》。

十、评审委员会组成

评审委员会组成

本项目评标委员会：评审专家 5 人。专家在开标前 1 天由需求部门推荐专业类型，经政府采购领导小组办公室主任审核并报经政府采购领导小组组长签字确定后，在开标当天由代理机构提交贵州省公共资源交易中心按规定在省综合评标专家库内随机抽取。

十一、公示期：3 个工作日

十二、意见的反馈的方式

联系人：周小雁

电子邮箱：18985005099@189.cn

电话：0851-86906036；18985005099；