政府采购项目

项 目 编 号：HWDL2025013

2025年大荔县网络安全检查技术服务项目

竞争性磋商文件

采　　购　人：中国共产党大荔县委员会宣传部

采购代理机构：华文项目管理有限公司

日　　期：2025年5月

目 录

第一章 竞争性磋商公告

项目概况

中国共产党大荔县委员会宣传部2025年大荔县网络安全检查技术服务项目采购项目的潜在供应商应在大荔县西城街道办学门前17号获取采购文件，并于 2025年05月22日 10时00分 （北京时间）前提交响应文件。

一、项目基本情况

项目编号：HWDL2025013

项目名称：中国共产党大荔县委员会宣传部2025年大荔县网络安全检查技术服务项目

采购方式：竞争性磋商

预算金额：255,200.00元

采购需求：

合同包1(2025年大荔县网络安全检查技术服务项目):

合同包预算金额：255,200.00元

合同包最高限价：255,200.00元

品目号	品目名称	采购标的	数量（单位）	技术规格、参数及要求	品目预算(元)	最高限价(元)
1-1	其他信息技术服务	2025年大荔县网络安全检查技术服务项目	1(项)	详见采购文件	255,200.00	255,200.00

本合同包不接受联合体投标

合同履行期限：15日历天

二、申请人的资格要求：

1.满足《中华人民共和国政府采购法》第二十二条规定;

2.落实政府采购政策需满足的资格要求：

合同包1(2025年大荔县网络安全检查技术服务项目)落实政府采购政策需满足的资格要求如下:

（1）《节能产品政府采购实施意见》（财库[2004] 185号）；

（2）《环境标志产品政府采购实施的意见》（财库[2006]90号）；

（3）《国务院办公厅关于建立政府强制采购节能产品制度的通知》（国办发〔2007〕51号）；

（4）《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）；

（5）《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）；

（6）陕西省财政厅关于印发《陕西省中小企业政府采购信用融资办法》（陕财办采〔2018〕23号）；

（7）《财政部 发展改革委 生态环境部 市场监管总局关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9号）；

（8）《关于印发环境标志产品政府采购品目清单的通知》（财库〔2019〕18号）；（9）《关于印发节能产品政府采购品目清单的通知》（财库〔2019〕19号）；

（10）《陕西省财政厅关于加快推进我省中小企业政府采购信用融资工作的通知》（陕财办采〔2020〕15号）；

（11）《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）；

（12）《财政部 农业农村部 国家乡村振兴局关于运用政府采购政策支持乡村产业振兴的通知》（财库〔2021〕19号）；

（13）其他需要落实的政府采购政策。

如有最新颁布的政府采购政策，按最新的文件执行。

3.本项目的特定资格要求：

合同包1(2025年大荔县网络安全检查技术服务项目)特定资格要求如下:

（1）法定代表人（负责人）参与磋商时需提供法定代表人（负责人）身份证明书及法定代表人（负责人）身份证；被授权人参与磋商时需提供法定代表人（负责人）授权委托书及被授权人身份证；

（2）供应商不得为“信用中国”网站（www.creditchina.gov.cn ）中列入失信被执行人和重大税收失信主体的供应商，不得为中国政府采购网（www.ccgp.gov.cn)政府采购严重违法失信行为记录名单中被财政部门禁止参加政府采购活动的供应商；

（3）单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得同时参加同一合同项下的政府采购活动。

三、获取采购文件

时间： 2025年05月12日 至 2025年05月16日 ，每天上午 08:00:00 至 12:00:00 ，下午 14:00:00 至 18:00:00 （北京时间）

途径：大荔县西城街道办学门前17号

方式：现场获取

售价： 500元

四、响应文件提交

截止时间： 2025年05月22日 10时00分00秒 （北京时间）

地点：大荔县阳光路北段8号黄色楼响丁当三楼会议室

五、开启

时间： 2025年05月22日 10时00分00秒 （北京时间）

地点：大荔县阳光路北段8号黄色楼响丁当三楼会议室

六、公告期限

自本公告发布之日起3个工作日。

七、其他补充事宜

1.获取采购文件时，请携带有效的单位授权委托书（附法定代表人及被授权人身份证复印件）、被授权人身份证；

2.请供应商按照陕西省财政厅关于政府采购供应商注册登记有关事项通知中的要求，通过陕西省政府采购网（http://www.ccgp-shaanxi.gov.cn/）注册登记加入陕西省政府采购供应商库；

3.因“中国共产党大荔县委员会宣传部”无陕西省政府采购网账号，需借用“中共大荔县委办公室”账号发布项目信息。本项目实际采购人为“中国共产党大荔县委员会宣传部”。

八、对本次招标提出询问，请按以下方式联系。

1.采购人信息

名称：中共大荔县委办公室

地址：大荔县司令部街

联系方式：18992359529

2.采购代理机构信息

名称：华文项目管理有限公司

地址：大荔县西城街道办学门前17号

联系方式：19991683602

3.项目联系方式

项目联系人：宋宁

电话：19991683602

华文项目管理有限公司

2025年05月11日

采购更正公告（第一次）

一、项目基本情况

原公告的采购项目编号：HWDL2025013

原公告的采购项目名称：中国共产党大荔县委员会宣传部2025年大荔县网络安全检查技术服务项目

首次公告日期：2025年05月11日

二、更正信息：

更正事项：采购公告

更正原因：

其他原因

更正内容：

原公告的响应文件提交截止时间：2025-05-22 10:00:00，更正为：2025-05-26 15:00:00。

原公告的开启时间：2025-05-22 10:00:00，更正为：2025-05-26 15:00:00。

其他内容不变

更正日期：2025年05月15日

三、其他补充事项

1.获取采购文件时，请携带有效的单位授权委托书（附法定代表人及被授权人身份证复印件）、被授权人身份证；

2.请供应商按照陕西省财政厅关于政府采购供应商注册登记有关事项通知中的要求，通过陕西省政府采购网（http://www.ccgp-shaanxi.gov.cn/）注册登记加入陕西省政府采购供应商库；

3.因“中国共产党大荔县委员会宣传部”无陕西省政府采购网账号，需借用“中共大荔县委办公室”账号发布项目信息。本项目实际采购人为“中国共产党大荔县委员会宣传部”。

四、凡对本次公告内容提出询问，请按以下方式联系。

1.采购人信息

名称：中共大荔县委办公室

地址：大荔县司令部街

联系方式：18992359529

2.采购代理机构信息

名称：华文项目管理有限公司

地址：大荔县西城街道办学门前17号

联系方式：19991683602

3.项目联系方式

项目联系人：宋宁

电话：19991683602

华文项目管理有限公司

2025年05月15日

第二章 竞争性磋商须知

一、供应商须知前附表

项号	内 容	说明及要求
1	项目名称	2025年大荔县网络安全检查技术服务项目
2	标段名称	2025年大荔县网络安全检查技术服务项目
3	采购内容	根据陕西省网络安全检查相关文件要求，对大荔县党政机关、企事业单位的重要互联网应用系统(含网站)采用信息收集、远程监测、人工渗透等技术手段进行安全检查，结合各单位实际安全现状，编写技术报告。
4	服务地点	大荔县
5	采购人	中国共产党大荔县委员会宣传部
6	采购人联系方式	18992359529
7	磋商内容	2025年大荔县网络安全检查技术服务项目**采购范围内的全部内容**（具体要求详见磋商文件第五章采购内容及要求）。
8	服务期限	15日历天
9	质量标准	达到合格标准及第五章“采购内容及要求”。
10	资金来源及落实情况	财政资金，已落实
11	**最高限价**	**¥255200.00元（大写：人民币贰拾伍万伍仟贰佰元整）** **备注：各供应商磋商报价不能超过最高限价，否则按无效磋商处理。**
12	**开标现场监标人核验原件**	**法定代表人参与磋商时需提供法定代表人身份证明书及本人身份证原件；被授权人参与磋商时需提供法定代表人授权委托书及本人身份证原件。** **注：1.供应商会议现场手持法定代表人授权委托书或法人身份证明书。**

		2.供应商凭法定代表人身份证明书或授权委托书及身份证原件提交磋商响应文件，未携带法定代表人身份证明书或授权委托书及身份证原件，代理机构拒绝接收其磋商响应文件。
13	供应商资格要求	**（一）供应商基本资格要求：满足《中华人民共和国政府采购法》第二十二条规定，需提供以下证明资料：** 1.供应商应具有独立承担民事责任的能力且具备向采购人提供相关服务的企业法人、事业法人、其他组织或者自然人，企业法人应提供统一社会信用代码的营业执照；事业法人应提供统一社会信用代码的事业单位法人证；其他组织应提供合法证明文件；自然人应提供身份证明文件； 2.具有良好的商业信誉和健全的财务会计制度以及有依法缴纳税收和社会保障资金的良好记录； **①财务状况报告：**提供具有财务审计资质单位出具的2023年或2024年度财务审计报告（成立时间至磋商时间不足一年的可提供成立后任意时段的资产负债表）或响应文件递交截止时间前六个月内其基本账户银行出具的资信证明（附基本账户证明）或政府采购信用担保机构出具的磋商担保函； **②税收缴纳证明：**提供响应文件递交截止时间前一年内任意一个月的缴费凭据（依法免税的供应商应提供相关文件证明）； **③社会保障资金缴纳证明：**提供响应文件递交截止时间前一年内任意一个月的社保缴费凭据或社保机构开具的社会保险参保缴费情况证明（依法不需要缴纳社会保障资金的供应商应提供相关证明）； 3.提供具有履行本合同所必需的设备和专业技术能力的说明或承诺（格式自拟，加盖供应商公章）； 4.提供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的书面声明（格式自拟，加盖供应商公章）。

		（二）供应商特定资格要求，需提供以下资格证明资料： （1）法定代表人（负责人）参与磋商时需提供法定代表人（负责人）身份证明书及法定代表人（负责人）身份证；被授权人参与磋商时需提供法定代表人（负责人）授权委托书及被授权人身份证； （2）供应商不得为“信用中国”网站（www.creditchina.gov.cn ）中列入失信被执行人和重大税收失信主体的供应商，不得为中国政府采购网（www.ccgp.gov.cn ）政府采购严重违法失信行为记录名单中被财政部门禁止参加政府采购活动的供应商； （3）单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得同时参加同一合同项下的政府采购活动。 **备注：以上资格证明文件供应商必须完全提供(除注明原件外，均为扫描件并加盖供应商公章)并胶装在磋商响应文件中，一项不合格即按照无效投标处理(注:按照陕西省财政厅关于政府采购领域贯彻落实《陕西省优化营商环境三年行动计划(2021-2023年)》的通知(陕财办采(2021)31号)文件对供应商参与政府采购活动建立“承诺+信用管理”的准入管理制度要求，以上①②③内容若提供承诺函，可根据本磋商文件格式（格式详见 附件一）要求出具承诺函，成交单位的承诺函随同成交结果-并公示。**
14	磋商有效期	90日历天（从递交竞争性磋商响应文件的截止之日起）
15	磋商保证金	**本项目不收取磋商保证金**
16	响应文件份数	“正本”：1份，“副本”：2份，“电子文档”：U盘1份（WORD版文件），每份文件须清楚地标明“正本”、“副本”。若正本与副本不符，以正本为准。 **注：为了节约成本，鼓励各供应商双面打印本项目竞争性磋商响应文件。**
17	**响应文件递交截止时间及响应文**	**时 间：2025年05月26日15时00分前** **地 点：大荔县阳光路北段8号黄色楼响丁当三楼会议室**

	件递交地点	
18	**磋商开启时间及地点**	**时 间：2025年05月26日15时00分** **地 点：大荔县阳光路北段8号黄色楼响丁当三楼会议室**
19	评标方法及标准	综合评分法，详见评审标准
20	磋商轮次	2轮（响应文件中的报价为第一轮报价） 最后一轮报价时间：磋商中通知 备注：在磋商过程中，磋商小组认为还需再次磋商时，通知各供应商进行再次磋商，若供应商拒绝再次磋商，则该供应商的二次报价即为其最终报价。
21	**付款方式**	**合同签订后付款70%，履约验收合格后付款至100%。**
22	招标代理服务费	按照《国家发展改革委关于进一步放开建设项目专业服务价格的通知》（发改价格〔2015〕299号）的要求，参照计价格〔2002〕1980号、发改价格〔2011〕534号文件的计费标准，以中标（成交）价为基数计算，按照标准收取。**由成交供应商在领取成交通知书前一次性向招标代理机构支付。** **交款账户：** **账户名称：华文项目管理有限公司渭南分公司** **账户号码：61050164900800001082** **开户银行：中国建设银行股份有限公司渭南分行营业部**
23	现场踏勘	不组织
24	合同要求	1）响应供应商接受竞争性磋商文件规定的风险划分原则，未提出新的风险划分办法； 2）响应供应商未增加发包人的责任范围，也未减少响应供应商义务； 3）响应供应商未提出不同的服务验收、计量、支付办法； 4）响应供应商未对合同纠纷、事故处理办法提出异议； 5）响应供应商在磋商过程中没有欺诈行为； 6）响应供应商对合同条款没有重要保留。

25	**是否专门面向中小企业采购**	**否，本项目非专门面向中小企业采购** **本项目所属行业：软件和信息技术服务业**
26	其他未尽事宜	按照《中华人民共和国政府采购法》及相关法律法规执行。

二、供应商须知

（一）总则

1、本项目采用竞争性磋商方式

2、名词解释

（1）采购人：中国共产党大荔县委员会宣传部

（2）采购代理机构：华文项目管理有限公司

（3）监督部门：大荔县财政局

（4）供应商：是指响应和符合竞争性磋商文件规定资格条件要求的单位。

3、磋商费用：供应商应自行承担所有与参加本次磋商有关的费用。不论磋商的结果如何，代理机构和采购人在任何情况下均无义务和责任承担这些费用。

4、适用法律：本次采购活动及由本次采购产生的合同受中华人民共和国相关法律法规的制约和保护。

5、竞争性磋商文件的约束力：供应商一旦获取了本竞争性磋商文件并参加磋商，即被认为接受了本竞争性磋商文件中的所有条件和规定。

6、法定代表人为同一个人的两个及两个以上法人，母公司、全资子公司及其控股公司，都不得同时参加本项目同一合同下的磋商。

7、供应商应认真阅读竞争性磋商文件中所有的章节、条款、格式、规范和附件等要求。如果没有按照竞争性磋商文件要求编制竞争性磋商响应文件及提供

相关资料，其风险由供应商自行承担。

8、供应商所提供的所有资料（包括复印件）必须清晰，如因提供的资料难以辨认，其风险由供应商自负。

9、本次采购不接受联合体磋商。

10、分包

不允许。

11、偏离

详见供应商须知前附表。

12、代理机构对采购人拖欠成交人合同款不承担任何连带或非连带的责任，任何情况下，成交人若主张或要求其合同款相关的民事权利均只能直接针对采购人主张或要求。

13、因本次政府采购活动产生的一切纠纷（包括合同纠纷），有关各方应友好协商解决，协商不成，则向大荔县仲裁委员会申请仲裁。

14、招标代理服务费：

按照《国家发展改革委关于进一步放开建设项目专业服务价格的通知》（发改价格〔2015〕299号)的要求，参照计价格〔2002〕1980号、发改价格〔2011〕534号文件的计费标准，以中标（成交）价为基数计算，按照标准收取。

由成交供应商在领取成交通知书前一次性支付招标代理费。

15、本竞争性磋商文件的解释权属采购代理机构。

（二）竞争性磋商文件的澄清、补充及修改

1、竞争性磋商文件包括下列内容：

第一章　竞争性磋商公告

第二章　竞争性磋商须知

第三章　磋商办法

第四章　合同主要条款

第五章　采购内容及要求

第六章　磋商响应文件格式

2、采购人或者采购代理机构对已发出的竞争性磋商文件如果进行澄清或修改（澄清或者修改的内容可能影响竞争性磋商响应文件编制的），必须在响应文件递交截止时间至少5日前以书面形式通知所有获取竞争性磋商文件的潜在供应商，不足5日的，采购人或者采购代理机构应当顺延递交竞争性磋商响应文件的截止时间。

3、任何要求对竞争性磋商文件进行澄清的供应商，均应按竞争性磋商文件中的通讯地址以书面形式（盖供应商公章）递交到代理机构（购买磋商文件地址）和采购单位，应在响应文件递交截止时间3日前提出。代理机构或采购人应收到异议之日起3日内将以书面形式作出答复，同时将书面答复发给每个购买竞争性磋商文件的供应商，但不说明问题的来源。

4、如果上述答复涉及对竞争性磋商文件的修改或补充，则它将被视为竞争性磋商文件的一部分。凡原先所发竞争性磋商文件中的内容与答复中的内容不一致之处，应按照后形成的书面答复为准。

5、对竞争性磋商文件的修改是竞争性磋商文件的组成部分，将以书面形式通知所有购买竞争性磋商文件的供应商，并对其具有约束力。供应商在收到上述通知后，应毫不延误地以书面形式向代理机构确认；无论供应商是否及时地以书面形式向代理机构确认，代理机构都将依据发出信函、传真的相关凭据或电话记录等认定供应商已经收到上述通知。

6、为使供应商有充分时间对竞争性磋商文件的修改部分进行研究或由于其他原因，可以延长响应文件递交截止日期和磋商会议日期、改变磋商会议地点，并以书面形式通知供应商。

7、供应商任何疑问，都必须在磋商会议前5天前提出，否则，不接受针对竞争性磋商文件提出的质疑和投诉。

（三）竞争性磋商响应文件的组成及编制

1、竞争性磋商响应文件组成部分

（1）磋商申请函

（2）报价表

（3）法定代表人身份证明书

（4）法定代表人授权委托书

（5）技术方案

（6）本项目拟投入人员汇总表

（7）业绩

（8）供应商资格证明文件

（9）供应商承诺书

（10）政府采购供应商拒绝政府采购领域商业贿赂承诺书

（11）中小企业声明函

（12）残疾人福利性单位声明函（如有）

（13）监狱企业相关资格证明材料（如有）

2、竞争性磋商响应文件必须使用简体中文，竞争性磋商响应文件中若有英文或其他语言文字的资料，应翻译成中文。

3、度量衡单位除竞争性磋商文件技术规格中另有规定外均采用中华人民共和国法定的计量单位。

4、竞争性磋商响应文件应以A4规格的纸张打印。

5、供应商应将竞争性磋商响应文件装订成册，并编排目录、标明连续页码。

6、竞争性磋商响应文件应按照竞争性磋商文件给出的竞争性磋商响应文件格式按顺序编制。

（四）磋商报价

1、磋商报价以人民币报价，供应商在填写磋商报价时，金额单位要统一，数字、文字要清晰。

2、总磋商报价等于各分项报价与各项费用之和，不得采用总价下浮的方式。

3、采购最高限价

最高限价：¥255200.00元（大写：人民币贰拾伍万伍仟贰佰元整）；

供应商报价大于磋商最高限价，作为不实质性响应竞争性磋商文件，均为无效报价，按无效磋商处理。

4、供应商报价中不得包含竞争性磋商文件要求以外的内容，否则，在评标时不予核减，但在授予合同时，采购人有权将这部分价格从其成交价格中扣除。

5、总报价中不得缺漏竞争性磋商文件所要求的内容，否则，评标时将有效磋商文件中该项内容的最高价计入其评标总价，但在授予合同时，缺漏项目的报价视作已含在其他项目的报价中，这些项目将作为免费赠送而包含在合同内。

（五）磋商保证金

1、磋商保证金：**本项目不收取磋商保证金**

2、供应商须在文件递交截止时间前向采购代理机构交纳磋商保证金（以到账时间为准），交纳时请注明标段名称（可简写）。

3、各供应商应按磋商文件规定的金额递交保证金，并作为其响应文件的组成部分。

4、保证金应为人民币，可采用下列任何一种形式支付：

转账、电汇、保函、支票、汇票、本票等。

①转账或者电汇形式提交的保证金应当从供应商基本账户按规定向磋商文件指定的账户提交保证金；

②以保函形式缴纳保证金的，必须是陕西省财政厅认定的具有开具保函资格的单位开具的保函或商业银行保函。（供应商须在递交响应文件时将保证金保函原件提交采购代理机构进行查验）；

5、凡没有随附保证金交纳凭证的响应文件，视为非响应性磋商，其响应文件无效。

6、未成交单位的保证金，在成交通知书发出后五个工作日内退还；成交单位的保证金，在合同签订后五个工作日内无息退还。**（合同签订后三个工作日内，须向采购代理机构提供一份合同原件，以便及时退还保证金）**

7、供应商以保函形式交纳的，保函退还时间参照上述（6）条款。

因供应商自身原因导致未及时退还的，由供应商自行负责。

有下列情形之一的，磋商保证金不予退还：

1）供应商在递交响应文件截止时间后撤回响应文件的；

2）供应商在响应文件中提供虚假材料的；

3）除因不可抗力或磋商文件认可的情形以外，成交供应商不与采购人签订

合同的；

4）供应商与采购人、其他供应商或者采购代理机构恶意串通的；

5）磋商文件规定的其他情形。

（六）磋商有效期

1、磋商有效期见本须知前附表第13项所规定的期限，在此期限内，凡符合本竞争性磋商文件要求的磋商响应文件均保持有效。

2、在特殊情况下，采购人在原定磋商有效期内，可以根据需要以书面形式向供应商提出延长磋商有效期的要求，对此要求供应商须以书面形式予以答复。供应商可以拒绝采购人这种要求，而不被没收磋商保证金。同意延长磋商有效期的供应商既不能要求也不允许修改其磋商响应文件，但需要相应的延长磋商保证金的有效期，在延长的磋商有效期内，本须知第五项关于磋商保证金的退还与没收的规定仍然适用。

（七）竞争性磋商响应文件的正本和副本要求

1、供应商应按照要求，准备正本1 份，副本2份，电子文件U盘1份（WORD版文件），每份竞争性磋商响应文件须清楚地标明“正本”或“副本”字样。一旦正本和副本不符，以正本为准。

2、竞争性磋商响应文件的正本按照要求签署和盖章后，副本可以是是正本的扫描件，但正本和副本的内容必须相同。否则，磋商小组误读误评的风险供应商必须自行承担。

3、竞争性磋商响应文件不论是书写、打印或复制，均应做到清晰、整洁、规范。

（八）竞争性磋商响应文件的签署、盖章

1、在竞争性磋商文件给出的竞争性磋商响应文件格式中，凡是标明由供应商盖章的地方，竞争性磋商响应文件都必须加盖供应商统一对外的公章，凡是标明由法定代表人或委托代理人签字或盖章的，签署姓名全称或加盖私章。竞争性磋商响应文件封套上有明确规定的必须由法定代表人或委托代理人签字或盖章。

2、竞争性磋商响应文件不得行间插字、涂改或增删。如有修改错漏处，必须由供应商的法定代表人或其委托代理人签字或盖章并加盖供应商公章。

（九）竞争性磋商响应文件的密封

1、供应商应将竞争性磋商响应文件正本、副本标明“正本”、“副本”的字样，正副本分开密封包装，不论供应商成交与否，竞争性磋商响应文件均不退回。

①封套上注明标段名称、项目编号、供应商名称、“正本”或“副本”，法定代表人或委托代理人签字或盖章，并加盖单位公章，“于XX年XX月XX日XX时前不得开启”字样。

②竞争性磋商响应文件密封要求：电子文件U盘1份（WORD版文件），密封在竞争性磋商响应文件正本内，正本、副本（一起包封）分开密封。

2、如果封袋（盒）未按上述要求密封、加写标记或标注不清，采购人对误投或过早启封概不负责。未按上述规定提交的竞争性磋商响应文件，一切后果由供应商负责。

（十）竞争性磋商响应文件的递交

1、供应商应在规定的时间和地点递交竞争性磋商响应文件。

2、代理机构将拒绝迟交的竞争性磋商响应文件并原封退回。

3、未按规定进行密封的竞争性磋商响应文件，代理机构将拒绝接受。

4、供应商在递交竞争性磋商响应文件后，如果有修改和撤回要求，必须以书面形式通知代理机构名称，使代理机构能在响应文件递交截止时间前收到。其修改书或撤回通知书,应由法定代表人或其委托代理人签署,并在信封上注明“修改”或“撤回”字样。

5、在磋商有效期内，供应商不得撤回竞争性磋商响应文件。

（十一）磋商会议

1、在磋商文件规定的时间和地点，由采购代理机构组织磋商工作，供应商须委派代表参加，签名报到以证明其出席。

2、由监标人查验供应商代表的资格。（身份证及法定代表人授权委托书或法人身份证明书）

3、由供应商代表与监标人共同检查响应文件的密封情况，经检查无误后，签字确认。

4、采购代理机构工作人员按照顺序，将各供应商首次响应文件的份数等内容公布。

5、由采购人对供应商资格进行审查。

6、将响应文件送至专家室进行评审。

7、采购代理机构工作人员对供应商磋商报价等内容进行记录，并由监标人签字确认。

8、磋商过程由采购代理机构指定专人记录。

第三章 磋商办法

（一）磋商小组职责及义务

1、磋商小组组成：由采购人代表和评审专家共3人组成，其中评审专家人数2人，专家名单由有关人员在财政部门设立的政府采购评审专家库中抽取。

2、磋商小组职责

（1）确认磋商文件；

（2）确定符合资质条件的供应商参加磋商；

（3）审查供应商的响应文件并做出评价；

（4）要求供应商解释或者澄清其响应文件；

（5）编写评审报告。

（6）告知采购人或采购代理机构在评审过程中发现供应商违法违规行为。

3、磋商小组义务

（1）遵纪守法、客观、公正、廉洁地履行职责；

（2）根据磋商文件的规定独立进行评审，对个人的评审意见承担法律责任；

（3）参与评审报告的起草；

（4）配合采购人、采购代理机构答复供应商提出的质疑；

（5）配合财政部门的投诉处理和监督检查工作。

（6）确认磋商文件：磋商小组对磋商文件进行审阅，无异议进行签字确认；有异议进行修改，修改内容经采购人确认后，磋商小组以书面形式通知所有供应商。

（二）磋商方法及程序

1、磋商方法：综合评分法。

响应文件满足磋商文件全部实质性要求且按照评审因素的量化指标评审得分最高的供应商为成交候选人。

2、磋商程序：磋商的全过程分为不公布第一次磋商报价，供应商符合性及有效性，磋商过程，磋商承诺，最终报价，综合评审等阶段。

（1）第一次报价：记录各供应商的响应文件中的报价、服务期等内容，报价不公开。

（2）供应商符合性及有效性：按照采购文件中的要求对各供应商提供的竞争性磋商响应文件进行符合性及有效性审查，对于没有按采购文件要求的供应商，不进入下一步评审程序。

（3）磋商过程

磋商小组在符合性及有效性评审的基础上对各供应商的响应文件认真阅读，并对报价、商务、技术等内容进行一对一的磋商。各供应商就磋商中的技术、商务、价格等内容按要求进行补充、完善、澄清、承诺，但补充完善的内容必须在其授权范围内。磋商小组以补充、完善后的内容作为评审的依据。

（4）各供应商对磋商小组在磋商过程中的问题予以澄清说明，做出承诺，同时对报价及构成再次进行成本分析、核算，并在此基础上进行二次报价。

（5）磋商小组对各供应商磋商内容进行确认，进行二次报价，二次报价超过一次报价的，为无效报价，按无效文件处理。

A、在对所有供应商进行有效性、完整性、符合性审查时，通过必要的澄清，从质量和技术、服务均能满足磋商文件实质性响应要求的基础上，筛选出合格供应商。不合格供应商的响应文件按无效处理，磋商小组要告知有关供应商。

B、磋商小组给予所有合格供应商一次最后报价的机会。供应商要以书面形式提交最后报价(各合格供应商的最后报价将作为综合评分法中价格分的计算依据，并由其法定代表人或被授权人签字或盖章。已提交响应文件的供应商，在提交最后报价之前，可以根据磋商情况以书面形式退出磋商。

（6）磋商小组以磋商响应文件、磋商承诺内容、最终报价为依据，按照评审办法，推荐成交候选人。

（7）磋商文件的实质性变更

A、在磋商过程中，磋商小组可以根据磋商文件和磋商情况实质性变动采购需求中的技术、服务要求以及合同草案条款，但不得变动磋商文件中的其他内容。实质性变动的内容，须经采购人代表确认。

B、对磋商文件作出的实质性变动是磋商文件的有效组成部分，磋商小组将及时以书面形式同时通知所有参加磋商的供应商。

C、供应商应当按照磋商文件的变动情况和磋商小组的要求重新提交响应文件，并由其法定代表人或授权代表签字或者加盖公章。

3、在磋商过程中，磋商小组可以根据磋商文件和磋商情况实质性变动采购需求中的技术、服务要求以及合同草案条款，但不得变动磋商文件中的其他内容。实质性变动的内容，须经采购人代表确认。对磋商文件作出的实质性变动是磋商文件的有效组成部分，磋商小组应当及时以书面形式同时通知所有参加磋商的供应商。供应商应当按照磋商文件的变动情况和磋商小组的要求重新递交响应文件，并由其法定代表人或被授权委托人签字或盖章。

4、磋商文件能够详细列明采购标的的技术、服务要求的，磋商结束后，磋商小组将要求所有实质性响应的供应商在规定时间内递交最后报价。磋商文件不

能详细列明采购标的的技术、服务要求，需经磋商由供应商提供最终设计方案或解决方案的，磋商结束后磋商小组按照少数服从多数的原则投票推荐3家以上供应商的设计方案或解决方案，并要求其在规定时间内递交最后报价。最后报价是供应商响应文件的有效组成部分。

5、已递交磋商响应文件的供应商，在递交最后报价之前，可以根据磋商情况退出磋商。采购人、采购代理机构将退还退出磋商的供应商的磋商保证金。

6、经磋商确定最终采购需求和递交最后报价的供应商后，由磋商小组采用综合评分法对递交最后报价的供应商的磋商响应文件和最后报价进行综合评分。综合评分法，是指响应文件满足磋商文件全部实质性要求且按评审因素的量化指标评审得分最高的供应商为成交候选供应商的评审方法。

7、评审时，磋商小组各成员独立对每个有效磋商响应的文件进行评价、打分，然后汇总每个供应商每项评分因素的得分。

8、磋商小组应当根据综合评分情况，按照评审得分由高到低顺序推荐3名成交候选供应商，并编写评审报告。评审得分相同的，按照最后报价由低到高的顺序推荐。评审得分且最后报价相同的，按照技术指标优劣顺序推荐。

9、除资格性检查认定错误、分值汇总计算错误、分项评分超出评分标准范围、客观分评分不一致、经磋商小组一致认定评分畸高畸低的情形外，采购人或采购代理机构不得以任何理由组织重新评审。

10、终止磋商活动条款

出现下列情形之一的，将终止竞争性磋商采购活动，发布项目终止公告并说明原因，重新开展采购活动：

（1）因情况变化，不再符合规定的竞争性磋商采购方式适用情形的；

（2）出现影响采购公正的违法、违规行为的；

（3）除《政府采购竞争性磋商采购方式管理暂行办法》第二十一条第三款规定的情形外，在采购过程中符合要求的供应商或者报价未超过最高限价的供应商不足3家的；

（4）采购人或采购代理机构发现磋商小组未按照磋商文件规定的评审标准进行评审的，应当重新开展采购活动，并同时书面报告本级财政部门。

11、政策性扣减

（1）本项目为非专门面向小微企业采购的采购项目，采购标的对应的中小企业划分标准所属行业为：其他未列明行业。

服务采购项目，对符合价格扣除条件的小微企业报价给予15%的扣除，用扣除后的价格参加评审

在政府采购活动中，供应商提供的货物、工程或者服务符合下列情形的，享受中小企业扶持政策：

在货物采购项目中，货物由中小企业制造，即货物由中小企业生产且使用该中小企业商号或者注册商标；在工程采购项目中，工程由中小企业承建，即工程施工单位为中小企业；在服务采购项目中，服务由中小企业承接，即提供服务的人员为中小企业依照《中华人民共和国劳动民法典》订立劳动合同的从业人员。

在货物采购项目中，供应商提供的货物既有中小企业制造货物，也有大型企业制造货物的，不享受本办法规定的中小企业扶持政策。以联合体形式参加政府采购活动，联合体各方均为中小企业的，联合体视同中小企业。其中，联合体各方均为小微企业的，联合体视同小微企业。

中小企业参加政府采购活动，应当出具符合财库〔2020〕46号规定的《中小企业声明函》，否则按无效磋商处理。

（2）监狱企业参加政府采购活动时，应当提供相关证明文件。监狱企业参加政府采购活动时，视同小微企业。

（3）符合条件的残疾人福利性单位在参加政府采购活动时，应当提供《残疾人福利性单位声明函》，并对声明的真实性负责。残疾人福利性单位参加政府

采购活动时，视同中小企业；残疾人福利性单位属于小微企业的，不重复享受政策。

12、信用担保

陕西省政府采购信用担保及信用融资政策

（1）为支持和促进中小企业发展，进一步发挥政府采购政策功能作用，有效缓解中小企业融资难等问题，根据财政部财库【2011】124号文件的精神，陕西省财政厅制订了《陕西省政府采购信用担保试点工作实施方案（试行）》，为参与陕西省政府采购项目的供应商提供政府采购信用担保，并按照程序确定了合作的担保机构。供应商在缴纳投标保证金时可自愿选择通过担保机构保函的形式缴纳；中标供应商如果需要融资贷款服务的，可凭中标通知书、政府采购合同等相关资料，按照文件规定的程序申请办理，具体规定可登陆陕西省政府采购网(www.ccgp-shaanxi.gov.cn/）重要通知专栏中查询了解。

（2）政府采购信用融资政策详见附件“温馨提示”。

（三）评审

磋商评审的全过程分为供应商资格审查，响应文件符合性审查，磋商过程，最终报价及综合评审等阶段。

1、供应商资格审查：由采购人对供应商资格进行审查，按照法律法规及磋商文件第二章“供应商须知前附表”所述资格要求进行资格审查，以确认供应商是否具备相应资格。有一项因素不符合审查标准的，供应商不能通过资格审查，其磋商无效。**有关资格证明材料的证书、证件原件备查。**

（一）供应商基本资格条件：满足《中华人民共和国政府采购法》第二十二条规定，需提供以下证明资料：

序号	审查内容	审查标准
1	营业执照等证明文件	合法有效，具有独立承担民事责任的能力且具备向采购人提供相关服务企业法人、事业单位、其他组织或者自然人。
2	具有良好的商业信誉和健全的财务会计制度以及有依法缴纳税收和社会保障资金的良好记录	**①财务状况报告：**提供具有财务审计资质单位出具的2023年或2024年度财务审计报告（成立时间至磋商时间不足一年的可提供成立后任意时段的资产负债表）或响应文件递交截止时间前六个月内其基本账户银行出具的资信证明（附基本账户证明）或政府采购信用担保机构出具的磋商担保函； **②税收缴纳证明：**提供响应文件递交截止时间前一年内任意一个月的缴费凭据（依法免税的供应商应提供相关文件证明）； **③社会保障资金缴纳证明：**提供响应文件递交截止时间前一年内任意一个月的社保缴费凭据或社保机构开具的社会保险参保缴费情况证明（依法不需要缴纳社会保障资金的供应商应提供相关证明）；
3	具有履行合同的声明	提供具有履行本合同所必需的设备和专业技术能力的说明或承诺；（格式自拟，加盖供应商公章）
4	无重大违法记录书面声明	参加政府采购活动前三年内在经营活动中无重大违法记录的书面声明；（格式自拟，加盖供应商公章）
（二）供应商特定资格要求，需提供以下资格证明资料：		
序号	**审查内容**	**审查标准**
1	法定代表人授权书	法定代表人授权书（附法定代表人、被授权人身份证复印件）及被授权人身份证（法定代表人直接参加招标，须提供法定代表人身份证明及身份证）
2	信用信息	供应商不得为“信用中国”网站（www.creditchina.gov.cn ）信用服务中列入失信被执行人和重大税收失信主体的供应商，不得为中国政府采购网（www.ccgp.gov.cn ）政府采购严重违法失信行为记录名单中被财政部门禁止参加政府采

		购活动的供应商(**采购代理机构于本项目磋商文件发售之日至磋商响应文件递交截止之日期间查询相关信用记录，对列入失信被执行人、税收违法黑名单、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》第二十二条规定的供应商，采购代理机构将拒绝其参与政府采购活动，查询结果以电子或纸质方式留存**）
3	无控股、管理承诺	单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得同时参加同一合同项下的政府采购活动（格式自拟，加盖供应商公章）
备注：以上资格证明文件供应商必须完全提供(除注明原件外，均为扫描件并加盖供应商公章)并胶装在磋商响应文件中，一项不合格即按照无效投标处理（注:按照陕西省财政厅关于政府采购领域贯彻落实《陕西省优化营商环境三年行动计划(2021-2023年)》的通知(陕财办采(2021)31号)文件对供应商参与政府采购活动建立“承诺+信用管理”的准入管理制度要求，以上①②③内容若提供承诺函，可根据本磋商文件格式（格式详见 附件一）要求出具承诺函，成交单位的承诺函随同成交结果一并公示。		

2、响应文件符合性审查：磋商小组在对磋商响应文件的有效性、完整性和响应程度进行审查时，可以要求供应商对磋商响应文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容等作出必要的澄清、说明或者更正。供应商的澄清、说明或者更正不得超出响应文件的范围或者改变磋商响应文件的实质性内容。

序号	项目内容	审查条件
1	供应商名称	供应商名称应与营业执照及报名时相一致
2	响应文件签署、盖章	磋商响应文件按竞争性磋商文件要求进行签署、盖章
3	响应文件书写	磋商响应文件书写无潦草、字迹模糊不清难以辨认的情况
4	磋商报价	磋商报价没有超出最高限价

5	磋商有效期	满足磋商文件规定
6	服务期	满足磋商文件规定
7	其他	磋商文件规定的其他情形

3、经过对供应商及磋商响应文件的资格性和符合性审查，出现下列情况者（包含但不限于），按无效磋商处理：

（1）供应商没有经过正常渠道领取文件或供应商的名称与登记领取磋商文件的单位名称不符。

（2）供应商的报价超出最高限价的。

（3）响应文件中未提交法定代表人授权书（法定代表人直接参加磋商未按要求提交其有效身份证明书及身份证)或授权书的合法性或有效性不符合磋商文件规定。

（4）资格证明文件的有效性或符合性不符合要求的。

（5）响应文件没有盖单位公章，无有效期或有效期达不到磋商文件的要求。

（6）响应文件与磋商文件要求不一致，或附加了采购人难以接受的条件。

（7）磋商内容出现漏项或数量与要求不符，出现重大负偏差。

（8）响应文件达不到采购要求。

（9）响应报价与市场价偏离较大，低于成本，形成不正当竞争。

（10）提供虚假证明，开具虚假资质，出现虚假应答或故意隐瞒行为。

4、磋商：磋商小组所有成员集中与各供应商分别单独进行磋商，并给所有参加磋商供应商平等的磋商机会。

5、比较与评价

（1）磋商小组在评审过程中，发现响应文件出现下列情况之一者，按以下原则修正：

A、大写金额与小写金额不一致的，以大写金额为准；

B、总价金额与单价汇总金额不一致的，以单价金额计算结果为准；

C、单价金额小数点有明显错位的，应以总价为准，并修改单价；

D、对不同文字文本响应文件的解释发生异议的，以中文文本为准；

E、文字与图表不一致的，以文字为准；

F、正本与副本不一致的，以正本为准；

（2）按照磋商文件规定的评审方法和标准，对审查合格的文件进行商务和技术评审，综合比较和评价，最低报价不做为成交的唯一条件。

6、供应商澄清：磋商小组要求供应商澄清、说明或者更正响应文件将以书面形式作出。供应商的澄清、说明或者更正应当由法定代表人或被授权委托人签字或盖章。

（四）评审标准

1、评审原则

（1）公平、公正、科学择优；

（2）质量符合国家各项规定规范标准，服务期满足竞争性磋商文件要求，项目实施方案合理可行；

（3）报价为合理低价，且不低于成本价；本项目不保证最低磋商报价人成交；

2、评审内容

（1）磋商最终书面报价；

（2）商务部分；

（3）技术部分。

3、评标方法

本项目采用综合评分法。

响应性文件满足采购文件全部实质性要求，按照采购文件中规定的评审因素量化指标评审对本项目进行综合评审后，以评标总得分最高的供应商作为本项目成交候选单位或者成交人的评标方法。若有两个或两个以上最高得分相同，推荐其中报价最低的供应商为成交候选人。若得分相同且报价相同的，则由全体磋商小组成员无记名投票，确定成交候选人排序。

4、评审标准

所有实质性响应的申请单位在规定时间内提交最终磋商书面报价，最终磋商书面报价的新报价不得高于申请文件中的第一次磋商报价，否则将导致磋商文件无效。最终磋商书面报价为最终报价，并作为计分依据，最终报价是磋商单位响应文件的有效组成部分。

磋商小组根据竞争性磋商文件所确定的评审办法计算磋商报价得分。磋商小

组依据得分高低顺序进行排名，推荐前三名为成交候选人，并由采购人确定排名第一的成交候选人为成交供应商。

采购人将磋商小组书面报告和成交通知书报监督机关备案。

依法公示后向成交人发放成交通知书。

采购人向成交人发放成交通知书后，得分最高的成交人放弃成交或因不可抗力不能履行合同的，采购人可以确定得分第二的供应商为成交人。得分第二的供应商因同样原因不能签订合同的，采购人可以确定得分第三的供应商为成交人，采购人也可以依法重新进行磋商活动。

评审指标分值构成 （总计100分）

磋商报价 20分

商务部分 10分

技术部分 70分

评审要素及分值一览表

项别	总分值		评分标准
	100	分值	
磋商报价	20	（20分）	价格分统一采用低价优先法计算，即满足竞争性磋商响应文件要求且磋商价格最低的磋商报价为磋商基准价，其价格分为满分。其他供应商的价格分统一按照下列公式计算： 磋商报价得分=(磋商基准价/最后磋商报价）×20%×100 注：1、磋商小组认为供应商的最终报价明显低于其他通过符合性审查供应商的报价，有可能影响服务质量或者不能诚信履约的，应当在磋商现场提供书面说明及相关证明材料。供应商不能证明其报价合理性的，为无效磋商； 2、本项目为非专门面向小微企业采购的采购项目，对符合价格扣除条件的小微企业报价给予15%的扣除，用扣除后的价格参加评审

技术部分	70	总体方案（20分）	**评审内容：** 供应商针对本项目制定的总体方案，包含但不限于①项目需求理解②服务计划；③安全检查工作的服务思路、原则、特点的理解；④重难点分析。 **评审标准：** 1.完整性：实施方案须全面，思路清晰、分析透彻，内容完整、方案科学、合理； 2.可实施性；切合本项目实际情况，步骤明确、可操作性强； 3.针对性：能够紧扣项目实际情况，专业性强、内容科学、合理。 **赋分标准（20分）：** 根据评审标准，按照提供内容的完整性、可实施性、针对性响应情况每项得（0-5]分，未提供或完全背离评审标准得0分。
		网络安全检查评估方案（10分）	**评审内容：** 针对本项目服务内容提出开展网络安全全面检查评估方案，方案包括：①远程检测方式检查评估方案；②现场检查方式检查评估方案。 **评审标准：** 1.完整性：方案须全面，完整、科学、合理； 2.可实施性；切合本项目实际情况，步骤明确、可操作性强； 3.针对性：能够紧扣项目实际情况，专业性强、内容科学、合理。 **赋分标准（10分）：** 根据评审标准，按照提供内容的完整性、可实施性、针对性响应情况每项得（0-5]分，未提供或完全背离评审标准得0分。

		保障措施（25分）	**评审内容：** 根据本项目服务内容，提出多方面的保障措施，以确保项目顺利实施：①远程技术检测服务质量的保障措施；②现场检查服务质量的保障措施；③服务进度保障措施；④项目风险控制措施和机制；⑤对本项目接触到的相关信息有具体的保密措施。 **评审标准：** 1.完整性：方案须全面，完整、科学、合理； 2.可实施性；切合本项目实际情况，步骤明确、可操作性强； 3.针对性：能够紧扣项目实际情况，专业性强、内容科学、合理。 **赋分标准（25分）：** 根据评审标准，按照提供内容的完整性、可实施性、针对性响应情况每项得（0-5]分，未提供或完全背离评审标准得0分。
		资料汇总整理方案（15分）	**评审内容：** 针对本项目服务内容提出资料汇总整理方案，方案包括：①资料保存管理方案；②资料报告校对、检查方案；③相关成果报告的准确性保障方案。 **评审标准：** 1.完整性：方案须全面，完整、科学、合理； 2.可实施性；切合本项目实际情况，步骤明确、可操作性强； 3.针对性：能够紧扣项目实际情况，专业性强、内容科学、合理。 **赋分标准（15分）：** 根据评审标准，按照提供内容的完整性、可实施性、针对性响应情况每项得（0-5]分，未提供或完全背离评审标准得0分。
商务部分	20分	团队人员配备（6分）	拟为本项目配备的人员具有相关专业职称证书，每有一人计2分，最多得6分 注：提供相关证书资料，不提供或完全背离评审标准得0分。
		业绩（4分）	供应商具有近三年（2022年5月至今）的类似业绩（合同扫描件并加盖供应商公章，以合同签订时间为准）每个计2分，最多得4分；未提供不得分。

注：上述要求的相关证明材料以投标文件正本中提供的有关证书复印件并加盖投标人公章为依据，复印件清晰可见。

（五）确定成交人及签订合同

1、确定成交人。代理机构将于采购人依法确定成交人后发布成交公告，并向成交人发出成交通知书。成交人在接到通知后，必须在5个工作日内领取成交通知书并支付采购代理服务费。

2、采购人在签订合同时，保留根据项目实际情况在合法范围内进行调整的权力，包括对货物数量及服务予以增加或减少。

3、签订合同。

（1）成交人应及时与采购人签订合同，代理机构作为见证方见证。

（2）如果成交人未能按规定领取成交通知书并签约，经监管部门同意后，采购人将取消其成交资格，并不退还其磋商保证金。在此情况下将另选成交人或重新招标。

4、竞争性磋商文件、成交人的竞争性磋商响应文件、对竞争性磋商响应文件的书面澄清、成交通知书等均作为合同的附件，是合同的组成部分。

（六） 质疑与投诉

1、供应商认为采购文件、采购过程和成交结果使自己的合法权益受到损害的，可依法首先向采购人提出质疑，对采购人的质疑答复不满意或采购人未在规定期限内作出答复的，供应商可向财政主管部门提起投诉，投诉人对投诉处理决定不服或者逾期未作处理的，可依法向上一级主管部门申请行政复议或向采购人当地的人民法院提起行政诉讼。质疑邮箱：huawendlzb@163.com，联系人：宋宁，联系电话：19991683602，地址：详见竞争性磋商公告。

2、质疑供应商应按照财政部制定的《政府采购质疑函范本》格式（可从财政部官方网站下载）和《政府采购质疑和投诉办法》的要求，在法定质疑期内以纸质形式提出质疑，针对同一采购程序环节的质疑应一次性提出。

3、超出法定质疑期的、重复提出的、分次提出的或内容、形式不符合《政府采购质疑和投诉办法》的，质疑供应商将依法承担不利后果。

（七）落实的政府采购政策

（1）《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）；

（2）《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）；

（3）《三部门联合发布关于促进残疾人就业政府采购政策的通知》(财库〔2017〕141号）；

（4）《关于运用政府采购政策支持乡村产业振兴的通知》(财库〔2021〕19号）；

（5）陕西省财政厅关于印发《陕西省中小企业政府采购信用融资办法》(陕财办采〔2018〕23号）；

（6）《关于进一步加大政府采购支持中小企业力度的通知》(财库〔2022〕19号）

（7）《陕西省财政厅关于加快推进我省中小企业政府采购信用融资工作的通知》（陕财办采〔2020〕15 号）；（8）其他需要落实的政府采购政策。

第四章 合同主要条款

注：本合同仅为合同的参考文本，合同签订双方可根据项目的具体要求进行修订。

2025年大荔县网络安全检查技术服务项目

政府采购合同书

甲方（采购人）：中国共产党大荔县委员会宣传部

乙方（供应商）：

合同范本

（此合同草案条款，采购人和成交供应商所签订的合同不得对磋商文件确定的事项和成交供应商的响应文件做实质性修改，最终签订的合同以采购人确定的合同内容为准。）

甲方（采购人）：_____

乙方（供应商）：_____

甲乙双方根据_____政府采购项目（项目编号：_____）采购结果及相关竞争性磋商文件、竞争性磋商响应文件，经协商一致，订立本合同，供双方共同遵守：

第一条　项目概况

服务内容：_____

服务地点：甲方指定地点

成交价格（含税）：人民币_____元。

乙方负责项目实施过程中的所有费用，甲方不再另付任何费用。

第二条　服务期限

服务期限：15日历天

合同有效期限：自____年___月___日至____年___月___日。

甲方与乙方将在本合同的有效期内，各指定一名代表负责处理与本合同有关的事务，其工作计划将由双方代表协商制定。当发现技术问题或就技术问题发生争议时，双方代表应分析原因、分清责任并协商解决方案。

乙方依本合同约定向甲方提交系统设计及实施方案，甲方应当及时进行评审鉴定及认可，若经甲方评审发现乙方提交的设计与方案存在缺陷，乙方负责进行修改。本项目完成后，由乙方向甲方提交验收申请书。

验收由甲方按合同及相关附件中的有关规定进行，乙方提供必要的配合，验收应满足本合同内容的服务内容和服务标准。如果项目实施结果符合本合同约定

的验收标准，双方将签署三份《验收合格证书》，其中两份由甲方保留，一份由乙方保留。

第三条　费用的结算

1、结算依据：本项目竞争性磋商文件、竞争性磋商响应文件、采购合同以及与本项目有关的其他资料。

2、付款方式：合同签订后付款70%，履约验收合格后付款至100%。

第四条　甲方的违约责任

1、如甲方未按本合同约定向乙方付款的，甲方应承担违约责任，每迟延一周，甲方应向乙方支付相当于合同总价0.05%的违约金，不足一周按一周计算。

2、甲方违反合同规定拒绝接收服务的，应当承担由此对乙方造成的损失。

第五条　乙方的违约责任

1、若由于乙方原因，不能在合同规定时间内完成项目实施，乙方应承担违约责任，每迟延一周，乙方应向甲方支付相当于合同总价0.05%的违约金，不足一周按一周计算。

2、乙方所交服务不符合国家法律法规和合同规定的，甲方有权拒收，并由乙方承担一切费用。

3、由于工作成果质量低劣未达到合同中约定的要求标准、由于乙方责任导致工期延误或乙方有其他违反本合同条款行为的，甲方随时享有单方解除本合同的权利，并享有就由于上述原因造成甲方的全部损失(包括但不限于甲方在此之前支付的所有费用)向乙方要求赔偿的权利。

4、在合同履行过程中，由于乙方原因导致服务无法进行的，由乙方承担由此为甲方造成的全部损失。

第六条　保密条款

对工作中了解到的甲方的技术、机密等进行严格保密，不得向他人泄漏。本合同的解除或终止不免除应承乙方担的保密义务。

第七条　不可抗力

1、本合同所称不可抗力，是指本合同各方由于地震、台风、水灾、火灾、战争以及其它不能预见、不能避免且不可克服的客观情况。

2、本合同任何一方因不可抗力不能履行或不能完全履行本合同的义务时，应在不可抗力发生后立即通知本合同的其它方、积极采取措施避免或减轻不可抗力可能给其它方造成的损失，并在不可抗力发生之日起的 10 个日历日内向其它方提供由有关部门出具的不可抗力证明文件。

3、因不可抗力不能履行合同的，根据不可抗力的影响，部分或全部免除责任，但法律另有规定的除外。迟延履行合同后发生不可抗力的，不能免除责任。

4、如果因不可抗力的影响致使本合同中止履行 30 个日历日或以上时，甲方或者乙方均有权利书面通知对方终止本合同。

第八条　争议解决

双方本着友好合作的态度,对合同履行过程中发生的违约行为进行及时的协商解决,如不能协商解决可向甲方住所地法院起诉。其它未尽事宜,由双方友好协商解决,并参照《中华人民共和国民法典》有关条款执行。

第九条　监督和管理

1、政府采购合同履行中，采购人需追加与合同标的相同的货物、工程或者服务的，在不改变合同其他条款的前提下，可以与供应商协商签订补充合同，但所有补充合同的采购金额不得超过原合同采购金额的百分之十。

2、甲乙双方均应自觉配合有关监督管理部门对合同履行情况的监督检查，如实反映情况，提供有关资料；否则，将对有关单位、当事人按照有关规定予以处罚。

第十条　无效合同

甲乙双方如因违反政府采购法及相关法律法规的规定，被宣告合同无效的，一切责任概由过错方自行承担。

第十一条 附则

1、_____项目（项目编号：_____）的竞争性磋商文件、成交通知书、乙方竞争性磋商响应文件及澄清说明文件都是本合同的组成部分，甲、乙双方必须全面遵守，如有违反，应承担违约责任。

2、本合同一式五份,甲乙双方各执二份,政府采购监督管理机构一份。

3、本合同自签字盖章之日起生效。

4、附件：

甲 方	乙 方
（盖章）	（盖章）
地址：	地址：
法定代表人：	法定代表人：
被授权人：（签字）	被授权人：（签字）
日期： 年 月 日	日期： 年 月 日

第五章 采购内容及要求

一、采购内容

序号	服务内容	服务清单		数量	单位
1	根据陕西省网络安全检查相关文件要求，对全县党政机关、企事业单位的重要互联网应用系统(含网站)采用信息收集、远程监测、人工渗透等技术手段进行安全检查，结合各单位实际安全现状，编写技术报告。随即选取党政机关及重点企事业单位进行现场检	网络资产收集	对目标网络系统或主机进行信息收集，摸清目标网络环境情况，梳理目标网络资产信息。	1	项
2		渗透测试	通过远程检测的方式，对互联网系统（含网站）通过人工挖掘的方式进行漏洞识别及漏洞利用，充分挖掘和暴露系统的弱点，从而查找系统存在的安全风险和可能产生的危害，并给出整改建议及渗透测试报告。	1	项
3		现场检查	通过现场检查的方式，依据《网络安全检查评估工作指南》，对党政机关或企事业单位开展网络安全检查检测，指导运维人员对网络进行修复和加固工作，消除风险隐患，核查标准规范，强化防护能力。深入区县对部分内网系统进行专项技术抽查。并根据技术检测结果，对于问题严重的区县进行现场访谈。配合网信办根据检测及访谈结果进行现场反馈，现场根据各单位实际情况进行技术指导。	1	项
4		重要敏感时期保障服	在重要敏感时期保障前加强值班值守，对互联网上的业务系统开展远程监测工作。	1	项

	查访谈，对机房内网开展技术检测，并现场提供技术指导。	务			
5		网络安全应急支撑指导服务	在发生网络安全事件之后，及时跟进应急响应进行指导处置，第一时间遏制威胁缓解系统影响，最大程度减少损失。	1	项
6		网络安全汇总报告	将各项完成项进行分析汇总，编制检查结果报告，并按照县委宣传部领导要求进行修改完善。	1	项
7		网络安全大讲堂	加强网络安全宣传和教育工作，开展网络安全管理人员和技术人员专业技能培训，提高各级单位人员的安全防护意识及相关人员防护技能水平，通过对网络安全领域的法规政策解读,提升人员信息安全意识,提商对网络安全的敏感度。	1	次
8		其它事项	支撑的其它网络安全技术服务。	1	项

二、检查目的

通过开展信息安全检查，进一步梳理、掌握大荔县重要网络与信息安全基本情况，查找突出的问题和薄弱环节，分析面临的安全威胁和风险，有针对性的采取防范对策和改进措施，加强网络与信息系统安全管理和技术防护，促进安全防护能力和水平提升，预防和减少重大信息安全事件的发生。

三、工作目标

认真贯彻落实网络强国战略思想和全省网络安全和信息化工作会议精神，深入实施《中华人民共和国网络安全法》，《党委（党组）网络安全工作责任制实施办法》，按照习近平总书记“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”的重要指示精神，狠抓责任落实，以排查风险、通报预警、有效处置、保障安全为目标，着力发现和化解网络安全风险，全面提升网络安全服务保障能力和水平，为践行“五个扎实”，落实“五新”战略，实现“追赶超越”提供坚实的网络安全保障。

四、工作依据

《陕西省关键信息基础设施网络安全检查评估工作指南》

《信息安全技术信息安全风险评估规范》（GB/T209842007）

《信息安全技术云计算服务安全指南》（GB/T311672014）

《信息安全技术云计算服务安全能力要求》（GB/T311682014）

《信息安全技术信息系统安全等级保护基本要求》（GB/T222392008）

《信息技术安全技术信息安全管理体系要求》（GB/T220802008）

《信息技术安全技术信息技术安全性评估准则》（GB/T183362001）

五、实施范围

大荔县范围内关键信息基础设施，涵盖县、区党政机关门户网站和重点新闻网站，向公众提供水、电、气、热等服务的应用系统，党政机关、事业单位、国有企业、大型互联网平台运行的存储、处理个人信息数量超过100万的信息系统，以及为上述重要信息系统提供运行环境的云平台或其他一旦发生网络安全事件影响的重要信息系统。

六、具体检查内容

1.网络安全管理情况

按照国家、省和我县网络安全政策和标准规范要求，建立健全网络安全管理制度及落实情况。重点检查网络安全主管领导、管理机构和信息安全员岗位设置及履职情况，网络安全责任制落实及事故责任追究情况，人员、资产、采购、外包服务等日常安全管理情况，网络安全经费保障情况等。

2.远程网络渗透测试

授权第三方专业技术团队使用技术平台检测与渗透测试相结合的方式，对大荔县、区（县）范围内与互联网连接的网站及互联网业务系统进行安全技术检测（包括技术平台检测、渗透测试），经过设备扫描后，进行人工漏洞验证，对存在的安全漏洞隐患进行及时修复加固。

3.机房内网弱密码检测专项服务

机房内网弱密码检测专项服务，对用户系统中是否使用有弱密码的问题进行集中云检测，并进行统一的管理，发布，通知等工作。

4.对关键或薄弱环节开展督导抽查

本次项目需要抽查部分党政机关进行以下几方面的现场检查工作和检查数据分析及报告整理编写：

安全健康状态检查：负责检查信息资产情况，主要包括信息系统建设、信息系统核心设备及虚拟资产情况，网络安全设备及终端设备资产情况；负责开展内部网络安全测试，主要包括内部主机安全测试、网络隔离测试、无线安全测试和内网渗透测试情况等。

安全组织管理情况：负责核查安全管理机构及人员情况，网络安全管理部门及网络安全技术人员是否明确；负责核查安全管理制度情况，安全组织架构是否

完备，网络安全管理部门及网络安全技术人员是否明确，安全管理制度内容是否合理及修订执行情况；负责核查安全建设管理情况，网络安全产品的采购、开发、测试验收及安全服务商选择情况。

人员安全能力情况：负责核查人员安全管理情况，主要包括安全教育培训情况、离职人员处理情况、外部人员访问情况、重点岗位人员录用和审查情况、人员考核情况等。

安全运维实施情况：负责检查安全运维情况，主要包括机房环境情况、网络安全管理情况、系统安全管理情况、恶意代码防范管理情况；负责检查信息系统数据及备份恢复和管理情况；负责检查日常监测情况，主要包括日常安全监测、日志分析、威胁监测情况。

安全应急保障情况：负责检查应急组织是否明确、应急预案制定是否合理和应急演练开展情况等。

5.网络安全培训

开展2025年度网络安全课堂培训，主要功能或目标:按照要求，结合大荔县实际，通过现场搭培训，演示了勒索病毒、网页篡改等常见网络安全攻击事件，全流程展现了网络安全事件的预警响应、信息通报、应急处置和改进加固等各个环节，梳理有效应对突发事件的工作流程，进一步明确网络日常维护和管理的各项工作要求。

6.风险安全评估

对目标单位进行风险评估。通过人工安全漏洞扫描评估，及时发现服务器、应用系统等设备中存在的安全漏洞，通过现场访谈，掌握安全制度方面的不足，指导运维人员对网络进行修复和加固工作，消除由于安全漏洞而给各关基单位带

来的网络安全风险。

7.结果分析汇总

技术保障小组将对县级及各区县检查结果数据，进行横纵向对比分析，寻找普遍存在安全问题的检查项和存在明显问题的行业进行重点关注和结果通报。并对历史数据进行积累和对比分析，形成历史档案，发现安全趋势，指导长期本县的网络安全结果开展。同时，汇总各单位提交的自查报告、自查表、风险评估报告、网络安全工作报告，结合技术检测结果、现场检查结果、专项检查结果等，进行数据分析和数据验证后，编制《2025年大荔县网络安全检查报告》，包括相应的整改计划和整改措施等，提交至大荔县委网信办。

七、合同履行要求

1、严格按照磋商文件和合同的要求完成服务，不得擅自变更服务内容和进度。

2、如因不可抗力等原因无法按时履行合同，应及时通知采购人，并采取相应的补救措施。

3、接受采购人的监督和检查，及时整改存在的问题。

4、服务结束后，应按照要求提交检查报告和相关资料。

八、商务要求

1、服务期：15日历天

2、服务地点：大荔县

3、付款方式：合同签订后付款70%，履约验收合格后付款至100%。

4、项目验收：

4.1服务期满后，采购人根据竞争性磋商文件和竞争性磋商响应文件及相关

文件，进行验收，确认服务内容是否达到采购要求。

4.2采购人组织供应商(必要时请有关专家)进行验收，验收合格后，填写项目验收单作为对项目的最终认可。

4.3供应商向采购人提供服务过程中的所有资料,以便采购人日后管理。

4.4验收依据

（1）合同文本及合同补充文件（条款）。

（2）竞争性磋商文件。

（3）成交人的磋商响应文件。

（4）国家相关标准、行业标准或者其他标准、规范。

5、违约责任：

（1）按《中华人民共和国民法典》中的相关条款执行。

（2）未按合同要求提供服务质量不能满足技术要求，采购人有权终止合同，并对成交单位违约行为进行追究，同时按《政府采购法》的有关规定进行处罚。

附件一：《网络安全检查操作指南》

网络安全检查操作指南

为指导关键信息基础设施网络安全检查工作，依据《关于开展关键信息基础设施网络安全检查的通知》（中网办发〔2022〕3号，以下简称《检查通知》），参照《信息安全技术 政府部门信息安全管理基本要求》（GB/T 292452012）等国家网络安全技术标准规范，制定本指南。

本指南主要用于各地区、各部门、各单位在开展关键信息基础设施网络安全检查工作（以下简称“检查工作”）时参考。

1. 关键信息基础设施摸底

1.1. 关键信息基础设施定义及范围

关键信息基础设施是指面向公众提供网络信息服务或支撑能源、通信、金融、交通、公用事业等重要行业运行的信息系统或工业控制系统，且这些系统一旦发生网络安全事故，会影响重要行业正常运行，对国家政治、经济、科技、社会、文化、国防、环境以及人民生命财产造成严重损失。

关键信息基础设施包括**网站类**，如党政机关网站、企事业单位网站、新闻网站等；**平台类**，如即时通信、网上购物、网上支付、搜索引擎、电子邮件、论坛、地图、音视频等网络服务平台；**生产业务类**，如办公和业务系统、工业控制系统、大型数据中心、云计算平台、电视转播系统等。

1.2. 确定关键信息基础设施步骤

关键信息基础设施的确定，通常包括三个步骤，一是确定关键业务，二是确定支撑关键业务的信息系统或工业控制系统，三是根据关键业务对信息系统或工业控制系统的依赖程度，以及信息系统发生网络安全事件后可能造成的损失认定关键信息基础设施。

（一）确定本地区、本部门、本行业的关键业务。

可参考表1，结合本地区、本部门、本行业实际梳理关键业务。关键信息基础设施涉及的关键业务包含但不限于以下行业：

表1 关键信息基础设施业务判定表

行业		关键业务
能源	电力	电力生产（含火电、水电、核电等）
		电力传输
		电力配送
	石油石化	油气开采
		炼化加工
		油气输送
		油气储存
	煤炭	煤炭开采
		煤化工
金融		银行运营
		证券期货交易
		清算支付
		保险运营
交通	铁路	客运服务
		货运服务
		运输生产
		车站运行
	民航	空运交通管控
		机场运行

行业		关键业务
		订票、离港及飞行调度检查安排
		航空公司运营
	公路	公路交通管控
		智能交通系统（一卡通、ETC收费等）
	水运	水运公司运营（含客运、货运）
		港口管理运营
		航运交通管控
水利		水利枢纽运行及管控
		长距离输水管控
		城县水源地管控
医疗卫生		医院等卫生机构运行
		疾病控制
		急救中心运行
环境保护		环境监测及预警（水、空气、土壤、核辐射等）
工业制造（原材料、装备、消费品、电子制造）		企业运营管理
		智能制造系统（工业互联网、物联网、智能装备等）
		危化品生产加工和存储管控（化学、核等）
		高风险工业设施运行管控

行业	关键业务
县政	水、暖、气供应管理
	城县轨道交通
	污水处理
	智慧城县运行及管控
电信与互联网	语音、数据、互联网基础网络及枢纽
	域名解析服务和国家顶级域注册管理
	数据中心/云服务
广播电视	电视播出管控
	广播播出管控
教育	信息公开（大中专院校、中小学网站、校园网）
	教学科研管理业务系统
新闻网站	
商业平台	即时通信、网上购物、网上支付、搜索引擎、电子邮件、论坛、地图、音视频等
政府部门	信息公开
	面向公众服务
	办公业务系统

（二）确定关键业务相关的信息系统或工业控制系统。

根据关键业务，逐一梳理出支撑关键业务运行或与关键业务相关的信息系统或工业控制系统，形成候选关键信息基础设施清单。如电力行业火电企业的发电机组控制系统、管理信息系统等；县政供水相关的水厂生产控制系统、供水管网监控系统等。

（三）认定关键信息基础设施。

对候选关键信息基础设施清单中的信息系统或工业控制系统，根据本地区、本部门、本行业实际，参照以下标准认定关键信息基础设施。

A.网站类

符合以下条件之一的，可认定为关键信息基础设施：

1. 县级（含）以上党政机关网站。（2022年检查中，所有党政机关网站均应填写上报登记表）

2. 重点新闻网站。（2022年检查中，所有新闻网站均应填写上报登记表）

3. 日均访问量超过100万人次的网站。

4. 一旦发生网络安全事故，可能造成以下影响之一的：

（1）影响超过100万人工作、生活；

（2）影响单个地县级行政区30%以上人口的工作、生活；

（3）造成超过100万人个人信息泄露；

（4）造成大量机构、企业敏感信息泄露；

（5）造成大量地理、人口、资源等国家基础数据泄露；

（6）严重损害政府形象、社会秩序，或危害国家安全。

5. 其他应该认定为关键信息基础设施。

B.平台类

符合以下条件之一的，可认定为关键信息基础设施：

1. 注册用户数超过1000万，或活跃用户（每日至少登陆一次）数超过100万。

2. 日均成交订单额或交易额超过1000万元。

3. 一旦发生网络安全事故，可能造成以下影响之一的：

（1）造成1000万元以上的直接经济损失；

（2）直接影响超过1000万人工作、生活；

（3）造成超过100万人个人信息泄露；

（4）造成大量机构、企业敏感信息泄露；

（5）造成大量地理、人口、资源等国家基础数据泄露；

（6）严重损害社会和经济秩序，或危害国家安全。

4.其他应该认定为关键信息基础设施。

C.生产业务类

符合以下条件之一的，可认定为关键信息基础设施：

1. 地县级以上政府机关面向公众服务的业务系统，或与医疗、安防、消防、应急指挥、生产调度、交通指挥等相关的城县管理系统。

2. 规模超过1500个标准机架的数据中心。

3. 一旦发生安全事故，可能造成以下影响之一的：

（1）影响单个地县级行政区30%以上人口的工作、生活；

（2）影响10万人用水、用电、用气、用油、取暖或交通出行等；

（3）导致5人以上死亡或50人以上重伤；

（4）直接造成5000万元以上经济损失；

（5）造成超过100万人个人信息泄露；

（6）造成大量机构、企业敏感信息泄露；

（7）造成大量地理、人口、资源等国家基础数据泄露；

（8）严重损害社会和经济秩序，或危害国家安全。

4.其他应该认定为关键信息基础设施。

1.3. 关键信息基础设施信息登记

各单位梳理确定本单位所主管的关键信息基础设施，并填写登记表。主要包括：

a）设施主管单位信息；

b）设施主要负责人、网络安全管理部门负责人、运维单位负责人联系方式；

c）设施提供服务的基本类型、功能描述、网页入口信息、发生网络安全事故后影响分析、投入情况、信息技术产品国产化率；

e）数据存储情况；

f）运行环境情况；

g）运行维护情况；

h）网络安全状况；

i）商用密码使用情况。

2. 网络安全检查

2.1. 单位基本情况

对本单位基本情况进行登记，包括单位名称、组织机构代码、网络安全专职工作人员三方面内容。

表2 单位基本情况检查表

单位名称		组织机构代码	
网络安全专职工作人员	①本单位网络安全专职工作人员总数：_____ ②网络安全专职工作人员缺口：_____		

2.2. 信息系统基本情况

对本单位信息系统基本情况进行梳理，主要包括信息系统数量、互联网接入情况、门户网站基本情况三方面内容。

表3 信息系统基本情况检查表

信息系统数量	①信息系统总数（包括本单位自行运维和委托其他单位运维的信息系统）：_____个 其中：网站数： 业务系统数： 办公系统数（含邮件系统）： ②本年度新投入运行信息系统数量：_____个
互联网接入	①互联网接入口总数：_____ □接入中国联通 接入口数量：_____ □接入中国电信 接入口数量：_____ □其他：_____接入口数量：_____
门户网站	①域名：_____ .cn 域名 NS 记录：_____

	.cn域名A记录：_____ ②IP地址段：_____ ③主要协议/端口：_____ ④接入运营商：_____接入带宽：_____ ⑤CDN提供商：_____

2.3. 网络安全责任制落实情况检查

网络安全责任制落实情况检查通常包括网络安全管理工作单位领导、网络安全管理工作内设机构、网络安全责任制度建设和落实情况的检查。

2.3.1 要求

a）应明确一名主管领导，负责本单位网络安全管理工作，根据国家法律法规有关要求，结合实际组织制定网络安全管理制度，完善技术防护措施，协调处理重大网络安全事件；

b）应指定一个机构，具体承担网络安全管理工作，负责组织落实网络安全管理制度和网络安全技术防护措施，开展网络安全教育培训和监督检查等；

c）应建立健全岗位网络安全责任制度，明确岗位及人员的网络安全责任。

2.3.2 检查方式

文档查验、人员访谈。

2.3.3 检查方法

a）查验领导分工等文件，检查是否明确了网络安全主管领导；查验网络安全相关工作批示、会议记录等，了解主管领导履职情况；

b）查验本单位各内设机构职责分工等文件，检查是否指定了网络安全管理机构（如工业和信息化部指定办公厅为网络安全管理机构）；

c）查验工作计划、工作方案、规章制度、监督检查记录、教育培训记录等文档，了解管理机构履职情况；

d）查验岗位网络安全责任制度文件，检查系统管理员、网络管理员、网络安全员、一般工作人员等不同岗位的网络安全责任是否明确；

e）访谈关键岗位网络安全员，检查其网络安全意识和网络安全知识、技能掌握情况；

f）查验工作计划、工作报告等相关文档，检查网络安全员日常工作开展情况。

表4 网络安全责任制落实情况检查表

负责网络安全管理工作的单位领导	①负责网络安全管理工作的领导：□已明确 □未明确 ②姓名：_____ ③职务：_____ ④是否本单位主要负责同志：□是 □否
负责网络安全管理的内设机构	①负责网络安全管理的内设机构：□已明确 □未明确 ②机构名称：_____ ③负责人：_____职 务：_____ ④联系人：_____办公电话：_____ 移动电话：_____
网络安全责任制度建设和落实情况	①网络安全责任制度：□已建立 □未建立 ②网络安全检查责任：□已明确 □未明确 ③本年度网络安全检查专项经费：□已落实，_____万 □无专项经费

2.4. 网络安全日常管理情况检查

2.4.1 人员管理检查

2.4.1.1 要求

a）应与重点岗位的计算机使用和管理人员签订网络安全与保密协议，明确网络安全与保密要求和责任；

b）应制定并严格执行人员离岗离职网络安全管理规定，人员离岗离职时应终止信息系统访问权限，收回各种软硬件设备及身份证件、门禁卡等，并签署安全保密承诺书；

c）应建立外部人员访问机房等重要区域审批制度，外部人员须经审批后方可进入，并安排本单位工作人员现场陪同，对访问活动进行记录并留存；

d）应对网络安全责任事故进行查处，对违反网络安全管理规定的人员给予严肃处理，对造成网络安全事故的依法追究当事人和有关负责人的责任，并以适当方式通报。

2.4.1.2 检查方式

文档查验、人员访谈。

2.4.1.3 检查方法

a）查验岗位网络安全责任制度文件，检查系统管理员、网络管理员、网络安全员、一般工作人员等不同岗位的网络安全责任是否明确；检查重点岗位人员网络安全与保密协议签订情况；访谈部分重点岗位人员，抽查对网络安全责任的了解程度；

b）查验人员离岗离职管理制度文件，检查是否有终止系统访问权限、收回软硬件设备、收回身份证件和门禁卡等要求；检查离岗离职人员安全保密承诺书签署情况；查验信息系统账户，检查离岗离职人员账户访问权限是否已被终止；

c）查验外部人员访问机房等重要区域的审批制度文件，检查是否有访问审批、人员陪同等要求；查验访问审批记录、访问活动记录，检查记录是否清晰、完整；

d）查验安全事件记录及安全事件责任查处等文档，检查是否发生过因违反制度规定造成的网络安全事件、是否对网络安全事件责任人进行了处置。

表5 人员管理检查结果记录表

人员管理	①重点岗位人员安全保密协议：□全部签订 □部分签订 □均未签订 ②人员离岗离职安全管理规定：□已制定 □未制定 ③外部人员访问机房等重要区域审批制度：□已建立 □未建立

2.4.2 信息资产管理情况检查

2.4.2.1 要求

a）应建立并严格执行信息资产管理制度；

b）应指定专人负责信息资产管理；

c）应建立信息资产台账（清单），统一编号、统一标识、统一发放；

d）应及时记录信息资产状态和使用情况，保证账物相符；

e）应建立并严格执行设备维修维护和报废管理制度。

2.4.2.2 检查方式

文档查验、人员访谈。

2.4.2.3 检查方法

a）查验信息资产管理制度文档，检查信息资产管理制度是否建立；

b）查验设备管理员任命及岗位分工等文件，检查是否明确专人负责信息资产管理；访谈设备管理员，检查其对信息资产管理制度和日常工作任务的了解程度；

c）查验信息资产台账，检查台账是否完整（包括设备编号、设备状态、责任人等信息）；查验领用记录，检查是否做到统一编号、统一标识、统一发放；

d）随机抽取台账中的部分设备登记信息，查验是否有对应的实物；随机抽取一定数量的实物，查验其是否纳入信息资产台账，同台账是否相符；

e）查验相关制度文档和记录，检查设备维修维护和报废管理制度建立及落实情况。

表6 信息资产管理检查记录表

信息资产管理	①信息资产管理制度：□已建立 □未建立 ②设备维修维护和报废管理： □已建立管理制度，且记录完整 □已建立管理制度，但记录不完整 □未建立管理制度

2.4.3 经费保障情况检查

2.4.3.1 要求

a）应将网络安全设施运行维护、网络安全服务采购、日常网络安全管理、网络安全教育培训、网络安全检查、网络安全风险评估、网络安全应急处置等费用纳入部门年度预算；

b）应严格落实网络安全经费预算，保证网络安全经费投入。

2.4.3.2 检查方式

文档查验。

2.4.3.3 检查方法

a）会同本单位财物部门人员，查验上一年度和本年度预算文件，检查年度预算中是否有网络安全相关费用；

b）查验相关财务文档和经费使用账目，检查上一年度网络安全经费实际投入情况、网络安全经费是否专款专用。

表7 经费保障检查结果记录表

经费保障	①上一年度信息化总投入：_____万元，网络安全实际投入：_____万元，其中采购网络安全服务比例：_____ ②本年度信息化总预算（含网络安全预算）：_____万元，网络安全预算：_____万元，其中采购网络安全服务比例：_____

2.5. 网络安全防护情况检查

2.5.1 网络边界安全防护情况检查

2.5.1.1 要求

a）非涉密信息系统与互联网及其他公共信息网络应实行逻辑隔离，涉密信息系统与互联网及其他公共信息网络应实行物理隔离；

b）建立互联网接入审批和登记制度，严格控制互联网接入口数量，加强互联网接入口安全管理和安全防护；

c）应采取访问控制、安全审计、边界完整性检查、入侵防范、恶意代码防范等措施，进行网络边界防护；

d）应根据承载业务的重要性对网络进行分区分域管理，采取必要的技术措施对不同网络分区进行防护、对不同安全域之间实施访问控制；

e）应对网络日志进行管理，定期分析，及时发现安全风险。

2.5.1.2 检查方式

文档查验、现场核查。

2.5.1.3 检查方法

a）查验网络拓扑图，检查重要设备连接情况，现场核查内部办公系统等非涉密系统的交换机、路由器等网络设备，确认以上设备的光纤、网线等物理线路没有与互联网及其他公共信息网络直接连接，有相应的安全隔离措施；

b）查验网络拓扑图，检查接入互联网情况，统计网络外联的出口个数，检查每个出口是否均有相应的安全防护措施（互联网接入口指内部网络与公共互联网边界处的接口，如联通、电信等提供的互联网接口，不包括内部网络与其他非公共网络连接的接口）；

c）查验网络拓扑图，检查是否在网络边界部署了访问控制（如防火墙）、入侵检测、安全审计以及非法外联检测、病毒防护等必要的安全设备；

d）分析网络拓扑图，检查网络隔离设备部署、交换机VLAN划分情况，检查网络是否按重要程度划分了安全区域，并确认不同区域间采用了正确的隔离措施；

e）查验网络日志（重点是互联网访问日志）及其分析报告，检查日志分析周期、日志保存方式和保存时限等。

表8 网络边界安全防护检查结果记录表

网络边界安全防护	①网络安全防护设备部署（可多选）： □防火墙 □入侵检测设备 □安全审计设备 □防病毒网关 □抗拒绝服务攻击设备 □Web应用防火墙 □其它 ②设备安全策略配置： □使用默认配置 □根据需要配置

	③网络访问日志： □留存日志 □未留存日志

2.5.2 无线网络安全防护情况检查

2.5.2.1 要求

a）采取身份鉴别、地址过滤等措施对无线网络的接入进行管理，采用白名单管理机制，防止非授权接入造成的内网渗透事件发生；

b）修改无线路由设备的默认管理地址；

c）修改无线路由管理账户默认口令，设置复杂口令，防止暴力破解后台；

d）用户接入认证加密采用WPA2及更高级别算法，防止破解接入口令。

2.5.2.2 检查方式

现场核查。

2.5.2.3 检查方法

a）登录无线设备管理页面，查看加密方认证方式是否采用WPA2以上；

b）检查用户接入认证及管理端口登录口令，包括口令强度和更新频率，查看是否登录页面采用默认地址及默认口令；

c）登录无线网络设备管理端，检查安全防护策略配置情况，包括是否设置对接入设备采取身份鉴别认证措施和地址过滤措施；

表9 无线网络安全防护情况检查结果记录表

无线网络安全防护	①本单位使用无线路由器数量：_____ ②无线路由器用途： □访问互联网：_____个 □访问业务/办公网络：_____个 ③安全防护策略（可多选）： □采取身份鉴别措施 □采取地址过滤措施 □未设置安全防护策略

	④无线路由器使用默认管理地址情况： □存在 □不存在 ⑤无线路由器使用默认管理口令情况： □存在 □不存在

2.5.3 电子邮件系统安全防护情况检查

2.5.3.1 要求

a）应加强电子邮件系统安全防护，采取反垃圾邮件等技术措施；

b）应规范电子邮箱的注册管理，原则上只限于本部门工作人员注册使用；

c）应严格管理邮箱账户及口令，采取技术和管理措施确保口令具有一定强度并定期更换。

2.5.3.2 检查方式

文档查验、现场核查。

2.5.3.3 检查方法

a）查验电子邮件系统采购合同或部署文档，检查电子邮件系统建设方式；

b）查验电子邮件系统管理相关规定文档，检查是否有注册审批流程要求；查验服务器上邮箱账户列表，同本单位人员名单进行核对，检查是否有非本单位人员使用；

c）查看邮箱口令策略配置界面，检查电子邮件系统是否设置了口令策略，是否对口令强度和更改周期等进行要求。

d）查验设备部署或配置情况，检查电子邮件系统是否采取了反垃圾邮件、病毒木马防护等技术安全防护措施；

表10 电子邮件系统安全防护检查结果记录表

	①建设方式：□自行建设 □由上级单位统一管理 □使用第三方服务 邮件服务提供商_____

电子邮件安全防护	②帐户数量：_____个 ③注册管理：□须经审批登记 □任意注册 ④注销管理：□人员离职后，及时注销 □无管理措施 ⑤口令管理：□使用技术措施控制口令强度 位数要求：□4位 □6位 □8位 其他： 复杂度要求：□数字 □字母 □特殊字符 更换频次要求：□强制定期更换，更换频次： □无强制更换要求 □没有采取技术措施控制口令强度 ⑥安全防护：（可多选） □采取数字证书 □采取反垃圾邮件措施 □其他：

2.5.4 终端计算机安全防护情况检查

2.5.4.1 要求

a）应采用集中统一管理方式对终端计算机进行管理，统一软件下发，统一安装系统补丁，统一实施病毒库升级和病毒查杀，统一进行漏洞扫描；

b）应规范软硬件使用，不得擅自更改软硬件配置，不得擅自安装软件；

c）应加强账户及口令管理，使用具有一定强度的口令并定期更换；

d）应对接入互联网的终端计算机采取控制措施，包括实名接入认证、IP地址与MAC地址绑定等；

e）应定期对终端计算机进行安全审计；

f）非涉密计算机不得存储和处理国家秘密信息。

2.5.4.2 检查方式

现场核查、工具检测。

2.5.4.3 检查方法

a）查看集中管理服务器，抽查终端计算机，检查是否部署了终端管理系统或采用了其他集中统一管理方式对终端计算机进行管理，包括统一软硬件安装、统一补丁升级、统一病毒防护、统一安全审计等；

b）查看终端计算机，检查是否安装有与工作无关的软件；

c）使用终端检查工具或采用人工方式，检查终端计算机是否配置了口令策略；

d）访谈网络管理员和工作人员，检查是否采取了实名接入认证、IP地址与MAC地址绑定等措施对接入本单位网络的终端计算机进行控制；将未经授权的终端计算机接入网络，测试是否能够访问互联网，验证控制措施的有效性；

e）查验审计记录，检查是否对终端计算机进行了安全审计。

表11 终端计算机安全防护检查结果记录表

终端计算机安全防护	①管理方式： □集中统一管理（可多选） □规范软硬件安装 □统一补丁升级 □统一病毒防护 □统一安全审计 □对移动存储介质接入实施控制 □统一身份管理 □分散管理 ②接入互联网安全控制措施： □有控制措施（如实名接入、绑定计算机IP和MAC地址等） □无控制措施 ③接入办公系统安全控制措施： □有控制措施（如实名接入、绑定计算机IP和MAC地址等） □无控制措施

2.5.5 移动存储介质检查

2.5.5.1 要求

a）应严格存储阵列、磁带库等大容量存储介质的管理，采取技术措施防范外联风险，确保存储数据安全；

b）应对移动存储介质进行集中统一管理，记录介质领用、交回、维修、报废、销毁等情况；

c）非涉密移动存储介质不得存储涉及国家秘密的信息，不得在涉密计算机上使用；

d）移动存储介质在接入本部门计算机和信息系统前，应当查杀病毒、木马等恶意代码；

e）应配备必要的电子信息消除和销毁设备，对变更用途的存储介质要消除信息，对废弃的存储介质要进行销毁。

2.5.5.2 检查方式

文档查验、人员访谈、现场核查。

2.5.5.3 检查方法

a）访谈网络管理员，检查大容量存储介质是否存在远程维护，对于有远程维护的，进一步检查是否有相应的安全风险控制措施；查看光纤、网线等物理线路连接情况，检查大容量存储介质是否在无防护措施情况下与互联网及其他公共信息网络直接连接；

b）查验相关记录，检查是否对移动存储介质进行统一管理，包括统一领用、交回、维修、报废、销毁等；

c）查看服务器和办公终端计算机上的杀毒软件，检查是否开启了移动存储介质接入自动查杀功能；

d）查看设备台账或实物，检查是否配备了电子信息消除和销毁设备。

表12 移动存储介质安全防护检查结果记录表

移动存储介质安全防护	①管理方式： □集中管理，统一登记、配发、收回、维修、报废、销毁 □未采取集中管理方式

	②信息销毁： □已配备信息消除和销毁设备 □未配备信息消除和销毁设备

2.5.6 漏洞修复情况检查

2.5.6.1 要求

a）应定期对本单位主机、网络安全防护设备、信息系统进行漏洞检测，对于发现的安全漏洞及时进行修复处置；

b）重视自行监测发现与第三方漏洞通报机构告知的漏洞风险，及时处置。

2.5.6.2 检查方法

人员访谈、现场核查。

2.5.6.3 检查要求

a）查看相关漏洞扫描记录，确定扫描时间和周期；

b）查验收到的漏洞风险通报，访谈网站安全管理人员是否对漏洞风险进行及时处置；

c）查验事件处置记录，检查网络安全事件报告和通报机制建立情况，是否对所有网络安全事件都进行了处置。

表13 漏洞修复情况检查结果记录表

漏洞修复情况	①漏洞检测周期：□每月 □每季度 □每年 □不进行漏洞检测 ②20023年自行发现漏洞数量：_____个 收到漏洞风险通报数量：_____个 其中已得到处置的漏洞风险数量：_____个

2.6. 网络安全应急工作情况检查

2.6.1 要求

a）应制定网络安全事件应急预案，原则上每年评估一次，并根据实际情况适时修订；

b）应组织开展应急预案的宣贯培训，确保相关人员熟悉应急预案；

c）每年应开展网络安全应急演练，检验应急预案的可操作性，并将演练情况报网络安全主管部门；

d）应建立网络安全事件报告和通报机制，提高预防预警能力；

e）应明确应急技术支援队伍，做好应急技术支援准备；

f）应做好网络安全应急物资保障，确保必要的备机、备件等资源到位；

g）应根据业务实际需要对重要数据和业务系统进行备份。

2.6.2 检查方式

文档查验、人员访谈。

2.6.3 检查方法

a）查验应急预案文本等，检查应急预案制定和年度评估修订情况；

b）查验宣贯材料和培训记录，检查是否开展过预案宣贯培训；访谈系统管理员、网络管理员和工作人员，检查其对应急预案的熟悉程度；

c）查验演练计划、方案、记录、总结等文档，检查本年度是否开展了应急演练；

d）查验事件处置记录，检查网络安全事件报告和通报机制建立情况，是否对所有网络安全事件都进行了处置；

e）查验应急技术支援队伍合同及安全协议、参与应急技术演练及应急响应等工作的记录文件，确认应急技术支援队伍能够发挥有效的应急技术支撑作用；

f）查验设备或采购协议，检查是否有网络安全应急保障物资或有供应渠道；

g）查验备份数据和备份系统，检查是否对重要数据和业务系统进行了备份。

表14 网络安全应急工作检查结果记录表

应急预案	□已制定 20023年修订情况：□修订 □未修订 □未制定
	20023年应急预案启动次数：_____
应急演练	□20023年已开展，演练次数：_____，其中实战演练数：_____

	□20023年未开展
应急技术队伍	□本部门所属 □外部服务机构 □无

2.7. 网络安全教育培训情况检查

2.7.1 要求

a）应加强网络安全宣传和教育培训工作，提高网络安全意识，增强网络安全基本防护技能；

b）应定期开展网络安全管理人员和技术人员专业技能培训，提高网络安全工作能力和水平；

c）应记录并保存网络安全教育培训、考核情况和结果。

2.7.2 检查方式

文档查验、人员访谈。

2.7.3 检查方法

a）查验教育宣传计划、会议通知、宣传资料等文档，检查网络安全形势和警示教育、基本防护技能培训开展情况；

b）访谈机关工作人员，检查网络安全基本防护技能掌握情况；

c）查验培训通知、培训教材、结业证书等，检查网络安全管理和技术人员专业技能培训情况。

表15 网络安全教育培训检查结果记录表

培训次数	2025年开展网络安全教育培训（非保密培训）的次数：_____
培训人数	2025年参加网络安全教育培训的人数：_____ 占本单位总人数的比例：_____%

2.8. 技术产品使用情况检查

对本单位使用的技术产品使用情况进行全面检查，以便针对性地开展网络安全管理和防护工作。

重点梳理主要技术产品（包括服务器、终端计算机、数据库管理系统、路由器、交换机、存储设备、邮件系统等类型）的数量、生产商（品牌）情况，记录结果（表16）。

表16 信息系统主要构成梳理记录表

<table>
<tr><td>检查项</td><td colspan="10">检查结果</td></tr>
<tr><td rowspan="3">服务器</td><td>品牌</td><td>联想</td><td>曙光</td><td>浪潮</td><td>华为</td><td>IBM</td><td>HP</td><td>DELL</td><td>Oracle</td><td></td></tr>
<tr><td>数量</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="10">其他：
1. 品牌_____，数量_____
2. 品牌_____，数量_____
①使用国产CPU的台数：_____
②使用国产操作系统的台数：_____</td></tr>
<tr><td rowspan="3">终端计算机
（含笔记本）</td><td>品牌</td><td>联想</td><td>长城</td><td>方正</td><td>清华同方</td><td>华硕</td><td>宏基</td><td></td><td></td></tr>
<tr><td>数量</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="10">其他：
1. 品牌_____，数量_____
2. 品牌_____，数量_____
①使用国产CPU的台数：_____
②使用国产操作系统的台数：_____
使用Windows xp/7/8的台数：_____
③安装国产字处理软件的台数：_____
④安装国产防病毒软件的台数：_____</td></tr>
<tr><td>数据库管理</td><td>品牌</td><td>金仓</td><td>达梦</td><td>Orac</td><td>DB2</td><td>SQLServer</td><td>Acces</td><td>Mysql</td><td></td></tr>
</table>

系统					le			s	
	数量							
	其他： 1. 品牌_____，数量_____ 2. 品牌_____，数量_____							
路由器	品牌	华为	中兴	锐捷网络	H3C	Cisco	Juniper	
	数量							
	其他： 1. 品牌_____，数量_____ 2. 品牌_____，数量_____							
交换机	品牌	华为	中兴	锐捷网络	H3C	Cisco	Juniper	
	数量							
	其他： 1. 品牌_____，数量_____ 2. 品牌_____，数量_____							
存储设备	总台数： 1. 品牌_____，数量_____ 2. 品牌_____，数量_____							
邮件系统	总数： 1. 品牌_____，数量_____ 2. 品牌_____，数量_____							

2.9. 商用密码使用情况

排查本单位商用密码使用情况、包括用途、类型、使用的密码算法等。

表17 渗透测试检查结果统计表

①密码功能用途（可多选）： □身份认证 □访问控制 □电子签名 □安全审计 □传输保护 □存储保护 □密钥管理 ②密码机 数量：_____ 密码系统 数量：_____ 智能IC卡 数量：_____ 智能密码钥匙 数量：_____ 动态令牌 数量：_____ ③所采用的密码算法： 对称算法：□SM1 □SM4 □SM7 □AES □DES □3DES 非对称算法：□SM2 □SM9 □RSA1024 □RSA2048 杂凑算法：□SM3 □SHA1 □SHA256 □SHA384 □SHA512 □MD5 其它：_____

2.10. 本年度技术检测及网络安全事件情况

2.10.1 技术检测情况

2.10.1.1 渗透测试

a）应重点对认定为关键信息基础设施的信息系统进行安全检测；

b）使用漏洞扫描等工具测试关键信息基础设施，检测是否存在安全漏洞；

c）开展人工渗透测试，检查是否可以获取应用系统权限，验证网站是否可以被挂马、篡改页面、获取敏感信息等，检查系统是否被入侵过（存在入侵痕迹）等。

表18 渗透测试检查结果统计表

渗透测试	进行渗透测试的系统数量： 其中，可以成功控制的系统数量：

2.10.1.2 恶意代码及安全漏洞检测

a）可根据工作实际合理安排年度检测的服务器数量，每1～2年对所有服务器进行一次技术检测，重要业务系统和门户网站系统的服务器应作为检测重点；

b）使用病毒木马检测工具，检测服务器是否感染了病毒、木马等恶意代码；

c）使用漏洞扫描等工具检测服务器操作系统、端口、应用、服务及补丁更新情况，检测是否关闭了不必要的端口、应用、服务，是否存在安全漏洞。

表19 恶意代码、安全漏洞检测结果统计表

恶意代码检测结果	①进行病毒木马等恶意代码检测的服务器台数：_____ 其中，存在恶意代码的服务器台数：_____ ②进行病毒木马等恶意代码检测的终端计算机台数：_____ 其中，存在恶意代码的终端计算机台数：_____
安全漏洞检测结果	①进行漏洞扫描的服务器台数：_____ 其中，存在高风险漏洞的服务器台数：_____ ②进行漏洞扫描的终端计算机台数：_____ 其中，存在高风险漏洞的终端计算机台数：_____

2.10.2 网络安全事件情况

a）查看入侵检测、网络防火墙、Web应用防火墙、数据库审计设备中日志记录，统计得出检测到的攻击数；

b）查阅本年度风险评估及系统安全测评评估报告等相关记录文档，统计出网络安全事件数；

c）查阅年度收到各平台发布的网络安全风险提示数。

表20 网络安全事件检查结果表

网络安全事件情况	①监测到的网络攻击次数：_____ 其中：本单位遭受DDoS攻击次数：_____ 系统被嵌入恶意代码次数：_____ ②网络安全事件次数：_____

	其中：服务中断次数：_____ 信息泄露次数：_____ 网页被篡改次数：_____

2.11. 外包服务管理情况检查

2.11.1 要求

a）应建立并严格执行信息技术外包服务安全管理制度；

b）应与信息技术外包服务提供商签订服务合同和网络安全与保密协议，明确网络安全与保密责任，要求服务提供商不得将服务转包，不得泄露、扩散、转让服务过程中获知的敏感信息，不得占有服务过程中产生的任何资产，不得以服务为由强制要求委托方购买、使用指定产品；

c）信息技术现场服务过程中应安排专人陪同，并详细记录服务过程；

d）外包开发的系统、软件上线应用前应进行安全测评，要求开发方及时提供系统、软件的升级、漏洞等信息和相应服务；

e）信息系统运维外包不得采用远程在线运维服务方式；

2.11.2 检查方式

文档查验、人员访谈。

2.11.3 检查方法

a）查验相关制度文档，检查是否有外包服务安全管理制度；

b）查验信息技术外包服务合同及网络安全与保密协议，检查网络安全责任是否清晰；

c）查验外包人员现场服务记录，查验记录是否完整（包括服务时间、服务人员、陪同人员、工作内容等信息）；

d）访谈系统管理员和工作人员，查验安全测评报告，检查外包开发的系统、软件上线前是否进行过网络安全测评及其方式；

e）查验外包服务合同及技术方案等文档，检查是否存在远程在线运维服务；如确需采用远程在线服务的，检查是否对安全风险进行了充分评估并采取了书面审批、访问控制、在线监测、日志审计等安全防护措施。

表21 外包服务管理检查结果记录表

外包服务机构1	机构名称	
	机构性质	□国有单位 □民营企业 □外资企业 □合资企业
	服务内容	□系统集成 □系统运维 □风险评估 □安全检测 □安全加固 □应急支持 □数据存储 □数据分析 □灾难备份 □安全监测 □流量清洗 □其他
外包服务机构2	机构名称	
	机构性质	□国有单位 □民营企业 □外资企业 □合资企业
	服务内容	□系统集成 □系统运维 □风险评估 □安全检测 □安全加固 □应急支持 □数据存储 □数据分析 □灾难备份 □安全监测 □流量清洗 □其他

3. 检查总结整改

3.1. 汇总检查结果

检查实施完成后，检查办公室应及时对检查结果进行梳理、汇总，从安全管理、技术防护等方面对检查发现的问题和隐患进行分类整理。

3.2. 分析问题隐患

检查办公室应对检查发现的问题和隐患逐项进行研究，深入分析产生的原因。结合年度网络安全形势，对本单位面临的网络安全威胁和风险程度、信息系统抵御网络攻击的能力进行评估。

3.3. 研究整改措施

检查办公室在深入分析问题隐患的基础上，研究提出针对性的改进措施建议。本单位网络安全管理部门应根据检查办公室的建议，组织相关单位和人员进行整改，对于不能及时整改的，要制定整改计划和时间表，整改完成后应及时进行再评估。

3.4. 编写总结报告

本单位网络安全管理部门应组织检查办公室对检查工作进行全面总结，编写检查报告，网络安全检查总结报告的参考格式如下：

网络安全检查总结报告参考格式

一、报告名称

×××（单位名称）×××年网络安全检查总结报告。

二、检查总结报告组成

检查总结报告包括主报告、检查结果统计表及自评估表三部分。

三、主报告内容要求

（一）网络安全检查工作组织开展情况

概述检查工作组织开展情况、所梳理的关键信息基础设施情况。

（二）关键信息基础设施确定情况

此次检查确定关键信息基础设施的数量、分布、功能等情况。

（三）×××年网络安全主要工作情况

详细描述本单位×××年在网络安全管理、技术防护、应急管理、宣传教育等方面开展的工作情况。

（四）检查发现的主要问题和面临的威胁分析

1. 发现的主要问题和薄弱环节

2. 面临的安全威胁与风险

3. 整体安全状况的基本判断

（五）改进措施与整改效果

1. 改进措施

2. 整改效果

（六）关于加强网络安全工作的意见和建议

附件二：《网络安全自查表》

评估指标		评价要素	权重(V)	评价标准（P为量化值）	计分（P*V）
组织管理		分管领导	3	明确一名主管领导负责本部门网络安全工作。 已明确，本年度就网络安全工作作出批示或主持召开专题会议，P=1;已明确，本年度未就网络安全工作作出批示或主持召开专题会议，P=0.5；未明确，P=0。	
		责任部门	2	明确一个部门具体承担网络安全管理工作。 （应为本单位二级机构 ）。 已以正式文件等形式明确其职责，P=1;未明确，P=0。	
		信息安全员	2	各本单位及下属部门指定一名专职或兼职信息安全员。 P=指定网络安全员的机构数量与机构总数的比率。	
网络安全日常管理	规章制度	制度完整性	3	建立网络安全管理制度体系，涵盖人员管理、资产管理、采购管理、外包管理 、教育培训等方面。 制度完整，P=1；制度不完整，P=0.5；无制度,P=0。	
		制度发布	2	安全管理制度以正式文件等形式发布。 符合，P=1;不符合，P=0。	
	人员管理	保密协议	2	重点岗位人员（系统管理员、网络管	

				理员、网络安全员等）签订网络安全与保密协议。 P=重点岗位人员中签订网络安全与保密协议的比率。	
		离岗管理	2	人员离岗离职时，收回其相关权限，签署安全保密 承诺书。 符合，P=1；不符合，P=0。	
		到访管理	2	外部人员访问机房等重要区域时采取审批、人员陪同、进出记录等安全管理措施。 符合，P=1；不符合，P=0。	
	资产管理	责任落实	2	指定专人负责资产管理 ，并明确责任人职责。 符合，P=1；不符合，P=0。	
		建立台账	2	建立完整资产台账，统一编号、统一标识、统一发放。 符合，P=1；不符合，P=0。	
评估指标		评价要素	权重(V)	评价标准（P 为量化值）	计分 （P*V）
网络安全日常管理	资产管理	账物相符	2	资产台账和设备相一致。 符合，P=1；不符合，P=0。	
		维修报废	2	完整记录设备维修维护和报废信息（时间、地点、内容、责任人等）。 记录完整，P=1；记录不完整，P=0.5；无记录，P=0。	

		经费保障	3	将网络安全设施运维、日常管理、教育培训、检查评估等费用纳入年度预算 。 符合，P=1；不符合，P=0。	
	外包管理	服务协议	2	与信息技术外包服务提供商签订网络安全与保密协议 ，或在服务合同中明确网络安全与保密责任。 符合，P=1；不符合，P=0。	
		现场管理	2	现场服务过程中安排专人管理，并记录服务过程。 记录完整，P=1；记录不完整，P=0.5；无记录 ，P=0。	
		开发管理	2	外包开发的系统、软件上线前通过信息安全测评。 P=外包开发的系统、软件上线前通过信息安全测评的比率。	
		运维方式	2	原则上不得采用远程在线方式，确需采用时采取书面审批、访问控制、在线监测、日志审计等安全防护措施。 符合，P=1；不符合，P=0。	
网络安全防护管理	物理环境	机房安全	2	具备防盗窃、防破坏、防雷击、防火、防水、防潮、防静电及备用电力供应、温湿度控制、电磁防护等安全措施。 符合，P=1；不符合，P=0。	
		访问控制	1	机房配备门禁系统或有专人值守。 符合，P=1；不符合，P=0。	
	边界安全	访问控制	3	网络边界部署访问控制设备，能够阻	

				断非授权访问。 符合，P=1；有设备。但未配置侧咧，P=0.5；无设备,P=0。	
		入侵检测	2	网络边界部署入侵检测设备 ，定期更新检测规则库。 符合，P=1；有设备，但未定期更新，P=0.5；无设备，P=0。	
评估指标		评价要素	权重(V)	评价标准（P为量化值）	计分 （P*V）
网络安全防护管理	边界安全	安全审计	2	网络边界部署安全审计设备，对网络访问情况进行定期分析审计并记录审计情况。 符合，P=1；有设备，但未定期分析，P=0.5；无设备，P=0。	
		入口数量	2	同一办公区域内互联网接入口不超过2个。 符合，P=1；不符合，P=0。	
	设备安全	恶意代码	2	部署防病毒网关或统一安装防病毒软件，并定期更新恶意代码库。 符合，P=1；有设备，但未定期更新，P=0.5；无设备，P=0。	
		漏洞扫描	2	定期对服务器、网络设备、安全设备等进行安全漏洞扫描。 符合，P=1；不符合，P=0。	
		服务器口令策略	1	配置口令策略保证服务器口令强度和更新频率。 P=配置了口令策略的服务器比率。	

		服务器 安全审计	1	启用安全审计功能并进行定期分析。 P=安全审计日志进行定期分析的服务器比率。	
		服务器 补丁更新	2	及时对服务器操作系统补丁和数据库管理系统补丁进行更新。 P=补丁得到及时更新的服务器比率。	
		网络设备和安全设备 口令策略	1	配置口令策略保证网络设备和安全设备（指重要设备）口令强度和更新频率。 P=网络设备和安全设备中配置了口令策略的比率。	
		终端计算机统一防护	2	采取集中统一管理方式对终端进行防护，统一软件下发、安装系统补丁。 符合，P=1；不符合，P=0。	
		终端计算机接入控制	1	采取技术措施（如部署集中管理系统、将IP地址与MAC地址绑定等）对接入单位网络的终端计算机进行控制。 符合，P=1；不符合，P=0。	
		存储安全	1	配备必要的电子信息消除和销毁设备，对变更用途的存储介质进行信息消除，对废弃的存储介质进行销毁。 符合，P=1；不符合，P=0。	
评估指标		评价要素	权重(V)	评价标准（P为量化值）	计分 （P*V）
网络安全防护管理	应用系统 （无门户网站或邮	风险评估与等级保护	2	按《信息化条例》要求，对本单位信息系统实施等级保护，开展风险评估。 等级保护定级未备案或风险评估未采	

	件系统则相应项P=1）			取备案机构开展P=0.5;未实施等级保护或未开展风险评估P=0。	
		门户网站防篡改	2	门户网站采取网页防篡改措施。 符合，P=1；不符合，P=0。	
		门户网站抗拒绝服务攻击措施	1	门户网站采取抗拒绝服务攻击措施。 符合，P=1；不符合，P=0。	
		门户网站信息发布审核	2	网站信息发布前采取内容核查、审批等安全管理措施。 符合，P=1；不符合，P=0。	
		电子邮件账号审批注册	1	建立邮件账号开通审批程序，防止邮件账号任意注册使用。 符合，P=1；不符合，P=0。	
		电子邮箱账户口令策略	1	配置口令策略保证电子邮箱口令强度和更新频率。 符合，P=1；不符合，P=0。	
		邮件清理	1	定期清理工作邮件。 符合，P=1；不符合，P=0。	
	数据安全	存储保护	2	采取技术措施（如加密、分区存储等）对存储的重要数据进行保护。 符合，P=1；不符合，P=0。	
		传输保护	2	采取技术措施对传输的重要数据进行加密和校验。 符合，P=1；不符合，P=0。	
		数据和系统备份	2	采取技术措施对重要数据和系统进行	

				定期备份。 符合，P=1；不符合，P=0。	
		数据中心、灾备中心设立	1	数据中心、灾备中心应设在境内。 符合，P=1；不符合，P=0。	
网络安全应急管理		应急预案	2	制定网络安全事件应急预案（部门级预案，非单个系统的应急预案），并使相关人员熟悉应急预案。 符合，P=1；不符合，P=0。	
评估指标		评价要素	权重(V)	评价标准（P为量化值）	计分 （P*V）
网络安全应急管理		应急演练	2	开展应急演练，留存演练计划、方案、记录、总结等文档。 符合，P=1；不符合，P=0。	
		应急资源	1	制定应急技术支援队伍，配备必要的备件等应急物质。 符合，P=1；不符合，P=0。	
		事件处理	2	发生网络安全事件后，及时向主管领导报告，按照预案开展处置工作；重大事件及时通报网络安全主管部门。及时按照省信息安全主管部门处置网络安全事件。 发生过事件并按要求及时处置，或未发生事件，P=1；发生过事件未按要求及时处置，P=0。	
网络安全教育培训		意识教育	3	面向全体人员开展网络安全形势与警示教育、基本技能培训等活动。 本年度开展活动的次数>2，P=1；次数	

			=2，P=0.7；次数=1，P=0.3；次数=0，P=0。	
	专业培训	3	参加全省统一组织的管理人员和技术人员专业培训。 符合，P=1；不符合，P=0。	
网络安全检查	工作部署	1	下发检查工作相关文件或者组织召开专题会议，对年度检查工作进行部署。 符合，P=1；不符合，P=0。	
	工作机制	1	明确检查工作负责人、检查机构和检查人员。 符合，P=1；不符合，P=0。	
	技术检测	2	使用技术手段进行安全检测。 符合，P=1；不符合，P=0。	
	检查经费	1	安排并落实检查工作经费。 符合，P=1；不符合，P=0。	
	整改落实	3	完成上一年度信息安全检查整改，并针对本年度自查问题制定整改工作方案。 符合，P=1；无前一年度整改记录或本年度整改方案，P=0.5；不符合，P=0。	

网络安全情况表

部门组织情况				
分管领导	姓名		职务	
责任处室	名称		负责人	
	职务		电话	
信息安全员	姓名		移动电话	
	电话			

信息系统基本情况				
信息系统情况	信息系统总数			
	可以通过互联网访问的系统数量			
	不能通过互联网访问的系统数量			
	面向社会公众提供服务的系统数量			
	重要信息系统数量			
	本年度经过安全测评的系统数量			
互联网接入情况	互联网入口总数			
	电信入口数量		带宽（M）	
	联通入口数量		带宽（M）	
	其他入口数量		带宽(M)	
系统定级数量	第一级		第二级	
	第三级		第四级	
	第五级		未定级	
门户网站情况	域名			
	IP地址			
	运维主体			
信息技术产品使用情况				
服务器	总台数			
	国内品牌台数		其中国产CPU台数：	
	国外品牌台数			
	使用国产操作系统台数：			
	使用国外操作系统台数：			
终端计算机（含笔记本）	总台数			
	国内品牌台数		其中国产CPU台数：	

	国外品牌台数			
	使用国产操作系统台数：			
	使用国外操作系统台数：			
	使用windowsXP台数：			
	安装国产字处理软件的终端计算机台数：			
	安装国产防病毒软件的终端计算机台数：			
路由器	总台数			
	国内品牌台数		国外品牌台数	
交换机	总台数			
	国内品牌台数		国外品牌台数	
存储设备	总台数			
	国内品牌台数		国外品牌台数	
数据库管理系统	总台数			
	国内品牌台数		国外品牌台数	
邮件系统	总数			
	品牌		数量	
	品牌		数量	
负载均衡设备	总数			
	品牌		数量	
	品牌		数量	
防火墙	总数			
	品牌		数量	
	品牌		数量	
入侵检测设备	总数			
	品牌		数量	

	品牌		数量	
安全审计设备	总数			
	品牌		数量	
	品牌		数量	

外包服务机构情况表

外包服务机构1			
机构名称			
机构性质	□国有单位	□民营企业	□外资企业
服务内容	□系统集成 □安全检测 □数据存储 □其他：_____	□系统运维 □安全加固 □灾难备份	□风险评估 □应急支持
网络安全保密协议	□已签订	□未签订	
信息安全管理体系认证	已通过认证 认证机构：_____ □ 未通过认证		
外包服务机构2			
机构名称			
机构性质	□国有单位	□民营企业	□外资企业
服务内容	□系统集成 □安全检测 □数据存储 □其他：_____	□系统运维 □安全加固 □灾难备份	□风险评估 □应急支持
网络安全保密协议	□已签订	□未签订	
信息安全管理体系认证	已通过认证 认证机构：_____ □ 未通过认证		

重要信息系统情况调查表

<table>
<tr><td colspan="4">信息系统基本情况</td></tr>
<tr><td>信息系统名称</td><td colspan="3"></td></tr>
<tr><td>信息系统类型</td><td colspan="3">☐互联网系统 ☐内网/专网系统 ☐工业控制系统
(请根据系统类型选填下表内容)</td></tr>
<tr><td colspan="4">基本功能简介：</td></tr>
<tr><td colspan="4">等级保护定级：_____级（未定级留空）</td></tr>
<tr><td colspan="4">互联网系统</td></tr>
<tr><td>IP 地址</td><td></td><td>域名</td><td></td></tr>
<tr><td>是否面向社会公众提供服务</td><td>☐是 ☐否</td><td>系统运转连续性要求</td><td>可容忍中断时间：
☐小于 30 分钟
☐30 分钟至 12 小时
☐大于 12 小时</td></tr>
<tr><td>日 PV 量
（页面浏览量）</td><td></td><td>日 UV 量
（IP 访问量）</td><td></td></tr>
<tr><td>数据备份情况</td><td colspan="3">☐存储介质备份 ☐数据级灾备 ☐系统级灾备</td></tr>
<tr><td colspan="4">开发单位简介：</td></tr>
<tr><td colspan="4">运维单位简介：</td></tr>
<tr><td colspan="4"><u>内网/专网系统</u></td></tr>
<tr><td>是否与互联网数据交换</td><td>☐是 ☐否</td><td>系统运转连续性要求</td><td>可容忍中断时间：
☐小于 30 分钟
☐30 分钟至 12 小时</td></tr>
</table>

			□大于 12 小时
数据备份情况	□存储介质备份	□数据级灾备	□系统级灾备
开发单位简介：			
运维单位简介：			
工业控制系统			
是否连接互联网	□是 □否	系统运转连续性要求	可容忍中断时间： □小于 30 分钟 □30 分钟至 12 小时 □大于 12 小时
系统中断后可能造成的损失	□人身伤害□经济损失□环境污染□其它		
简要描述可能损害情况：			

信息系统密码应用情况

密码设备	使用情况			
IPsec VPN 密码机	□已采用 □未采用		使用国产算法	□是 □否
	数 量		厂家及型号	
SSL VPN 密码机	□已采用 □未采用		使用国产算法	□是 □否
	数 量		厂家及型号	
服务器密码机	□已采用 □未采用		使用国产算法	□是 □否
	数 量		厂家及型号	
第三方电子认证证书	□已采用 □未采用		认证机构名称	
安全认证网关	□已采用 □未采用		使用国产算法	□是 □否
	数 量		厂家及型号	

签名验证服务器	□已采用 □未采用	使用国产算法	□是 □否
	数 量	厂家及型号	
智能密码钥匙	□已采用 □未采用	使用国产算法	□是 □否
	数 量	厂家及型号	
电子签章系统	□已采用 □未采用	使用国产算法	□是 □否
	数 量	厂家及型号	
动态令牌	□已采用 □未采用	使用国产算法	□是 □否
	数 量	厂家及型号	
智能 IC 卡	□已采用 □未采用	使用国产算法	□是 □否
	数 量	厂家及型号	
加密 U 盘/加密硬盘	□已采用 □未采用	使用国产算法	□是 □否
	数 量	厂家及型号	
加密路由器	□已采用 □未采用	使用国产算法	□是 □否
	数 量	厂家及型号	
自建证书认证系统	□自建 □未自建	使用国产算法	□是 □否
	数 量	厂家及型号	
自建密钥管理系统	□已自建 □未自建	使用国产算法	□是 □否
	数 量	厂家及型号	
金融数据密码机	□已采用 □未采用	使用国产算法	□是 □否
	数 量	厂家及型号	
支付服务密码机	□已采用 □未采用	使用国产算法	□是 □否
	数 量	厂家及型号	
密码产品备案	□已备案 □未备案		
系统密码测评	□已测评 □未测评		
密码方案审查	□已审查 □未审查		

附件三：《网络安全检查工作检查表》

为指导网络安全现场检查工作（以下简称“检查工作”），参照《信息安全技术政府部门信息安全管理基本要求》（GB／T29245－2012）等国家网络安全技术标准规范，制定本检查表。本检查表共5大项，包括单位基本情况、信息安全培训情况、安全事件及安全防护情况、数据安全核查情况、安全管理核查情况。请各级各部门各单位配合做好检查工作。

一、单位基本情况			
单位名称			
单位地址			
检查时间			
联系人		联系电话	

二、信息安全培训情况	
年度培训计划	✪已定制 □未定制
上年度开展基础性安全教育培训的次数	
上年度参加基础性安全教育培训的人数	

三、安全事件及安全防护情况		
序号	安全事件调查	调查结果
1	是否发生过网络安全事件	□没有 □1次/年 □2次/年 □3次/年 □3次以上/年
2	发生的网络安全事件类型（多选）	□感染病毒/蠕虫/特洛伊木马程序 □拒绝服务攻击 □端口扫描攻击 □数据窃取 □破坏数据或网络 □篡改网页

		□垃圾邮件 □内部人员有意破坏 □内部人员滥用网络端口、系统资源 □被利用发送和传播有害信息 □网络诈骗和盗窃 □其他，其他说明
3	如何发现网络安全事件（多选）	□网络（系统）管理员工作检测发现 ❹通过事后分析发现 ❹通过安全产品发现 □有关部门通知或意外发现 ❹他人告知 □其他
4	网络安全事件造成损失评估	□非常严重，影响的信息系统有 □严重，影响的信息系统有 □一般，影响的信息系统有 □比较轻微，影响的信息系统有 □轻微，影响的信息系统有 □无法估计
5	可能的攻击来源	□内部 □外部 □都有 □病毒 □不清楚 ❹其他原因
6	导致发生网络安全事件的可能原因	□未修补或防范软件漏洞 □网络或软件配置错误 □登录密码过于简单或未修改 □缺少访问控制 □攻击者使用拒绝服务攻击 ❹攻击者利用软件默认设置 ❹利用内部用户安全管理漏洞或内部人员作案 ❹内部网络违规连接互联网 □攻击者使用欺诈方法 ❹其他
7	是否发生过硬件故障	□有 □无
8	是否发生过软件故障	□有 □无
9	是否发生过维护失误	□有 □无
10	是否发生过因用户操作失误引起的安全事件	❹有 □无
11	是否发生过物理设施/设备被破坏	□有 □无

12	网络安全防护	□防火墙 □web应用防火墙 □入侵检测设备 □入侵防御设备 □抗拒绝服务攻击设备 □安全审计设备 □防病毒网关 □网闸 □其他
		安全防护配置： □使用默认配置 □根据需要配置
		网络访问日志： □留存日志 □未留存日志
13	漏洞修复情况	漏洞检测周期： □每月 □每季度 □每年 □不进行漏洞检测
		上年度自行发现漏洞数量 个 收到漏洞风险通报数量 个 其中已处置漏洞风险数量 个

四、数据安全核查情况			
序号	检查项	检查细节	检查结果
1	个人数据	是否针对个人信息和重要数据建立保护制度，如《用户信息安全管理规定》、《数据管理制度》、《敏感数据的管理制度》等其他管理制度	⭘是 ⭘否
2		看当前收集的用户信息，与最初的授权协议想比较，确认是否有超出用户授权范围或违反相关要求收集存储、使用的情况	⭘是 ⭘否
3		确认数据的存储范围，核查该范围是否在用户授权范围内	⭘是 ⭘否
4		确认数据的使用范围，核查该范围是否在用户授权范围内	⭘是 ⭘否
5	数据完整性	查看主要设备、系统在数据传输过程中是否使用(HASH、M5等算法)进行完整性保护	⭘是 ⭘否
6		查看主要设备、系统在数据存储过程中是否使用(HAS、MD5等算法)进行完整性保护	⭘是 ⭘否

五、安全管理核查情况			
5.1 安全管理机构与人员			
序号	检查项	检查细节	检查结果

1	授权和审批	查看审批流程文档，内容是否包括系统变更、重要操作、物理访问和系统接入等事项	□是 □否
2		查看审批文档，内容是否包含了更新的信息	□是 □否
3		查看具体的审批文档，内容是否包含了详细审批过程	□是 □否
4	审核和检查	查看安全管理员安全检查的内容记录和结果文档，查看是否覆盖了系统运行相关的管理活动	□是 □否
5		检查安全检查记录，是否保存完善	□是 □否
6	重点岗位人员录用和审查	是否为与信息安全密切相关的重点、敏感岗位人员制定特殊的录用要求，对被录用人员的身份、背景和专业资格进行审查	□是 □否
7		是否对技术人员的技术技能进行考核	□是 □否
8		是否有严格的考核制度	□是 □否
9	保密协议	是否与从事关键岗位的人员签署保密协议	□是 □否
10	人员考核	是否定期对相关人员进行安全技能和安全知识的考核	□是 ◉否
11	安全意识教育	是否根据岗位要求进行有针对性的信息安全意识培训	□是 □否
12		是否有培训记录	□是 ◉否
13	安全技能培训	是否制定有针对性的安全技能培训	□是 □否
14		是否有培训记录	□是 □否
15	外部人员管理	外部人员访问受控区域是否得到授权和审批	□是 □否
16		是否有专人全程陪同	□是 □否
17	与外部组织沟通合作	是否与外部组织建立沟通合作机制	□是 ◉否
18		是否有正式的文件和程序	□是 □否
5.2 安全管理制度			
序号	检查项	检查细节	检查结果
1	制定和发布	管理制度是否由部门或专人负责制定	□是 □否

2		查看安全管理制度文档是否采用统一的文档格式	□是 □否
3		查看审批记录，安全管理制度是否报送相关管理人员进行审批	□是 □否
4	评审和修订	信息安全管理机构对安全管理制度的审定记录是否完整	□是 □否
5		信息安全管理机构对安全管理制度的修订记录是否完整	□是 ◉否
5.3 安全运维管理			
序号	检查项	检查细节	检查结果
1	环境管理	是否有机房安全管理制度	□是 ◉否
2		是否配备了专门机房安全管理员，对机房供配电等设施、设备和人员出入进行严格管理	□是 □否
3		是否有完整的设备和人员的出入登录记录	□是 □否
4	网络安全管理	是否有网络设备更新记录	□是 □否
5	系统安全管理	系统补丁是否更新及时，并在测试环境测试后安装到正式环境中	□是 □否
6		系统正式运行后，每年是否进行过风险评估	□是 □否
7	恶意代码防范管理	查看当前防病毒软件版本是否为最新	□是 □否
8		查看当前病毒库是否为最新	□是 □否
9		查看相关策略是否对外来移动介质进行查杀和病毒检测	□是 ◉否
10		是否有各类防病毒、恶意代码软件更新记录及病毒分析处理报告	□是 ◉否
5.4 日常检测管理			
序号	检查项	检查细节	检查结果
1	安全监测	是否有通信线路、主机、网络设备、应用软件运行状况、网络流量、用户行为的监测、报警记录	□是 □否
2		是否有监测、报警记录分析报告	□是 □否
3		查看是否建立安全管理中心，对相关安全事项进行集中管理	□是 □否
4	日志分析	查看网络日志，保存周期是否大	□是

		于6个月	⭘否
5		查看日志分析记录，是否确保有专人对日志进行审计并形成报告	□是 ⭘否
6	威胁检测	是否对网络威胁进行监测，开展网络安全态势分析	□是 □否
7		是否有固定、周期性的网络安全威胁信息来源	□是 □否
8		是否能够在知悉新出现的威胁后迅速部署监测策略	□是 □否
5.5 备份恢复管理			
序号	检查项	检查细节	检查结果
1	备份	是否根据数据的重要性及其对系统运行的影响，制定相应的灾难备份和恢复管理策略	□是 □否
2		查看关键设备、系统的备份策略及备份文件，是否与策略一致	□是 □否
3		查看关键设备、系统的异地备份策略及备份结果，是否与策略一致	□是 □否
4	恢复	是否定期查看备份数据的可用性	□是 □否
5		查看恢复测试记录，是否确保定期对备份数据进行恢复测试	□是 □否
6		是否收到上级主管单位下发的安全事件通报和威胁情报	□是 □否
7		针对安全事件或应急演练，是否启用了备份与恢复手段保障业务正常运行	□是 □否
5.6 安全应急管理			
序号	检查项	检查细节	检查结果
1	应急响应组织机构和应急资源	是否成立应急响应组织，明确成员的职责、分工和责任追究	□是 □否
2		是否在人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障	□是 ⭘否
3	应急预案	是否有统一应急预案框架	□是 □否
4		在应急预案框架下，是否针对多种(五种以上)网络安全事件的应急预案	□是 □否
5		查看恢复测试记录，是否确保定期对备份数据进行恢复测试	□是 □否
6		是否收到上级主管单位下发的	□是

		安全事件通报和威胁情报	□否
7	应急演练	是否根据数据的重要性及其对系统运行的影响，制定相应的灾难备份和恢复管理策略	□是 □否
8		查看关键设备、系统的备份策略及备份文件，是否与策略一致	□是 □否
9		查看关键设备、系统的异地备份策略及备份结果，是否与策略一致	□是 □否
10		是否定期查看备份数据的可用性	□是 □否
11		查看恢复测试记录，是否确保定期对备份数据进行恢复测试	□是 □否
5.7 安全整改管理			
1.是否有主管部门的检查结果		□是 □否	
2.是否有被检查信息的信息安全风险评估报告		□是 □否	
3.以往安全检查和风险评估中是否发现问题？		□是 □否	
4.发现的安全问题个数： 个。			
5.是否已经进行整改？		□是 □否	
6.是否有主管部门或安全机构通报的整改报告？		□是 □否	
7.已经整改的安全问题个数： 个，未整改安全问题个数： 个。			

被检查单位负责人签字（盖章）： 检查人员签字：

附件四：《安全服务授权书》

安全服务授权书

甲方：

乙方：

甲方委托乙方对甲方的进行服务。

为确保服务的顺利进行，并保证甲方系统、应用及网络的稳定性和数据的安全性，甲乙双方就下述事宜达成一致，特制订本协议。

详细信息如下：

工作任务	授权乙方项目组对提供服务
工作时间	
工作对象	
工作地点	
实施人员	
甲方监督人员	
资产对象	
备注：	

第六章 磋商响应文件格式

正/副本

政府采购项目

项 目 编 号：

2025年大荔县网络安全检查技术服务项目

磋商响应文件

供 应 商：_____（盖章）

法定代表人：_____（签字或盖章）

日 期：_____ 年_____ 月_____日

目 录

一、磋商申请函

二、报价表

三、法定代表人身份证明书

四、法定代表人授权委托书

五、技术方案

六、本项目拟投入人员汇总表

七、业绩

八、供应商资格证明文件

九、供应商承诺书

十、政府采购供应商拒绝政府采购领域商业贿赂承诺书

十一、中小企业声明函

十二、残疾人福利性单位声明函（如有）

十三、监狱企业相关资格证明材料（如有）

一、磋 商 申 请 函

致：中国共产党大荔县委员会宣传部：

1、根据已收到的项目编号为 HWDL2025013 的2025年大荔县网络安全检查技术服务项目的竞争性磋商文件，遵照《中华人民共和国政府采购法》的规定，我单位经研究竞争性磋商文件的磋商须知、合同条款、采购内容及要求及其他有关文件后，我方愿按上述要求提供服务。

2、我方已详细审核全部竞争性磋商文件，包括修改文件（如有时）及有关附件。

3、我方提交的磋商响应文件为：正本1份，副本2份，电子文件1份。

4、一旦我方成交，我方保证项目服务期_____，服务质量_____ 。

5、按竞争性磋商文件的规定，我公司磋商总价为人民币（大写）：_____（小写）¥：_____元。

6、我方同意所提交的磋商响应文件的磋商有效期90日历天（从递交竞争性磋商响应文件的截止之日起）内有效，在此期间内我方的磋商有可能成交，我方将受此约束。

7、除非另外达成协议并生效，你方的成交通知书和本磋商响应文件将成为约束我们双方的合同文件的组成部分。

供应商：_____（盖章）

单位地址：_____

法定代表人：_____（签字或盖章）

日　期：_____年____月____日

商务要求响应表

序号	名称	磋商文件商务要求	响应文件 （响应/不响应）	响应说明
1	服务期	15日历天		
2	质量标准	达到合格标准及第五章“采购内容及要求”。		
3	付款方式	合同签订后付款70%，履约验收合格后付款至100%。		
4	合同条款	磋商文件第四章		
5	商务要求	磋商文件第五章		
	……			

注：

1.响应说明填写：若优于磋商要求的内容具体填写。

2.表格不够用，各供应商可按此表复制。

供　应　商：_____（公章）

法定代表人或被授权委托人：_____（签字或盖章）

日　　期：_____年_____月_____日

二、报 价 表

2.1 第一次报价表

标段名称及编号	标段名称：2025年大荔县网络安全检查技术服务项目 项目编号：HWDL2025013
第一次报价	磋商总报价：人民币小写： 人民币大写：
服务期	
质量标准	达到合格标准及第五章“采购内容及要求”
备 注	

注：1、报价应是磋商文件所确定的磋商范围内的全部工作内容的价格体现。

2、报价包括但不限于项目人工费、机械费、验收费、管理费、税金、利润、磋商文件明示及暗示所有风险等所有费用，服务期内采购人不再增加任何费用。

3、供应商应充分考虑项目实施期间市场风险和政策性调整确定风险系数进行报价。

供 应 商：_____（公章）

法定代表人或被授权委托人：_____（签字或盖章）

日 期：_____年_____月_____日

分项报价表

（自拟）

2.2 最终磋商书面报价表

标段名称及编号	标段名称：2025年大荔县网络安全检查技术服务项目 项目编号：HWDL2025013
最终磋商书面报价	磋商总报价：人民币小写： 人民币大写：
服务期	
质量标准	达到合格标准及第五章“采购内容及要求”
备 注	

注：

1、报价应包括磋商文件所确定的磋商范围内的全部费用。

2、本表格式不得自行改动，无需附在磋商响应文件中。

3、最终报价采用此表格式，名称为“最终磋商书面报价表”，无须与磋商响应文件共同装订成册，但作为磋商响应文件的组成部分。

4、“最终磋商书面报价表”中的相关内容及日期磋商现场手填。

供 应 商：_____（公章）

法定代表人或被授权委托人：_____（签字或盖章）

日 期：_____年_____月_____日

三、法定代表人身份证明书

单位名称：_____

单位性质：_____

地　　址：_____

成立时间：_____年_____月_____日

经营期限：_____

姓　　名：_____ 性别：_____年龄：_____ 职务：_____

系_____（供应商名称）的法定代表人。

特此证明。

供应商：_____（盖章）

日　期：_____年_____月_____日

附：法定代表人身份证复印件（正、反两面）

四、法定代表人授权委托书

本授权委托书声明：我_____（姓名）系_____（供应商名称）的法定代表人，现授权委托_____（姓名）为我公司签署本项目的磋商响应文件的代理人，以本公司的名义参加___2025年大荔县网络安全检查技术服务项目___的磋商活动。代理人在磋商过程中所签署的一切文件和处理与之有关的一切事务，我均予以承认。

代理人无转委托权，特此委托。

委托期限：自磋商响应文件递交截止之日起90日历天

法定代表人（签字或盖章）：_____ 被授权人（签字）：_____

职　　务：_____ 职　　务：_____

身份证号：_____ 身份证号：_____

附：1、法定代表人身份证复印件（正、反两面）

2、代理人的身份证复印件（正、反两面）

供　应　商：_____（公章）

日　　期：_____年_____月_____日

五、技术方案

供应商应根据磋商文件要求的内容和顺序，采用文字并结合图表形式，对完成整个项目提出相应的技术方案。应包括但不限于以下内容：

（一）总体方案

（二）网络安全检查评估方案

（三）保障措施

（四）资料汇总整理方案

（五）团队人员配备

包括但不限于以上内容，供应商根据本项目实际情况以及磋商文件打分要求进行编写，格式自拟。

六、本项目拟投入人员汇总表

序号	姓　名	性别	年龄	工作年限	拟担任的职务	职称

注：1.供应商可适当调整该表格式，但不得减少信息内容。

2.提供人员证明信息（包括但不限于职称证或执业证、身份证、毕业证等）

供　应　商：_____（公章）

法定代表人或被授权委托人：_____（签字或盖章）

日　　期：_____年_____月_____日

项目负责人简历表

姓名		性别		年龄		学位		身份证号码	
职称		服务时间（年）			在本合同中拟任职			
学历	年毕业于 （学校） （专业）							
2. 经历								
时间	负责过的主要项目（类型和金额）					该项目中任职		备注

此表后附项目负责人的相关证书等复印件加盖供应商公章。

七、业绩

八、供应商资格证明文件

（一）供应商基本资格条件：满足《中华人民共和国政府采购法》第二十二条规定，需提供以下证明资料：

1.供应商应具有独立承担民事责任的能力且具备向采购人提供相关服务的企业法人、事业法人、其他组织或者自然人，企业法人应提供统一社会信用代码的营业执照；事业法人应提供统一社会信用代码的事业单位法人证；其他组织应提供合法证明文件；自然人应提供身份证明文件；

2.具有良好的商业信誉和健全的财务会计制度以及有依法缴纳税收和社会保障资金的良好记录；

①财务状况报告：提供具有财务审计资质单位出具的2023或2024年度财务审计报告（成立时间至磋商时间不足一年的可提供成立后任意时段的资产负债表）或响应文件递交截止时间前六个月内其基本账户银行出具的资信证明（附基本账户证明）或政府采购信用担保机构出具的磋商担保函；

②税收缴纳证明：提供响应文件递交截止时间前一年内任意一个月的缴费凭据（依法免税的供应商应提供相关文件证明）；

③社会保障资金缴纳证明：提供响应文件递交截止时间前一年内任意一个月的社保缴费凭据或社保机构开具的社会保险参保缴费情况证明（依法不需要缴纳社会保障资金的供应商应提供相关证明）；

3.提供具有履行本合同所必需的设备和专业技术能力的说明或承诺；（格式自拟，加盖供应商公章）

4.提供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的书面声明；（格式自拟，加盖供应商公章）

（二）供应商特定资格要求，需提供以下资格证明资料：

（1）法定代表人授权书（附法定代表人、被授权人身份证复印件）及被授权人身份证（法定代表人直接参加磋商，须提供法定代表人身份证明及身份证）；

（2）供应商不得为“信用中国”网站（www.creditchina.gov.cn ）中列入失信被执行人和重大税收失信主体的供应商，不得为中国政府采购网（www.ccgp.gov.cn）政府

采购严重违法失信行为记录名单中被财政部门禁止参加政府采购活动的供应商；

（3）单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得同时参加同一合同项下的政府采购活动。

九、供应商承诺书

致_____（采购人）：

作为参加贵单位组织的 _____（项目名称）的磋商供应商，本公司郑重承诺：

1、在参加本项目磋商之前不存在被依法禁止经营行为、财产被接管或冻结的情况，如有隐瞒实情，愿承担一切责任及后果。

2、近三年受到有关行政主管部门的行政处理、**不良行为记录为___次**（没有填**零**），如有隐瞒实情，愿承担一切责任及后果。

3、参加本次磋商提交的所有资格证明文件是真实的、有效的，如有隐瞒实情，愿承担一切责任及后果。

4、我方已阅读了《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》文件，并领会了文件的精神。因违反文件规定所产生的后果由我方自行承担。

供　应　商：_____（公　　章）

法定代表人或被授权委托人：_____（签字或盖章）

日　　期：_____年_____月_____日

十、政府采购供应商拒绝政府采购领域商业贿赂承诺书

为响应党中央、国务院关于治理政府采购领域商业贿赂行为的号召，我单位在此庄严承诺：

1、在参与政府采购活动中遵纪守法、诚信经营、公平竞标。

2、不向采购人、采购代理机构和政府采购磋商小组进行任何形式的商业贿赂以谋取交易机会。

3、不向采购代理机构和采购人提供虚假资格文件或采用虚假应标方式参与政府采购市场竞争并谋取中标、成交。

4、不采取“围标、陪标”等商业欺诈手段获得政府采购定单。

5、不采取不正当手段低毁、排挤其他供应商。

6、不在提供商品和服务时“偷梁换柱、以次充好”损害采购人的合法权益。

7、不与采购人、采购代理机构、政府采购磋商小组或其它供应商恶意串通，进行质疑和投诉，维护政府采购市场秩序。

8、尊重和接受政府采购监督管理部门的监督和采购代理机构的磋商要求，承担因违约行为给采购人造成的损失。

9、不发生其他有悖于政府采购公开、公平、公正和诚信原则的行为。

承诺单位：_____（公　　章）

法定代表人或被授权委托人：_____（签字或盖章）

地　　址：_____

邮　　编：_____

电　　话：_____

日　　期：_____年_____月_____日

十一、中小企业声明函

本公司郑重声明，根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）的规定，本公司参加**（单位名称）**的**（标段名称 ）**采购活动，提供的服务全部由符合政策要求的中小企业承接。相关企业的具体情况如下：

1. **（标段名称 ）**，属于**（ 其他未列明行业）**行业；承接企业为 （企业名称），从业人员___人，营业收入为____万元，资产总额为____万元， 属于_____（中型企业、小型企业、微型企业）；

2. （**标段名称 ）**，属于**（磋商文件中明确的所属行业）**行业；承接企业为（企业名称），从业人员____人，营业收入为_____万元，资产总额为_____万元，属于____（中型企业、小型企业、微型企业）；

……

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报。

企业名称（盖章）：_____

日　　期：_____

十二、残疾人福利性单位声明函（如有）

本单位郑重声明，根据《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） 的规定，本单位为符合条件的残疾人福利性单位，且本单位参加 （采购人） 单位的 项目采购活动提供本单位制造的货物(由本单位承担工程/提供服务），或者提供其他残疾人福利性单位制造的货物(不包括使用非残疾人福利性单位注册商标的货物）。

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

单位名称（盖章）：_____

日　　期：_____

十三、监狱企业相关资格证明材料（如有）

附件一：

具有良好的商业信誉和健全的财务会计制度以及有依法缴纳税收和社会保障资金的良好记录承诺

致：(采购人)

作为参加贵单位组织的（项目名称）的供应商，本公司郑重承诺:

1.我公司具有独立承担民事责任的能力；

2.我公司具有良好的商业信誉和健全的财务会计制度；

3.我公司有依法缴纳税收和社会保障资金的良好记录；

4.在参加本项目磋商之前不存在被依法禁止经营行为、财产被接管或冻结的情况，如有隐瞒实情，愿承担一切责任及后果；

5.近三年受到有关行政主管部门的行政处理、不良行为记录为__ 次(没有填零)，如有隐瞒实情，愿承担一切责任及后果。

6.参加本次磋商提交的所有资格证明文件是真实的、有效的，如有隐瞒实情，愿承担一切责任及后果。

7.我方已阅读了(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一财库(2016）125号)文件，并领会了文件的精神。因违反文件规定所产生的后果由我方自行承担。

企业名称（盖章）：

日期：

附件二：

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

各省、自治区、直辖市人民政府，国务院各部委、各直属机构及有关单位：

为贯彻落实《中华人民共和国中小企业促进法》和《国务院关于进一步促进中小企业发展的若干意见》（国发〔2009〕36号），工业和信息化部、国家统计局、发展改革委、财政部研究制定了《中小企业划型标准规定》。经国务院同意，现印发给你们，请遵照执行。

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

二〇一一年六月十八日

中小企业划型标准规定

一、根据《中华人民共和国中小企业促进法》和《国务院关于进一步促进中小企业发展的若干意见》(国发〔2009〕36号），制定本规定。

二、中小企业划分为中型、小型、微型三种类型，具体标准根据企业从业人员、营业收入、资产总额等指标，结合行业特点制定。

三、本规定适用的行业包括：农、林、牧、渔业，工业（包括采矿业，制造业，电力、热力、燃气及水生产和供应业），建筑业，批发业，零售业，交通运输业（不含铁路运输业），仓储业，邮政业，住宿业，餐饮业，信息传输业（包括电信、互联网和相关服务），软件和信息技术服务业，房地产开发经营，物业管理，租赁和商务服务业，租赁与商务服务业（包括科学研究和技术服务业，水利、环境和公共设施管理业，居民

服务、修理和其他服务业，社会工作，文化、体育和娱乐业等）。

四、各行业划型标准为：

（一）农、林、牧、渔业。营业收入20000万元以下的为中小微型企业。其中，营业收入500万元及以上的为中型企业，营业收入50万元及以上的为小型企业，营业收入50万元以下的为微型企业。

（二）工业。从业人员1000人以下或营业收入40000万元以下的为中小微型企业。其中，从业人员300人及以上，且营业收入2000万元及以上的为中型企业；从业人员20人及以上，且营业收入300万元及以上的为小型企业；从业人员20人以下或营业收入300万元以下的为微型企业。

（三）建筑业。营业收入80000万元以下或资产总额80000万元以下的为中小微型企业。其中，营业收入6000万元及以上，且资产总额5000万元及以上的为中型企业；营业收入300万元及以上，且资产总额300万元及以上的为小型企业；营业收入300万元以下或资产总额300万元以下的为微型企业。

（四）批发业。从业人员200人以下或营业收入40000万元以下的为中小微型企业。其中，从业人员20人及以上，且营业收入5000万元及以上的为中型企业；从业人员5人及以上，且营业收入1000万元及以上的为小型企业；从业人员5人以下或营业收入1000万元以下的为微型企业。

（五）零售业。从业人员300人以下或营业收入20000万元以下的为中小微型企业。其中，从业人员50人及以上，且营业收入500万元及以上的为中型企业；从业人员10人及以上，且营业收入100万元及以上的为小型企业；从业人员10人以下或营业收入100万元以下的为微型企业。

（六）交通运输业。从业人员1000人以下或营业收入30000万元以下的为中小微型企业。其中，从业人员300人及以上，且营业收入3000万元及以上的为中型企业；从业人员20人及以上，且营业收入200万元及以上的为小型企业；从业人员20人以下或营业收入200万元以下的为微型企业。

（七）仓储业。从业人员200人以下或营业收入30000万元以下的为中小微型企业。其中，从业人员100人及以上，且营业收入1000万元及以上的为中型企业；从业人员20人及以上，且营业收入100万元及以上的为小型企业；从业人员20人以下或营业收入100万元以下的为微型企业。

（八）邮政业。从业人员1000人以下或营业收入30000万元以下的为中小微型企业。其中，从业人员300人及以上，且营业收入2000万元及以上的为中型企业；从业人员20人及以上，且营业收入100万元及以上的为小型企业；从业人员20人以下或营业收入100万元以下的为微型企业。

（九）住宿业。从业人员300人以下或营业收入10000万元以下的为中小微型企业。其中，从业人员100人及以上，且营业收入2000万元及以上的为中型企业；从业人员10人及以上，且营业收入100万元及以上的为小型企业；从业人员10人以下或营业收入100万元以下的为微型企业。

（十）餐饮业。从业人员300人以下或营业收入10000万元以下的为中小微型企业。其中，从业人员100人及以上，且营业收入2000万元及以上的为中型企业；从业人员10人及以上，且营业收入100万元及以上的为小型企业；从业人员10人以下或营业收入100万元以下的为微型企业。

（十一）信息传输业。从业人员2000人以下或营业收入100000万元以下的为中小微型企业。其中，从业人员100人及以上，且营业收入1000万元及以上的为中型企业；从业人员10人及以上，且营业收入100万元及以上的为小型企业；从业人员10人以下或营业收入100万元以下的为微型企业。

（十二）软件和信息技术服务业。从业人员300人以下或营业收入10000万元以下的为中小微型企业。其中，从业人员100人及以上，且营业收入1000万元及以上的为中型企业；从业人员10人及以上，且营业收入50万元及以上的为小型企业；从业人员10人以下或营业收入50万元以下的为微型企业。

（十三）房地产开发经营。营业收入200000万元以下或资产总额10000万元以下

的为中小微型企业。其中，营业收入1000万元及以上，且资产总额5000万元及以上的为中型企业；营业收入100万元及以上，且资产总额2000万元及以上的为小型企业；营业收入100万元以下或资产总额2000万元以下的为微型企业。

（十四）物业管理。从业人员1000人以下或营业收入5000万元以下的为中小微型企业。其中，从业人员300人及以上，且营业收入1000万元及以上的为中型企业；从业人员100人及以上，且营业收入500万元及以上的为小型企业；从业人员100人以下或营业收入500万元以下的为微型企业。

（十五）租赁和商务服务业。从业人员300人以下或资产总额120000万元以下的为中小微型企业。其中，从业人员100人及以上，且资产总额8000万元及以上的为中型企业；从业人员10人及以上，且资产总额100万元及以上的为小型企业；从业人员10人以下或资产总额100万元以下的为微型企业。

（十六）其他未列明行业。从业人员300人以下的为中小微型企业。其中，从业人员100人及以上的为中型企业；从业人员10人及以上的为小型企业；从业人员10人以下的为微型企业。

五、企业类型的划分以统计部门的统计数据为依据。

六、本规定适用于在中华人民共和国境内依法设立的各类所有制和各种组织形式的企业。个体工商户和本规定以外的行业，参照本规定进行划型。

七、本规定的中型企业标准上限即为大型企业标准的下限，国家统计部门据此制定大中小微型企业的统计分类。国务院有关部门据此进行相关数据分析，不得制定与本规定不一致的企业划型标准。

八、本规定由工业和信息化部、国家统计局会同有关部门根据《国民经济行业分类》修订情况和企业发展变化情况适时修订。

九、本规定由工业和信息化部、国家统计局会同有关部门负责解释。

十、本规定自发布之日起执行，原国家经贸委、原国家计委、财政部和国家统计局2003年颁布的《中小企业标准暂行规定》同时废止。

附件三：

温馨提示

为不断深化“放管服”改革，提升行政服务效能，优化政府采购营商环境，积极不断发挥政府采购政策功能作用，有效缓解中小企业融资难、融资贵问题，根据陕西省财政厅《陕西省中小企业政府采购信用融资办法》（陕财办采〔2018〕23号）、《陕西省财政厅关于加快推进我省中小企业政府采购信用融资工作的通知》（陕财办采〔2020〕15 号）等有关文件精神，渭南市政府采购项目已全面推行中小企业政府采购信用融资工作，该政策能够有效帮助政府采购中标（成交）企业依托政采项目开展融资服务，进一步解决中小微企业“融资难、融资贵”问题。

“政府采购信用融资”是指银行业金融机构（以下简称银行）以政府采购诚信考核和信用审查为基础，凭借政府采购合同，按优于一般中小企业的贷款利率直接向申请贷款的供应商发放贷款的一种融资方式。政府采购信用融资坚持“财政引导，市场运行，银企自愿，互惠共赢”的原则。银行为参与政府采购融资的中小企业提供的产品，以信用贷款为主，贷款利率优于一般中小企业的贷款利率水平，相关产品信息（包括贷款发放条件、利率优惠、贷款金额）等将在陕西政府采购网予以展示。中小企业可根据各银行提供的方案，自行选择符合自身情况的金融产品，并根据方案中列明的联系方式和要求向相关银行提出信用融资申请。银行根据中小企业的申请开展尽职调查，合理确定融资授信额度。中小企业获得政府采购合同后，凭政府采购合同向银行提出融资申请。

本项目中标（成交）供应商，有融资需求的供应商可根据自身情况，在“陕西政府采购信用融资平台（含各市分平台）”查询并办理相关业务。具体供应商融资申请操作手册可登录以下网址查询：http：
//www.ccgp-shaanxi.gov.cn/zcdservice/zcd/shanxi/article/bzsc/127

附件：渭南市信用融资合作银行联系名单

渭南市信用融资合作银行联系名单

序号	银行名称	联系人	联系电话
1	建设银行	田宇	17797059890
2	浦发银行	孙哲龙 蒙波	13892383911 15249035320
3	中信银行	杨洋 耿浩	18191815559 13193388328
4	兴业银行	权奥星	15706090239
5	工商银行	张剑 张欢	18191356300 15229730006
6	长安银行	李华	13335331958
7	邮储银行	张萱	13028431555 18091365182

注：成交供应商如需在渭南市办理融资贷款服务的，可联系以上任意一家银行申请办理相关业务。