**国家税务总局天津市税务局安全运营、等保测评、密码应用安全性评估和密码应用安全服务项目**

**招标文件**

（项目编号：TGPC-2024-D-0312）

天津市政府采购中心

**2024.5**

**目 录**

**第一部分 投标邀请函**

**第二部分 招标项目要求**

**第三部分 投标须知**

**第四部分 合同条款**

**第五部分 投标文件格式**

第一部分 投标邀请函

受国家税务总局天津市税务局委托，天津市政府采购中心将以公开招标方式，对国家税务总局天津市税务局安全运营、等保测评、密码应用安全性评估和密码应用安全服务项目实施政府采购。现欢迎合格的供应商参加投标。

本项目为远程招投标，一律不接受纸质投标文件，只接受加盖投标人电子签章的PDF格式电子投标文件（以通过天津公共资源电子签章客户端正确读取签章信息为准）。供应商参加投标前须办理CA数字证书（USBKEY）和电子签章。投标人须按招标文件的规定在天津市政府采购中心招投标系统中提交网上应答并上传加盖投标人电子签章的PDF格式电子投标文件（以通过天津公共资源电子签章客户端正确读取签章信息为准）。

一、项目名称和编号

（一）项目名称：国家税务总局天津市税务局安全运营、等保测评、密码应用安全性评估和密码应用安全服务项目

（二）项目编号：TGPC-2024-D-0312

二、项目内容

第一包：2024年安全运营服务，合同履行期限：自合同签订之日起一年（特殊情况以合同为准）；

第二包：2024年等保测评服务，合同履行期限：合同签订之日至2024年12月31日；

第三包：2024年密码应用安全性评估服务，合同履行期限：合同签订之日至2024年12月31日；

第四包：2024年密码应用安全服务，合同履行期限：自合同签订之日起三年（特殊情况以合同为准）。

三、项目预算

第一包：4049600元；

第二包：1121000元；

第三包：1050000元；

第四包：2105000元。

四、供应商资格要求（实质性要求）

（一）根据《商用密码应用安全性评估管理办法》的规定，第三包投标人应为国家密码管理部门认定的密码评测机构，列入国家密码管理局公告（第42号）机构目录之内。

（二）投标人须具备《中华人民共和国政府采购法》第二十二条第一款规定的条件，提供以下材料：

1. 营业执照副本或事业单位法人证书或民办非企业单位登记证书或社会团体法人登记证书或基金会法人登记证书扫描件或自然人的身份证明扫描件。

2. 财务状况报告等相关材料：

A.经第三方会计师事务所审计的2022年度或2023年度财务报告扫描件。

B. 具有良好的商业信誉和健全的财务会计制度的书面声明。

注：A、B两项提供任意一项均可。

3. 依法缴纳税收和社会保障资金的书面声明。

4. 投标截止日前3年在经营活动中没有重大违法记录的书面声明（截至开标日成立不足3年的供应商可提供自成立以来无重大违法记录的书面声明）。

5. 提交具备履行合同所必需的设备和专业技术能力证明材料。

（三）本项目不接受联合体投标。

（四）本项目第二包专门面向中小企业采购，提供《中小企业声明函》。

五、项目需要落实的政府采购政策

（一）本项目第二包专门面向中小企业采购，第一包、第三包、第四包对小微企业报价给予20%的扣除。

（二）根据财政部发布的《关于政府采购支持监狱企业发展有关问题的通知》规定，监狱企业视同小微企业。

（三）根据财政部、民政部、中国残疾人联合会发布的《关于促进残疾人就业政府采购政策的通知》规定，残疾人福利性单位视同小微企业。

注：中小微企业以投标人填写的《中小企业声明函》为判定标准，残疾人福利性单位以投标人填写的《残疾人福利性单位声明函》为判定标准，监狱企业须投标人提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件，否则不予认定。以上政策不重复享受。

（四）涉及商品包装或快递包装的，按照《财政部办公厅、生态环境部办公厅、国家邮政局办公室关于印发<商品包装政府采购需求标准（试行）>、<快递包装政府采购需求标准（试行）>的通知》（财办库〔2020〕123号）要求执行。

（五）按照《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）的要求，根据开标当日解密截止时间“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）的信息，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，拒绝参与政府采购活动，同时对信用信息查询记录和证据进行打印存档。

六、获取招标文件时间、方式

（一）获取招标文件时间：2024年5月21日至2024年5月28日，每日9:00至17:00（北京时间，法定节假日除外）。

（二）获取招标文件的方式：

1. 获取招标文件网址：使用天津数字认证有限公司发出的CA数字证书（原天津市电子认证中心发出尚在有效期内的CA数字证书仍可使用）登录天津市政府采购中心网（网址：[http://tjgpc.zwfwb.tj.gov.cn](http://www.tjgpc.gov.cn)）-“网上招投标”-“供应商登录”-“市级集采机构入口”下载招标文件。

2. 供应商注册、CA数字证书（USBKey）领取、电子签章办理办法：

（1）天津市政府采购中心网注册：登录天津市政府采购中心网（http://tjgpc.zwfwb.tj.gov.cn）首页点击“供应商注册”，填写相关内容。天津市政府采购中心注册窗口联系电话：022-24538316。

（2）CA数字证书（USBKey）领取及电子签章办理：参见天津市政府采购中心网（http://tjgpc.zwfwb.tj.gov.cn）--服务指南--供应商注册、领取CA数字证书（USBKey）及电子签章制章的流程。

CA数字证书办理联系电话：400-0566-110或022-24538059。

电子签章办理联系电话：022-24538059。

（三）本项目不组织踏勘现场，不组织标前答疑会。

七、网上应答时间

2024年5月21日9:00至2024年6月11日8:30，使用天津数字认证有限公司发出的CA数字证书（原天津市电子认证中心发出尚在有效期内的CA数字证书仍可使用）登陆天津市政府采购中心网（网址：http://tjgpc.zwfwb.tj.gov.cn）-“网上招投标”-“供应商登录”-“市级集采机构入口”进行应答并提交。

网上应答帮助链接：http://tjgpc.zwfwb.tj.gov.cn/webInfo/getWebInfoListForwebInfoClass.do?fkWebInfoclassId=W008

八、投标截止时间及方式

（一）投标截止时间：2024年6月11日8:30。投标截止时间前提交网上应答并上传加盖投标人电子签章的PDF格式电子投标文件（以通过天津公共资源电子签章客户端正确读取签章信息为准）方为有效投标。

（二）投标方式：本项目投标采用网上电子投标方式，投标人须于投标截止时间前使用天津数字认证有限公司发出的CA数字证书（原天津市电子认证中心发出尚在有效期内的CA数字证书仍可使用）登陆天津市政府采购中心网（网址：http://tjgpc.zwfwb.tj.gov.cn）-“网上招投标”-“供应商登录”-“市级集采机构入口”提交网上应答并上传加盖投标人电子签章的PDF格式电子投标文件（以通过天津公共资源电子签章客户端正确读取签章信息为准）。

九、开标时间及方式

（一）开标解密时间：2024年6月11日8:30至9:30完成开标解密的投标为有效投标。

（二）开标解密方式：本项目采用网上开标方式，投标人须于规定时间内使用天津数字认证有限公司发出的CA数字证书（原天津市电子认证中心发出尚在有效期内的CA数字证书仍可使用）登陆天津市政府采购中心网（网址：http://tjgpc.zwfwb.tj.gov.cn）-“网上招投标”-“供应商登录”-“市级集采机构入口”完成开标解密。

（三）网上开标公示时间：2024年6月11日9:30至12:00。投标人可在规定时间内使用天津数字认证有限公司发出的CA数字证书（原天津市电子认证中心发出尚在有效期内的CA数字证书仍可使用）登陆天津市政府采购中心网（网址：http://tjgpc.zwfwb.tj.gov.cn）-“网上招投标”-“供应商登录”-“市级集采机构入口”自行查看开标信息。

十、采购代理机构名称、地址、联系人及联系方式

（一）采购代理机构名称：天津市政府采购中心

（二）采购代理机构地址：天津市河东区红星路79号二楼（邮编：300161）

（三）联系人：郭晓刚、杨光、鲁志强

（四）网址：http://tjgpc.zwfwb.tj.gov.cn

（五）对外办公时间：法定工作日9:00～12:00，14:00～17:00

（六）咨询服务电话：

1. 供应商注册咨询：022-24538316

2. CA证书和电子签章办理咨询：022-24538059

3. 采购文件咨询：022-24538176

4. 网上应答及解密操作咨询：022-24538309

十一、采购人的名称、地址和联系方式

（一）采购人名称：国家税务总局天津市税务局

（二）采购人地址：天津市河北区民主道16号

（三）采购人联系人：张轲

（四）采购人联系电话：022-24465512

十二、质疑方式

（一）供应商认为采购文件、采购过程和采购结果使自己的权益受到损害的，可以在知道或者应知其权益受到损害之日起七个工作日内，按照本项目采购文件第三部分《投标须知》“8. 询问与质疑”的相关规定，以书面原件形式针对同一采购程序环节一次性提出质疑，否则不予受理。

采购人质疑受理：

1. 联系部门：国家税务总局天津市税务局

2. 联系地址：天津市河北区民主道16号

3. 联 系 人：张轲

4. 联系方式：022-24465512

（二）供应商对质疑答复不满意的，或者采购人、天津市政府采购中心未在规定期限内作出答复的，供应商可以在质疑答复期满后15个工作日内，向采购人同级财政部门提出投诉，逾期不予受理。

十三、公告期限

招标公告的公告期限为5个工作日。

十四、招标代理服务费

本项目按以下比例向中标供应商收取招标代理服务费：

| 中标金额（万元） | 费率 |
| --- | --- |
| 100以下 | 1% |
| 100-500 | 0.8% |
| 500-1000 | 0.45% |
| 1000-5000 | 0.25% |
| 5000-10000 | 0.1% |
| 10000-100000 | 0.05% |

服务费按差额定率累进法计算，向下取整，精确到元。例如中标金额为6805000元，服务费=1000000×1%+（5000000-1000000）×0.8%+（6805000-5000000）×0.45%=50122.5元，服务费缴纳50122元。其中中标金额以《中标通知书》为准。

中标供应商应于中标公告发布之日起5个工作日内缴纳招标代理服务费，缴费单位名称须与投标单位名称一致，缴费时请注明项目编号及中标包号。

名 称：天津市公共资源交易中心

开户行及账号：中国建设银行股份有限公司天津明华支行

1205 0162 4900 0000 0675

银行联行号：105110039436

纳税人识别号：1212 0000 MB1E 44809C

地址：天津市河东区红星路79号

缴费及申请开票系统：http://pay.tjggzy.cn/

缴费及开票咨询电话：022-24532012

2024年5月21日

第二部分 招标项目要求

★一、商务要求

（一）报价要求

1. 投标报价以人民币填列。

2. 投标人的报价应包括：人员费用、服务费用、测评费用、管理费及税金等为完成招标文件规定的一切工作所需的全部费用。投标人所报价格应为最终优惠价格。

3. 验收相关费用由投标人负责。

（二）服务要求

投标人提供详细的服务方案。

（三）时间、地点要求

1. 时间要求：第一包合同履行期限：自合同签订之日起一年（特殊情况以合同为准）；

第二包合同履行期限：合同签订之日至2024年12月31日（特殊情况以合同为准）；

第三包合同履行期限：合同签订之日至2024年12月31日（特殊情况以合同为准）；

第四包合同履行期限：自合同签订之日起三年（特殊情况以合同为准）。

2. 服务地点：采购人指定地点（特殊情况以合同为准）。

（四）付款方式

第一包：签订合同后支付合同总额的30%；项目中期验收合格后支付合同总额的40%；项目结束验收合格后支付合同总额的30%（特殊情况以合同为准）；

第二包：签订合同后支付合同总额的30%；测评结束后出具满足等网络安全等级保护技术指标要求，加盖测评机构印章的《信息安全等级保护测评报告》且备案通过，经验收合格后支付合同总额的70%（特殊情况以合同为准）；

第三包：签订合同后支付合同总额的30%；测评结束后出具满足商用密码应用指标要求，加盖测评机构印章的《密码应用安全评估报告》且备案通过，经验收合格后支付合同总额的70%（特殊情况以合同为准）；

第四包：签订合同后支付合同总额的25%；项目满一年阶段性验收合格后支付合同总额的25%；项目满两年阶段性验收合格后支付合同总额的25%；项目结束验收合格后支付合同总额的25%。

（五）投标保证金和履约保证金

本项目不收取投标保证金和履约保证金。

（六）验收方法及标准

按照采购合同的约定和现行国家标准、行业标准或企业标准对每一服务环节、安全标准的履约情况进行考核与验收。必要时，采购人有权邀请参加本项目的其他投标人或者第三方机构参与验收。参与验收的投标人或者第三方机构的意见作为验收书的参考资料一并存档。验收结束后，应当出具验收书，列明各项服务的考核验收情况及项目总体评价，由验收双方共同签署。

二、技术要求

★（一）投标人须承诺所提供的服务、人员及设备符合相关国家强制性规定。

（二）具体需求详见本部分项目需求书。

三、评分因素及评标标准

第一包：

|  |  |  |  |
| --- | --- | --- | --- |
| 第一部分 价格（10分） | | | 分值 |
| 1 | 价格 | （1）投标报价超过采购预算的，投标无效，未超过采购预算的投标报价按以下公式进行计算。  （2）投标报价得分=（评标基准价/投标报价）×10  注：满足招标文件要求且投标报价最低的投标报价为评标基准价。 | 10 |
| 第二部分 客观分（24分） | | | 分值 |
| 1 | 投标人业绩 | 完全按照以下要求提供投标人曾实施的信息系统安全服务业绩，提供的证明材料均不得遮挡涂黑，否则不予认定加分。  A. 合同原件扫描件。包括合同金额、买卖双方名称及盖章、服务内容（至少包含漏洞扫描、配置核查、渗透测试、日志分析、代码审计、开发安全、网站安全监测、外包服务、信息系统安全建设、风险评估、应急演练、攻防演习、应急响应、重要时期保障、网络安全规划、网络安全体系咨询、网络安全管理体系建设等中的任意一项）、合同签订日期（应为2021年1月1日或以后）。  B. 上述合同履行良好的相关证明材料原件扫描件（加盖上述合同甲方单位公章或上述合同中所盖的甲方印章或甲方验收证明材料）。  每个业绩2分，最多4分 | 4 |
| 2 | 投标人相关证书评价 | 投标人具备CNCERT国家互联网应急中心颁发的网络安全应急服务支撑单位（甲级）、《国家信息安全测评信息安全服务资质证书-安全开发类》（二级或以上）、中国网络安全审查技术与认证中心颁发的《数据安全管理认证证书》，提供证书扫描件，每个合格的证书扫描件得1分，最多3分； | 3 |
| 3 | 投入人员评价 | （1）项目经理具备计算机、网络安全、信息安全相关专业硕士（或以上）毕业证书，提供合格的证书扫描件：0.5分，其他0分；  （2）项目经理具备6年（或以上）信息安全服务项目实施经验，提供工作简历扫描件，满足以上要求的：0.5分，其他0分；  （3）驻场工程师具备注册信息安全专业人员（CISP）证书 、注册信息安全工程师（CISE）证书、信息安全保障人员（CISAW）证书或注册渗透测试工程师（CISP-PTE），提供以上任意一种合格的证书扫描件得1分，其他0分；  （4）攻防演习防守团队中的安全专家至少1人具备注册信息系统安全专家（CISSP）证书、注册渗透测试工程师（CISP-PTE）证书或注册渗透测试专家（CISP-PTS）证书，提供合格的证书扫描件：1分，其他0分；  （5）攻防演习防守团队中的高级安全工程师（不含安全专家）至少2人具备注册信息安全专业人员（CISP）证书、注册信息安全工程师（CISE）证书、注册渗透测试工程师（CISP-PTE）证书或注册渗透测试专家（CISP-PTS）证书，提供以上合格的证书扫描件，2名人员均具备以上任意一种证书的得1分，其他0分；  （6）应急支撑团队中应急服务人员不少于3人，具备注册信息安全专业人员（CISP）证书、注册信息安全工程师（CISE）证书、信息安全保障人员（CISAW）证书、注册渗透测试工程师（CISP-PTE）证书、注册渗透测试专家（CISP-PTS）证书，提供以上任意一种合格的证书扫描件得1分，其他0分；  （7）应急支撑团队中应急安全专家不少于2人，具备注册信息系统安全专家（CISSP）证书、注册渗透测试工程师（CISP-PTE）证书、注册渗透测试专家（CISP-PTS）证书，提供以上任意一种合格的证书扫描件得1分，其他0分；  注：除项目经理外，一人持多证不重复积分。 | 6 |
| 4 | 投标人承诺评价 | 承诺完全满足招标文件“报价要求”、“时间地点要求”、“付款方式要求”和技术要求中非“★”号要求的：11分，其他0分。 | 11 |
| 第三部分 主观分（66分） | | | 分值 |
| 1 | 日常运维服务方案评价 | 至少包含信息资产管理、安全管理监控、7\*24小时互联网预警监控、安全加固技术支持、配置策略优化、网络威胁数据分析、基线配置检查、网络拓扑梳理等方面内容  满足招标文件要求，无瑕疵：8分；  方案内容存在1处瑕疵：6分；  方案内容存在2处瑕疵：4分；  方案内容存在3处瑕疵：2分；  未提供方案或不满足招标文件要求或内容存在4处及以上瑕疵：0分；  （本项所称“瑕疵”是指内容缺项、不完整或缺少关键点；非专门针对本项目或不适用本项目特性、套用其他项目内容；对同一问题前后表述矛盾；存在逻辑漏洞、科学原理或常识错误；不利于本项目目标的实现、现有技术条件下不可能出现的情形等任意一种情形） | 8 |
| 2 | 互联网高危漏洞检测挖掘和众测服务和数据安全运营服务方案评价 | 至少包含互联网高危漏洞检测挖掘和众测服务、数据安全运营服务（含数据安全风险评估）等方面内容  满足招标文件要求，无瑕疵：8分；  方案内容存在1处瑕疵：6分；  方案内容存在2处瑕疵：4分；  方案内容存在3处瑕疵：2分；  未提供方案或不满足招标文件要求或内容存在4处及以上瑕疵：0分；  （本项所称“瑕疵”是指内容缺项、不完整或缺少关键点；非专门针对本项目或不适用本项目特性、套用其他项目内容；对同一问题前后表述矛盾；存在逻辑漏洞、科学原理或常识错误；不利于本项目目标的实现、现有技术条件下不可能出现的情形等任意一种情形） | 8 |
| 3 | SSL证书服务和CDN加速服务方案评价 | 至少包含SSL证书服务（1个二级域名证书，6个多域名的三级域名证书）和CDN加速服务等方面内容  满足招标文件要求，无瑕疵：8分；  方案内容存在1处瑕疵：6分；  方案内容存在2处瑕疵：4分；  方案内容存在3处瑕疵：2分；  未提供方案或不满足招标文件要求或内容存在4处及以上瑕疵：0分；  （本项所称“瑕疵”是指内容缺项、不完整或缺少关键点；非专门针对本项目或不适用本项目特性、套用其他项目内容；对同一问题前后表述矛盾；存在逻辑漏洞、科学原理或常识错误；不利于本项目目标的实现、现有技术条件下不可能出现的情形等任意一种情形） | 8 |
| 4 | 安全检测服务方案评价 | 至少包含不少于4次互联网暴露面发现、每季度1次外部漏洞挖掘、不少于2次安全专项检查、至少每月1次内部安全扫描、至少每月1次病毒查杀工作、每季度1次安全日志分析服务、每季度1次安全审计服务、至少包含13个系统的代码审计等方面内容。  满足招标文件要求，无瑕疵：8分；  方案内容存在1处瑕疵：6分；  方案内容存在2处瑕疵：4分；  方案内容存在3处瑕疵：2分；  未提供方案或不满足招标文件要求或内容存在4处及以上瑕疵：0分；  （本项所称“瑕疵”是指内容缺项、不完整或缺少关键点；非专门针对本项目或不适用本项目特性、套用其他项目内容；对同一问题前后表述矛盾；存在逻辑漏洞、科学原理或常识错误；不利于本项目目标的实现、现有技术条件下不可能出现的情形等任意一种情形） | 8 |
| 5 | 重要时期保障服务方案评价 | 至少包含网络攻防演习、重要时期保障服务等方面内容  满足招标文件要求，无瑕疵：8分；  方案内容存在1处瑕疵：6分；  方案内容存在2处瑕疵：4分；  方案内容存在3处瑕疵：2分；  未提供方案或不满足招标文件要求或内容存在4处及以上瑕疵：0分；  （本项所称“瑕疵”是指内容缺项、不完整或缺少关键点；非专门针对本项目或不适用本项目特性、套用其他项目内容；对同一问题前后表述矛盾；存在逻辑漏洞、科学原理或常识错误；不利于本项目目标的实现、现有技术条件下不可能出现的情形等任意一种情形） | 8 |
| 6 | 安全服务配套工具评价 | 至少包含投入本项目的安全监控系统、APT攻击检测设备、基线配置核查工具、威胁狩猎系统、数据安全分析平台、敏感数据发现及风险评估系统、数据库审计与风险控制系统等工具的介绍  满足招标文件要求，无瑕疵：5分；  内容存在1处瑕疵：4分；  内容存在2处瑕疵：3分；  内容存在3处瑕疵：2分；  内容存在4处瑕疵：1分；  未提供或不满足招标文件要求或存在5处及以上瑕疵：0分；  （本项所称“瑕疵”是指内容缺项、不完整或缺少关键点；非专门针对本项目或不适用本项目特性、套用其他项目内容；对同一问题前后表述矛盾；存在逻辑漏洞、科学原理或常识错误；不利于本项目目标的实现、现有技术条件下不可能出现的情形等任意一种情形） | 5 |
| 7 | 网络安全宣传方案评价 | 至少包含2024年度网络安全宣传周活动（含方案、海报、视频、H5版的网络安全知识竞赛）、宣传讲座服务、安全咨询服务、应急演练服务等方面内容  满足招标文件要求，无瑕疵：8分；  方案内容存在1处瑕疵：6分；  方案内容存在2处瑕疵：4分；  方案内容存在3处瑕疵：2分；  未提供方案或不满足招标文件要求或内容存在4处及以上瑕疵：0分；  （本项所称“瑕疵”是指内容缺项、不完整或缺少关键点；非专门针对本项目或不适用本项目特性、套用其他项目内容；对同一问题前后表述矛盾；存在逻辑漏洞、科学原理或常识错误；不利于本项目目标的实现、现有技术条件下不可能出现的情形等任意一种情形） | 8 |
| 8 | 威胁情报服务方案评价 | 至少包含威胁建模服务、威胁通告服务、威胁处置服务（在48小时内提供临时应急处理方案）、威胁狩猎服务（提供2个高仿真交互系统部署诱骗攻击者对测试系统进行攻击）等方面内容。  满足招标文件要求，无瑕疵：5分；  方案内容存在1处瑕疵：4分；  方案内容存在2处瑕疵：3分；  方案内容存在3处瑕疵：2分；  方案内容存在4处瑕疵：1分；  未提供方案或不满足招标文件要求或内容存在5处及以上瑕疵：0分；  （本项所称“瑕疵”是指内容缺项、不完整或缺少关键点；非专门针对本项目或不适用本项目特性、套用其他项目内容；对同一问题前后表述矛盾；存在逻辑漏洞、科学原理或常识错误；不利于本项目目标的实现、现有技术条件下不可能出现的情形等任意一种情形） | 5 |
| 9 | 应急响应服务方案评价 | 至少包含应急响应的应对范围、响应时间、响应流程等方面内容，中标供应商应急人员需7\*24小时进行响应，按照采购人要求，服务方安全专家团队必须在2小时内到场。  满足招标文件要求，无瑕疵：8分；  方案内容存在1处瑕疵：6分；  方案内容存在2处瑕疵：4分；  方案内容存在3处瑕疵：2分；  未提供方案或不满足招标文件要求或内容存在4处及以上瑕疵：0分；  （本项所称“瑕疵”是指内容缺项、不完整或缺少关键点；非专门针对本项目或不适用本项目特性、套用其他项目内容；对同一问题前后表述矛盾；存在逻辑漏洞、科学原理或常识错误；不利于本项目目标的实现、现有技术条件下不可能出现的情形等任意一种情形） | 8 |
| 合计 | | | 100 |

第二包：

|  |  |  |  |
| --- | --- | --- | --- |
| 第一部分 价格（10分） | | | 分值 |
| 1 | 价格 | （1）投标报价超过采购预算的，投标无效，未超过采购预算的投标报价按以下公式进行计算。  （2）投标报价得分=（评标基准价/投标报价）×10  注：满足招标文件要求且投标报价最低的投标报价为评标基准价。 | 10 |
| 第二部分 客观分（30分） | | | 分值 |
| 1 | 投标人业绩 | 完全按照以下要求提供投标人曾实施的三级（或以上）网络安全等级保护测评服务业绩，提供的证明材料均不得遮挡涂黑，否则不予认定加分。  A. 合同原件扫描件。包括合同金额、买卖双方名称及盖章、服务内容、合同签订日期（应为2021年1月1日或以后）。  B. 上述合同履行良好的相关证明材料原件扫描件（加盖上述合同甲方单位公章或上述合同中所盖的甲方印章）。  每个业绩2分，最多8分 | 8 |
| 2 | 投标人相关证书评价 | 投标人具备质量管理体系认证证书、《网络安全等级测评与检测评估机构服务认证证书》、《信息安全应急处理服务资质认证证书》、《信息安全风险评估服务资质认证证书》，提供以上证书扫描件，每个合格的证书扫描件得2分，最多8分。 | 8 |
| 3 | 投入项目人员（含项目经理）评价 | 投入的项目人员（含项目经理）为投标单位正式员工，提供实施小组人员姓名、开标前半年内任意1个月的由投标单位为上述人员缴纳社会保险证明扫描件，否则不予认定加分。  （1）项目经理具有工业和信息化部教育与考试中心颁发的高级信息安全管理工程师证书和网络安全等级测评高级测评师证书，提供以上证书扫描件，每个合格的证书扫描件得1分，最多2分；  （2）实施小组人员具备网络安全等级测评中级测评师证书，提供证书扫描件，每个合格的证书扫描件得1分，最多5分；  （3）安全技术人员具备信息安全保障人员认证（CISAW）证书，提供以上证书扫描件，每个符合要求的人员得1分，最多1分；  （4）安全技术人员具备注册信息安全专业人员-注册渗透测试工程师（CISP-PTE）证书，提供以上证书扫描件，每个符合要求的人员得1分，最多1分； | 9 |
| 4 | 投标人承诺评价 | 承诺完全满足招标文件“报价要求”、“时间地点要求”、“付款方式要求”和技术要求中非“★”号要求的：5分，其他0分。 | 5 |
| 第三部分 主观分（60分） | | | 分值 |
| 1 | 人员岗位、职责评价 | 至少包含各岗位投入人员数量、各岗位内部人员安排配置方案  满足招标文件要求，无瑕疵：12分；  方案内容存在1处瑕疵：9分；  方案内容存在2处瑕疵：6分；  方案内容存在3处瑕疵：3分；  未提供方案或不满足招标文件要求或内容存在4处及以上瑕疵：0分；  （本项所称“瑕疵”是指内容缺项、不完整或缺少关键点；非专门针对本项目或不适用本项目特性、套用其他项目内容；对同一问题前后表述矛盾；存在逻辑漏洞、科学原理或常识错误；不利于本项目目标的实现、现有技术条件下不可能出现的情形等任意一种情形） | 12 |
| 2 | 等保测评及风险评估方案评价 | 至少包括本项目涉及的14个三级信息系统、5个二级信息系统的等级保护测评服务方案以及2个系统的关键基础设施风险评估服务方案  满足招标文件要求，无瑕疵：12分；  方案内容存在1处瑕疵：9分；  方案内容存在2处瑕疵：6分；  方案内容存在3处瑕疵：3分；  未提供方案或不满足招标文件要求或内容存在4处及以上瑕疵：0分；（本项所称“瑕疵”是指内容缺项、不完整或缺少关键点；非专门针对本项目或不适用本项目特性、套用其他项目内容；对同一问题前后表述矛盾；存在逻辑漏洞、科学原理或常识错误；不利于本项目目标的实现、现有技术条件下不可能出现的情形等任意一种情形） | 12 |
| 3 | 互联网安全检测方案评价 | 至少包括互联网暴露面检测、外部漏洞挖掘、敏感信息泄露检查方案  满足招标文件要求，无瑕疵：12分；  方案内容存在1处瑕疵：9分；  方案内容存在2处瑕疵：6分；  方案内容存在3处瑕疵：3分；  未提供方案或不满足招标文件要求或内容存在4处及以上瑕疵：0分；（本项所称“瑕疵”是指内容缺项、不完整或缺少关键点；非专门针对本项目或不适用本项目特性、套用其他项目内容；对同一问题前后表述矛盾；存在逻辑漏洞、科学原理或常识错误；不利于本项目目标的实现、现有技术条件下不可能出现的情形等任意一种情形） | 12 |
| 4 | 人员保密管理方案评价 | 至少包含保证服务过程中有可能获取的保密信息不泄露的措施：制定保密制度、服务人员保密培训、重点岗位双人服务、泄密惩罚办法。  满足招标文件要求，无瑕疵：12分；  方案内容存在1处瑕疵：9分；  方案内容存在2处瑕疵：6分；  方案内容存在3处瑕疵：3分；  未提供方案或不满足招标文件要求或内容存在4处及以上瑕疵：0分；（本项所称“瑕疵”是指内容缺项、不完整或缺少关键点；非专门针对本项目或不适用本项目特性、套用其他项目内容；对同一问题前后表述矛盾；存在逻辑漏洞、科学原理或常识错误；不利于本项目目标的实现、现有技术条件下不可能出现的情形等任意一种情形） | 12 |
| 5 | 项目质量控制及保证措施评价 | 至少包含服务过程中保证服务质量的控制措施、对出现项目质量问题时如何挽回、服务态度保障、人员业务专业化水平保障等方面内容  满足招标文件要求，无瑕疵：12分；  方案内容存在1处瑕疵：9分；  方案内容存在2处瑕疵：6分；  方案内容存在3处瑕疵：3分；  未提供方案或不满足招标文件要求或内容存在4处及以上瑕疵：0分；  （本项所称“瑕疵”是指内容缺项、不完整或缺少关键点；非专门针对本项目或不适用本项目特性、套用其他项目内容；对同一问题前后表述矛盾；存在逻辑漏洞、科学原理或常识错误；不利于本项目目标的实现、现有技术条件下不可能出现的情形等任意一种情形） | 12 |
| 合计 | | | 100 |

第三包

|  |  |  |  |
| --- | --- | --- | --- |
| 第一部分 价格（10分） | | | 分值 |
| 1 | 价格 | （1）投标报价超过采购预算的，投标无效，未超过采购预算的投标报价按以下公式进行计算。  （2）投标报价得分=（评标基准价/投标报价）×10  注：满足招标文件要求且投标报价最低的投标报价为评标基准价。 | 10 |
| 第二部分 客观分（40分） | | | 分值 |
| 1 | 投标人业绩 | 完全按照以下要求提供投标人曾实施的商用密码应用安全性评估服务业绩，提供的证明材料均不得遮挡涂黑，否则不予认定加分。  A. 合同原件扫描件。包括合同金额、买卖双方名称及盖章、服务内容、合同签订日期（应为2020年1月1日或以后）。  B. 上述合同履行良好的相关证明材料原件扫描件（加盖上述合同甲方单位公章或上述合同中所盖的甲方印章）。  每个业绩2分，最多10分 | 10 |
| 2 | 投标人相关证书评价 | 投标人具有质量管理体系认证证书、信息安全服务资质认证证书、中国合格评定国家认可委员会检验机构认可证书（检测能力范围包含商用密码安全性评估相关内容）和检验检测机构资质认定证书（许可使用CMA标识，检测能力范围包含商用密码安全性评估相关内容），提供证书扫描件，每个合格的证书扫描件得2分，最多8分。 | 8 |
| 3 | 投入项目人员（含项目经理）评价 | 投入的项目人员（含项目经理）为投标单位正式员工，提供项目人员姓名、开标前半年内任意1个月的由投标单位为项目人员缴纳社会保险证明扫描件，否则不予认定加分。  （1）投入的项目经理具备《商用密码应用安全性评估人员测评能力考核证书》，提供证书扫描件，获得以上证书且成绩优秀的得2分，获得以上证书且成绩合格的得1分，其他0分。  （2）投入的项目经理具备高级（或以上）工程师职称证书，提供合格的证书扫描件：2分，其他0分；  （3）投入的项目经理具备注册网络安全渗透评估专业人员（NSATP-A）证书、信息安全保障人员认证（CISAW）证书、信息系统安全认证专业人员（CISSP）证书，每个合格的证书扫描件得2分，最多6分；  （4）投入的项目人员（不含项目经理）具备《商用密码应用安全性评估人员测评能力考核证书》，提供证书扫描件，每个获得以上证书且成绩优秀的人员得1分，每个获得以上证书且成绩合格的人员得0.5分，最多3分。 | 13 |
| 4 | 投标人承诺评价 | 承诺完全满足招标文件“报价要求”、“时间地点要求”、“付款方式要求”和技术要求中非“★”号要求的：9分，其他0分。 | 9 |
| 第三部分 主观分（50分） | | | 分值 |
| 1 | 项目理解评价 | 至少包含项目需求、测评对象、测评标准、测评范围及内容、密码需求分析、密码应用安全、密钥安全及安全管理制度等方面内容。  满足招标文件要求，无瑕疵：10分；  方案内容存在1处瑕疵：7.5分；  方案内容存在2处瑕疵：5分；  方案内容存在3处瑕疵：2.5分；  未提供方案或不满足招标文件要求或内容存在4处及以上瑕疵：0分；  （本项所称“瑕疵”是指内容缺项、不完整或缺少关键点；非专门针对本项目或不适用本项目特性、套用其他项目内容；对同一问题前后表述矛盾；存在逻辑漏洞、科学原理或常识错误；不利于本项目目标的实现、现有技术条件下不可能出现的情形等任意一种情形） | 10 |
| 2 | 项目实施方案评价 | 至少包含测评流程、测评方法、实施计划、项目组织、项目交付等方面内容  满足招标文件要求，无瑕疵：10分；  方案内容存在1处瑕疵：7.5分；  方案内容存在2处瑕疵：5分；  方案内容存在3处瑕疵：2.5分；  未提供方案或不满足招标文件要求或内容存在4处及以上瑕疵：0分；  （本项所称“瑕疵”是指内容缺项、不完整或缺少关键点；非专门针对本项目或不适用本项目特性、套用其他项目内容；对同一问题前后表述矛盾；存在逻辑漏洞、科学原理或常识错误；不利于本项目目标的实现、现有技术条件下不可能出现的情形等任意一种情形） | 10 |
| 3 | 质量保障方案评价 | 至少包含质量保障体系、技术保障、进度保障、沟通机制、风险控制及应急响应等方面内容。  满足招标文件要求，无瑕疵：10分；  方案内容存在1处瑕疵：7.5分；  方案内容存在2处瑕疵：5分；  方案内容存在3处瑕疵：2.5分；  未提供方案或不满足招标文件要求或内容存在4处及以上瑕疵：0分；（本项所称“瑕疵”是指内容缺项、不完整或缺少关键点；非专门针对本项目或不适用本项目特性、套用其他项目内容；对同一问题前后表述矛盾；存在逻辑漏洞、科学原理或常识错误；不利于本项目目标的实现、现有技术条件下不可能出现的情形等任意一种情形） | 10 |
| 4 | 保密管理方案评价 | 至少包含保密管理制度、保密管理技术措施、人员保密管理、文档保密管理等方面内容  满足招标文件要求，无瑕疵：10分；  方案内容存在1处瑕疵：7.5分；  方案内容存在2处瑕疵：5分；  方案内容存在3处瑕疵：2.5分；  未提供方案或不满足招标文件要求或内容存在4处及以上瑕疵：0分；（本项所称“瑕疵”是指内容缺项、不完整或缺少关键点；非专门针对本项目或不适用本项目特性、套用其他项目内容；对同一问题前后表述矛盾；存在逻辑漏洞、科学原理或常识错误；不利于本项目目标的实现、现有技术条件下不可能出现的情形等任意一种情形） | 10 |
| 5 | 培训方案评价 | 至少包含培训计划、培训内容等方面内容  满足招标文件要求，无瑕疵：10分；  方案内容存在1处瑕疵：7.5分；  方案内容存在2处瑕疵：5分；  方案内容存在3处瑕疵：2.5分；  未提供方案或不满足招标文件要求或内容存在4处及以上瑕疵：0分；  （本项所称“瑕疵”是指内容缺项、不完整或缺少关键点；非专门针对本项目或不适用本项目特性、套用其他项目内容；对同一问题前后表述矛盾；存在逻辑漏洞、科学原理或常识错误；不利于本项目目标的实现、现有技术条件下不可能出现的情形等任意一种情形） | 10 |
| 合计 | | | 100 |

第四包：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 第一部分 价格（10分） | | | | 分值 |
| 1 | 价格 | （1）投标报价超过采购预算的，投标无效，未超过采购预算的投标报价按以下公式进行计算。  （2）投标报价得分=（评标基准价/投标报价）×10  注：满足招标文件要求且投标报价最低的投标报价为评标基准价。 | | 10 |
| 第二部分 客观分（30分） | | | | 分值 |
| 1 | 投标人业绩 | 完全按照以下要求提供投标人曾实施的商用密码应用建设、改造项目相关业绩，提供的证明材料均不得遮挡涂黑，否则不予认定加分。  A. 合同原件扫描件。包括买卖双方名称及盖章、服务内容、合同签订日期（应为2021年1月1日或以后）。  B. 上述合同履行良好的相关证明材料原件扫描件（加盖上述合同甲方单位公章或上述合同中所盖的甲方印章）。  每个业绩2分，最多6分。 | | 6 |
| 2 | 投标人相关证书评价 | | 投标人须同时具备有效的CCRC信息安全服务资质认证（信息系统安全集成）、信息安全服务资质（软件安全开发）、信息安全服务资质（信息系统安全运维）证书,每满足一项得1分，有其中一项认证达到一级的得2分，本项满分6分，其他及未提供不得分； | 6 |
| 3 | 投入人员评价 | | 投入的人员为投标单位正式员工，提供姓名、开标前半年内任意1个月的由投标单位为项目人员缴纳社会保险证明扫描件，否则不予认定加分。  （1）项目经理具有信息系统项目管理师（高级）、网络安全服务能力评价证书（CCSS-CM），每提供1种证书扫描件得2分，最多4分；  （2）团队人员的资格证书应覆盖CISP注册信息安全工程师、软件设计师、数据库认证专家、售后服务管理师、信息系统项目管理师等证书，每提供上述一类不同的人员资格证书得1分，最多4分。  注：1人持多证可重复计分。 | 8 |
| 4 | 投标人承诺评价 | | 承诺完全满足招标文件“报价要求”、“时间地点要求”、“付款方式要求”和技术要求中非“★”号要求的：10分，其他0分。 | 10 |
| 第三部分 主观分（60分） | | | | 分值 |
| 1 | 项目需求理解分析评价 | 至少包含系统现状、任务目标、实施要求、建设重点及难点等方面内容  满足招标文件要求，无瑕疵：12分；  方案内容存在1处瑕疵：8分；  方案内容存在2处瑕疵：4分；  未提供方案或不满足招标文件要求或内容存在3处及以上瑕疵：0分；  （本项所称“瑕疵”是指内容缺项、不完整或缺少关键点；非专门针对本项目或不适用本项目特性、套用其他项目内容；对同一问题前后表述矛盾；存在逻辑漏洞、科学原理或常识错误；不利于本项目目标的实现、现有技术条件下不可能出现的情形等任意一种情形） | | 12 |
| 2 | 项目服务方案评价 | 至少包含服务方案设计原则及依据、建设思路、总体架构、网络架构、建设内容等方面内容，能精准提出本项目整体技术方案，提供清晰、详实的税务重要系统的密码改造方案；  满足招标文件要求，无瑕疵：12分；  方案内容存在1处瑕疵：8分；  方案内容存在2处瑕疵：4分；  未提供方案或不满足招标文件要求或内容存在3处及以上瑕疵：0分；  （本项所称“瑕疵”是指内容缺项、不完整或缺少关键点；非专门针对本项目或不适用本项目特性、套用其他项目内容；对同一问题前后表述矛盾；存在逻辑漏洞、科学原理或常识错误；不利于本项目目标的实现、现有技术条件下不可能出现的情形等任意一种情形） | | 12 |
| 3 | 整体运行维护方案评价 | 至少包含针对本项目系统的运维计划、实施方案等方面内容  满足招标文件要求，无瑕疵：9分；  方案内容存在1处瑕疵：6分；  方案内容存在2处瑕疵：3分；  未提供方案或不满足招标文件要求或内容存在3处及以上瑕疵：0分；  （本项所称“瑕疵”是指内容缺项、不完整或缺少关键点；非专门针对本项目或不适用本项目特性、套用其他项目内容；对同一问题前后表述矛盾；存在逻辑漏洞、科学原理或常识错误；不利于本项目目标的实现、现有技术条件下不可能出现的情形等任意一种情形） | | 9 |
| 4 | 定期预防性检查方案 | 至少包含预防性检查频率、检查内容、发现问题后的解决方案等方面内容  满足招标文件要求，无瑕疵：9分；  方案内容存在1处瑕疵：6分；  方案内容存在2处瑕疵：3分；  未提供方案或不满足招标文件要求或内容存在3处及以上瑕疵：0分；  （本项所称“瑕疵”是指内容缺项、不完整或缺少关键点；非专门针对本项目或不适用本项目特性、套用其他项目内容；对同一问题前后表述矛盾；存在逻辑漏洞、科学原理或常识错误；不利于本项目目标的实现、现有技术条件下不可能出现的情形等任意一种情形） | | 9 |
| 5 | 故障管理处理方案 | 至少包含响应时间、故障处理方案、防止再发方案等方面内容  满足招标文件要求，无瑕疵：9分；  方案内容存在1处瑕疵：6分；  方案内容存在2处瑕疵：3分；  未提供方案或不满足招标文件要求或内容存在3处及以上瑕疵：0分；  （本项所称“瑕疵”是指内容缺项、不完整或缺少关键点；非专门针对本项目或不适用本项目特性、套用其他项目内容；对同一问题前后表述矛盾；存在逻辑漏洞、科学原理或常识错误；不利于本项目目标的实现、现有技术条件下不可能出现的情形等任意一种情形） | | 9 |
| 6 | 突发事件管理方案 | 至少包含针对恶意攻击、访问量激增等处理方案  满足招标文件要求，无瑕疵：9分；  方案内容存在1处瑕疵：6分；  方案内容存在2处瑕疵：3分；  未提供方案或不满足招标文件要求或内容存在3处及以上瑕疵：0分；  （本项所称“瑕疵”是指内容缺项、不完整或缺少关键点；非专门针对本项目或不适用本项目特性、套用其他项目内容；对同一问题前后表述矛盾；存在逻辑漏洞、科学原理或常识错误；不利于本项目目标的实现、现有技术条件下不可能出现的情形等任意一种情形） | | 9 |
| 合计 | | | | 100 |

四、投标文件内容要求

（一）投标人须按照《投标须知》“C 投标文件的编制”中的相关要求编制投标文件。

（二）投标文件格式参照第五部分“投标文件格式”。

项目需求书

本项目属于软件和信息技术服务业。

第一包：

一、项目背景

近年来，税务总局在网络安全规划建设中，将建设智能安全运营中心列为一项重点工程，将其作为网络安全工作的重要支撑和有力抓手，力争实现安全防护自主可信，安全态势可知可见，安全现状可管可控，安全事件闭环运营。我局从2021年开始购买安全运营服务，以整体安全运营的理念将安全运维、漏洞扫描及监控预警、应急响应等单独的安全服务进行全面整合。以满足国家相关法律法规、符合国家税务总局相关制度规范为前提，实现攻防演练“零失分”，绩效考核无差错，安全事件不发生的安全防护目标，拟继续购买网络安全运营服务，强化网络安全保障，全面提升网络安全监控、预警、响应、处置、应急等综合能力。

二、项目内容

通过购买网络安全运营服务，完善我局的网络安全运营服务体系，协助我局提升安全整体规划管理，完善安全管理制度，优化安全管理流程。以整体安全运营的理念将安全运维、漏洞扫描及监控预警、互联网高危漏洞检测挖掘和众测服务等单独的安全服务进行全面整合，达到全面提升网络安全监控、预警、响应、处置、应急等综合能力。

三、项目需求

网络安全运营服务包括但不限于：

（1）日常运维服务

### ①信息资产管理（每月一次）

基于天津税务信息系统资产现状，对局内互联网端和内网端资产进行全生命周期管理。通过技术工具主动探测和人工完善校正，定期收集和梳理资产信息，包括厂商、型号、版本、账号授权等信息，形成《资产清单》。服务期内持续监测信息系统内的资产变化情况，包括资产的新增、变更和注销等。确认新增资产信息并开展上线前安全检查；确保变更资产信息准确性；排查处理非法接入资产；依照天津税务管理规范进行资产销毁等。

### ②安全管理监控（每月一次）

提供可视化监控工具，对网络安全设备进行日常监控，对设备异常情况进行实时预警提示。按照业务要求输出相关指标的安全健康检查报告。通过分析安全事件或日志信息，获取安全入侵告警信息，及时开展事件处理并出具详细处理报告。

### ③互联网预警监控（每月一次）

针对天津税务门户网站及各互联网业务系统进行7\*24小时的网站安全监测服务，包括但不限于网页篡改监测、网页挂马监测、网页敏感内容监测、网页黑链监测、网站平稳度监测、域名解析监测、网站漏洞扫描、钓鱼网站监测、代码泄露监测等内容，并实时通报安全事件，提供《互联网安全监控报告》，分析各网站的风险隐患和安全趋势。

### ④安全加固技术支持（按需提供）

针对网安部门和税务总局下发的漏洞通告，以及在各类检测、评估、扫描等工作中发现的安全隐患，结合信息系统的实际运行情况，提出具有可操作性的安全加固整改建议，并在整改完成后进行人工复核。加固范围包括局内现网网络设备、安全设备、主机操作系统、数据库、中间件及网络服务应用等。

### ⑤配置策略优化（按需提供）

针对现网网络设备、安全设备及终端主机的安全策略、规则及基础配置进行合规性审查，根据日志分析及误报信息优化配置策略，周期性清除冗余策略、僵尸策略，提供策略优化信息，包括但不限于设备名称、设备地址、策略变更时间、当前策略、策略变更内容、策略变更操作人等。

### ⑥网络威胁数据分析（按需提供）

针对安全事件的威胁数据分析服务，采用“以攻击者为中心”的安全视角，通过结合安全设备日志、全流量数据、主机日志数据、威胁情报等多种方式开展关联分析，以提供真实准确的事件分析结果，并提供安全事件分析报告。针对发现的高级定向攻击行为能够提供溯源分析服务，深入分析攻击者行为，利用样本逆向分析、情报分析、多维数据融合分析技术，溯源攻击者，梳理攻击路径，并提供防范建议。

### ⑦网络拓扑梳理（每季度一次）

绘制网络拓扑图以便符合天津市税务局真实网络架构情况。梳理机柜己上架运行设备信息,形成机柜拓扑图。梳理各个业务系统数据包流向范围,形成业务系统数据流拓扑图。

（2）安全检测服务

### ①互联网暴露面发现（每季度一次）

按照实际需要，结合服务工具和人工分析，针对天津税务互联网暴露面信息进行全面的探测扫描，包括但不限于：IP地址存活情况、端口服务开放情况、操作系统类型及版本、应用框架类型及版本、IP地址与域名对应关系等，形成《互联网暴露面发现报告》。及时发现不合规或存在安全风险的端口和服务，并提供有效且具有针对性的解决方案，协助进行处置整改。快速研判天津税务互联网暴露面资产所面临的安全威胁及风险形势，提供包括资产安全风险类别、安全风险等级、安全风险范围、安全风险对象等内容的安全风险通报预警服务。

### ②渗透测试（每季度一次）

以人工渗透为主，扫描工具为辅，模拟真实的网络安全攻击，识别内外部威胁风险，包括但不限于Web应用安全风险、业务安全风险、弱口令、配置不当、社工库利用、敏感信息泄露等。发现黑客入侵互联网网站和各互联网信息系统的攻击路径和攻击方式，并提供《渗透测试报告》，跟进后续漏洞修复检验等。

实施渗透测试工作前期，需确认渗透测试方案，方案内容主要包括渗透测试范围、最终对象、测试方式、测试要求的时间等内容。在测试实施过程中，提供自动化的安全扫描工具，完成初步的信息收集、服务判断、版本判断、补丁判断等工作。由专业安全服务人员对安全扫描的结果进行人工的确认和分析。并且根据收集的各类信息进行人工的进一步渗透测试深入。结合自动化测试和人工测试结果，服务人员需整理渗透测试服务的输出结果并编制渗透测试报告。在经过整改或加固后，服务人员进行回归测试。

另外，在重要保障工作前期按照需求，对特定系统单独进行渗透测试，提供《渗透测试报告》。

### ③安全专项检查（每季度一次）

按照实际需要，开展安全专项检查。主要针对在日常安全管理中的常见安全问题，包括但不限于：弱口令检查、敏感信息泄露检查、和供应链安全风险排查等。

通过弱口令检查服务避免服务器或者应用系统因为存在弱口令而被黑客暴力破解登录，并完全控制主机，甚至通过该主机发动内网攻击的情况发生，检查范围包括各类主机、数据库、中间件等，形成《弱口令清单》。

敏感信息泄漏检查范围主要包括Github平台、百度网盘、百度文库、CSDN、暗网等，检查内容包括天津税务信息系统源代码、邮件配置信息、数据库配置信息、FTP配置信息、关键岗位人员信息、税务数据信息等。

供应链安全风险排查范围主要包括设备制造商、软件供应商、系统集成商、第三方运维厂商等，重点关注厂商运维账号、VPN账号等风险点，定期进行清理整顿，清除幽灵账户；定期对应用及设备进行安全性测试，掌握应用及设备安全风险。

### ④内网安全扫描（每月一次）

定期利用专项技术工具对网络设备、安全设备、操作系统、服务器、中间件、数据库及应用系统等进行内部漏洞扫描，扫描前期明确扫描方式、扫描范围、扫描实施时间和设备接入点等，人工分析扫描结果，提供漏洞修复可落地建议，形成《漏洞扫描报告》，报告内容主要包括：漏洞厂商、威胁目标、危险级别、危害描述、检测依据以及详细解决方案等。对于已修复的漏洞进行复测检查，确认漏洞已被修复。

### ⑤病毒查杀工作（每季度一次）

按照需求提供专业化查杀工具，定期对服务器进行病毒扫描工作，更新病毒库版本，根据需要协调后台技术专家进行技术支持。

### ⑥安全日志分析服务（每周一次）

利用专业安全技术工具，通过对网络安全设备等进行日志分析，发现违规操作和风险点，进行综合评估并形成《安全日志分析报告》。日志分析类型主要包括：常见Web攻击行为、操作系统可疑行为、网络可疑行为和安全设备监控告警行为等。日志分析报告需包括背景描述、日志类型、日志时间段、关键日志内容和总结、安全建议等。

### ⑦安全审计服务（每月一次）

按照需求协助制定审计规范和审计策略，提供审计工具实现对局内数据库所有访问行为的监控和审计，对其中的危险操作进行告警、对数据库访问行为进行统计和图形化展现。

驻场运营团队定期查看数据库审计系统日志，对数据库操作行为进行全面的审计，包含操作风险审计和会话事件审计；对数据库实例进行多维度和多时间粒度的审计分析，包括但不限于风险、语句、会话和访问来源等；形成《数据库审计报告》，对数据库操作行为审计结果进行统计分析，包括但不限于审计总时长、审计语句总量、风险语句总量、风险语句类型分布、审计语句数量趋势、风险语句数量变化趋势、SQL语句类型分布、审计语句事件实时告警状态等。

### ⑧代码审计服务（按需提供）

按照需求由专业人员在税务局专用设备上通过人工检查和工具扫描的方式对本地特色软件提供专业源代码审计服务，包括但不限于门户网站、电子税务局、自助办税终端等13个业务系统，审计代码量不低于1500余万行。

服务前期需明确代码审计范围、审计方式和审计方案，通过技术工具实现初步的信息收集，由专业安全服务人员结合代码扫描结果进行分析和确认，编制代码审计报告。经整改或加固后，服务人员需开展二次检查并提交复查报告。

（3）威胁情报服务（按需提供）

### ①威胁建模服务

由驻场运营团队定期开展威胁建模服务，确认事件类型，主要包括失陷事件、风险主机事件、疑似失陷事件、恶意攻击事件等，针对不同类型事件规范威胁处置流程。

### ②威胁通告服务

收集和整理最新的安全漏洞、汇总各类安全平台披露（如国家漏洞平台、补天平台）的涉及天津税务的安全漏洞信息、安全事件、安全资讯，信息安全事件等信息，结合天津税务实际情况形成通告，以电子word文档形式实时或定期发送指定邮箱。通告内容包括但不限于：安全漏洞（补丁）通告、安全威胁通告、安全业界动态、恶意代码防范、紧急通告等信息。

### ③威胁处置服务

针对威胁通告或网安部门披露的重大漏洞和风险，由专业安全服务人员在48小时内提供威胁处置服务。识别重要信息系统网络安全威胁风险，及时检测漏洞、病毒木马、网络攻击情况，发现网络安全事件线索，封堵具有持续性攻击或针对性攻击的高危访问源，跟踪问题整改进度和整改效果，保障重要信息系统的网络安全。

### ④威胁狩猎服务

在攻防演练期间或者发生安全事件时,派遣安全专家提供技术支持,针对高级持续性威胁进行溯源分析、攻击者画像并捕获。

提供不少于2个高仿真交互系统，诱骗攻击者对仿真系统进行攻击,混淆攻击者的攻击目标，保护局内真实的业务系统，发现攻击者的浏览器信息、操作系统信息、MAC地址、地理信息、代理IP和设备指纹信息等,针对探测扫描、渗透攻击、权限获取、后门远控和跳板攻击等攻击路径进行分析取证，及时采取相关反制措施。结合局内真实业务网络架构部署仿真服务节点，类型主要包括数据库、Web应用、邮件和共享文件等,网络区域包括但不限于服务器区仿真、DMZ区仿真、数据库仿真、核心业务仿真和办公区仿真等，要求在合同和法律约束范围内开展威胁捕获。

（4）应急响应服务（按需提供）

服务期间在发生应用服务瘫痪、网络阻塞、DDoS攻击、服务器遭劫持、系统异常宕机、恶意入侵、黑客攻击、病毒爆发、内部安全事故等紧急安全问题时，派出技术支援团队赴现场进行技术支持，判断安全事件类型，控制事件影响范围，解决安全问题，恢复信息系统，提供《信息安全事件应急响应报告》，报告至少包括事故原因、过程描述、解决方案、处理结果、改进建议等。

另外，根据实际情况修订完善我局网络安全相关应急预案。组织至少1次桌面或实战应急演练，通过文档查阅、现场调研等方式编写应急演练方案、剧本，应急演练结束后编写应急演练总结。

（5）重要时期保障服务（按需提供）

### ①网络攻防演练

在公安部（1次3周）、税务总局（1次2周）的攻防演练期间，提供专业安全技术支撑服务，协助实现演练“零失分”的目标。委派值守团队(至少2名专家和4名高级辅助人员)提供7\*24小时现场值守服务，由专业安全服务人员组成风险监测组、分析研判组和事件处置组，风险监测组实时监控外部安全威胁情报、安全漏洞情报及外部披露情报，分析研判组对局内安全设备进行监控预警和日志分析，捕获异常攻击行为或访问操作行为，事件处置组进行策略调优和异常攻击行为封堵，提供《网络攻防演练活动日报》和《网络攻防演练活动总结报告》，对局内安全风险进行闭环。

### ②重要时期保障服务

按照实际需要在国家重要节日、活动时期以及黑客组织明确声明攻击行为期间，提供不少于6人的7\*24小时现场值守服务，开展安全保障检查、安全保障监控和安全保障响应，实时监测并分析网络攻击事件，及时进行相应封堵处置，提供《重要时期网络安全保障报告》。

重要活动开始前组织专业安全人员进行安全设备健康情况检查，主要包括CPU使用率、内存占用率、接口流量、接口工作状态、硬盘使用情况等；开展Web站点渗透测试、主机安全检查和安全漏洞扫描。重要活动进行期间进行安全设备告警事件实时监测，主要包括僵木蠕、拒绝服务攻击、漏洞远程利用、恶意代码传递等高危事件；对告警事件进行确认、排查、分析和处理。重要活动结束后进行成果汇报，总结网络安全风险和进一步网络安全工作建设重要。

## （6）网络安全宣传（按需提供）

组织2024年网络安全宣传周活动，提供活动所需方案、物资、人员等相关配套服务，主要包括：①实施方案；②宣传海报；③宣传视频；④安全讲座；⑤网络安全知识竞赛；⑥网络安全专项竞赛；⑦安全咨询服务等。

活动实施方案需明确活动主题、开展范围、组织形式、人员组织方案、流程和时间安排、环境布置、活动内容、后勤保障、活动应急方案等。

依据网安周活动主题设计并制作宣传海报、宣传视频、宣传奖品等物料。

安全讲座不少于6场，讲座主题包括但不限于网络安全意识、新型信息技术、数据安全、第三方人员保密教育等。网络安全意识教育专题讲座：邀请信息安全领域相关专家学者，围绕当前国内、国际网络安全形势，日常工作生活中的网络安全案例开展2次专题讲座。信息技术培训：邀请信息安全领域相关专家，围绕关键信息基础设施安全、云安全、大数据安全、个人信息保护、大模型、5G通信网络等内容开展1次信息技术培训。数据安全专题培训：邀请数据安全领域相关专家，围绕数据收集、使用、存储过程中的安全规范，国家相关法律法规，重大数据泄露事件等开展2次数据安全专题培训。第三方人员保密教育：邀请讲师开展信息安全保密教育1次。

提供专家指导服务不少于40人次，邀请从事信息化相关工作5年及以上的副高级及以上的工程师参与国家税务总局天津市税务局的项目论证、项目评审、项目验收等工作，提供专家意见。

提供不少于10人次的相关安全知识转移，主要使知识转移对象通过安全服务工作，掌握新时期下做好网络安全工作的方法，从改变信息安全从业人员思维与安全意识、增强人员专业网络安全知识和技能、建立人员管理与流程机制出发，结合管理支撑工具等方面进行信息安全与风险管控的提升，帮助我局构建信息安全与IT风险管理体系，提升网络安全风险防御能力。

（7）安全运营度量指标设计服务（按需提供）

提供安全运营度量指标设计服务,评估我局当前的信息安全工作状态，完善评价基准体系,识别系统风险资产、脆弱性和威胁，评估安全控制措施的有限性和差距，量化分析当前安全运营水平和状态,便于长期的安全运营规划和改进。

运营度量指标主要包括：网络设备、安全设备、终端主机、数据库、应用系统、安全管理等安全基线，资产管理与核查，漏洞挖掘与管理，威胁发现与防范，事件应急与处置，日常运行与维护等。

（8）数据安全运营服务（按需提供）

依据天津税务实际业务场景，以数据安全合规为目标，以数据资产为核心，对局内重要数据的流转风险进行监测及管控，构建常态化数据安全运营机制。提供技术工具实现数据安全基础审计、防护和数据安全集中管理。针对我局网络拓扑及数据流进行针对性建设，包括但不限于数据库操作审计和流量监测探针；实现局内重要数据、核心数据资产资源目录构建，监测数据间流转情况，对数据安全风险进行分析研判，集中管控数据安全设备。

数据资产清单构建：对局内重要数据资产进行测绘，主要包括数据资源名称、数据类型、所属业务系统、敏感级别等。

数据资产变化稽核：服务期间重点关注资产变化情况，针对变化资产进行针对性防护，定期形成最新数据资产清单。

数据流转监控：提供技术工具针对高敏、重要数据访问主体和流转途径节点进行实时监测和威胁分析，包括未知资产监测、敏感税务数据明文传输、接口访问异常等。

数据安全风险评估：立足于法律法规和天津税务数据安全管理规范，针对局内不少于15个重要业务系统的数据和数据处理活动开展数据安全风险评估，检验其合法合规程度，评估保护措施有效性，针对各业务系统形成《数据安全风险评估报告》、《数据安全风险整改建议》。

（9）SSL证书服务（按需提供）

二级域名：tianjin.chinatax.gov.cn。单独签发安装一张 通配符证书。三级域名：目前已知有6个三级域配置多域名证书。

（10）CDN加速服务（按需提供）

保障国家税务总局天津市税务局门户网站及网上办税系统在全国范围内的访问速度和稳定性，提升用户体验；另外面对日益严峻的网络安全形势，联动基于云的安全防御平台，通过安全防御平台实现Web攻击的有效预防和统一防御，采取覆盖从网络层到应用层的安全方案，建立应对大范围、大流量的网络攻击的防护措施，保障基于HTTP/HTTPS的用户业务在遭遇大流量DDoS攻击、CC攻击时能正常稳定在线，同时提供监控预警。

互联网门户网站备源与源站数据实时同步，且可针对应用进行监管，当互联网门户网站源站发生异常时，由备源端的应用接管相应的业务，并对外提供服务。

（11）互联网高危漏洞检测挖掘和众测服务

通过第三方专业安全厂商组织业内精英白帽子尝试模拟黑客入侵的方式，对我局互联网平台应用系统（包括但不限于WEB应用、移动APP、小程序）进行（每年2次，每次不少于15天）远程获取敏感数据,以最高等级多手段全方位检测的智能渗透策略揭露安全漏洞及系统存在的脆弱性，发现信息系统存在的安全漏洞、安全配置问题、应用系统安全漏洞，检查系统存在的弱口令，收集系统不必要开放的账号、服务、端口，发现互联网平台各应用系统潜在的高、中、低危漏洞，提出漏洞解决方案，并协助进行加固整改，提升互联网平台的安全防护水平，形成整体安全风险报告，有效应对税务总局绩效指标中的漏洞考核。

1. 动态防御服务

通过部署动态防御设备，将金三、金四业务流量引流至动态防御设备，实现对接入流量业务系统的动态防御，有效识别区分机器人与自然人的访问行为，结合业务系统特点，深度定制动态安全防护策略，并定期优化，有效防护0day/Nday漏洞、恶意爬虫、自动化攻击、未知威胁等新型攻击手段，深度发现网络安全隐患，提升网络安全防护水平，实现“从人防到技防”。

能力建设和服务内容包括：

①对攻击者的已知漏洞探测行为进行识别和拦截，为补丁修复赢得充分的时间窗口；

②建设应用层未知威胁攻击的防护能力，对应用层未知漏洞攻击可以进行预先防护：

③对没有明显攻击特征的新兴自动化攻击行为进行安全防护，有效防御撞库、客户信息爬取、应用层DDOS等攻击行为。

④实现基于http/https协议的动态安全防护，防护各类自动化攻击：防非法客户端、防逆向、防网站分析、防中间人、防重放、防协议漏洞、防扫描、防越权、防注入、防撞库、防垃圾注册、防盗链，提高应用系统防自动化工具攻击能力。

⑤按月出具动态防护报告，结合业务系统特点，深度定制动态安全防护策略，并定期优化，深度发现网络安全隐患，提升网络安全防护水平。

（13）全流量分析服务

抓取网络内全量流量数据，通过对网络和关键业务进行全天候、自动化、深度可视的安全及流量监控，在攻击溯源、风险排查、研判分析等多个维度上，进行长周期大容量数据包存储、快速数据包检索、灵活流量数据共享，为网络安全提供事前检测预警、事中分析研判、事后溯源取证能力，满足应对日益严重的网络攻击、增强安全响应能力的需求。同时，通过网络全链条的数据包捕获，进行攻击的空间溯源，定位攻击源头和攻击路径；同时能够通过数据包内容进行快速检索，对0day漏洞攻击进行时间回溯，发现已潜伏的历史攻击；从网络会话、原始数据包、横向移动、扫描行为、攻击历史、攻击结果等多维度对安全事件进行全面溯源分析，对攻击者和失陷系统绘制全面的IP画像，完整的绘制入侵、扩散、攻击的网络路径，使得安全运营人员具备对安全事件快速响应和压制攻击的能力；通过查看网络流量和会话，能够对内部网络资产和风险进行排查，挖掘内网的暗灰资产，消除可能的安全防护盲点。

（14）API安全防护服务

通过部署API安全防护系统，结合动态防御技术，实现API的资产管理、攻击防护、敏感数据管控和访问行为管控，从而解决API面临的各种安全风险与挑战。自动发现流量中的API资产和敏感接口，对API资产进行分组管理，并结合业务情况对API调用情况进行确认，精准发现失活API，及时对过期资产下线；利用智能规则匹配及行为分析的智能威胁检测引擎，持续监控并分析流量行为，有效检测威胁攻击；对API传输中的敏感数据进行识别，针对敏感数据可以进行脱敏，防止敏感数据泄露。

API安全防护能力建设和服务内容包括：

①实现API风险统一展示：对税务API相关运行状态统一展示，包括：API运行状态监控、API异常行为监控、API攻击监控、敏感数据监控等。

②实现API资产识别：能够基于大数据建模自动发现API接口，自动对API接口实现分类、分组，并指派责任人，实现数据分权管理。自动提取API接口样式，为API接口提供可视化的详情展示，实现API资产的生命周期管理；

③实现API运行状态监测：持续监控、分析税务API当前运行状况，支持获取、统计、展示API接口性能信息、调用行为等信息，并对违规参数或异常行为进行检测和告警；

④提供API安全防护能力：可通过AI智能威胁检测引擎，并利用机器学习获得的多种威胁模型来确定异常攻击，同时利用语义分析和流量学习技术，精准、快速地识别各类攻击，包括OWASP API Security Top10的安全攻击检测、API安全参数合规检测、API接口调用顺序检测等；

⑤提供API敏感数据管控能力：可通过敏感数据检测模型，对敏感信息进行自动分级及实时洞察，并能够及时对API接口回传报文中的敏感信息进行脱敏处理，规避数据泄漏风险。

⑥实现对API访问行为日志的采集与审计，并基于威胁情报信息辅助，实现对账号、IP、令牌及API安全事件的审计与溯源。

⑦按月出具动态防护报告，结合业务系统特点，深度对API运行状态及风险分析。

（15）安全服务配套工具

根据安全运营需要，结合安全服务内容，在服务期间按需提供相关配套工具，主要包括：

①安全监控系统

对信息系统安全风险、威胁事件进行统一关联分析，便于运维人员进行分析研判、溯源追踪和处置响应。

②流量分析探针

对网络流量进行采集，对网络扫描、探测、攻击行为进行实时监控，并进行分析告警。

③APT攻击检测系统

对网络流量进行采集，对高级持续威胁进行检测，实现感知信息资产失陷、攻击溯源分析等。

④数据库审计系统

针对不少于85套数据库访问流量进行采集、记录、分析，筛选出对数据库的高危操作或可疑操作，形成数据库审计报告。

⑤漏洞扫描系统

扫描探测内外网存活主机、开放端口、中间件和应用服务，识别信息系统漏洞和风险，提供漏洞详细报告和处置建议。

⑥威胁狩猎系统

按照实际要求在攻防演习期间使用该设备诱捕互联网攻击行为，提供入侵活动线索，协助刻画攻击者画像。

⑦数据安全分析平台

对天津税务系统重要数据资产进行梳理，实现数据资产可视化管理。

# 四、项目实施要求

## （一）项目总体要求

基于天津税务信息安全管理现状，依托于现有网络安全设备；或者通过提供相关产品，实现各项安全运营管理服务需求。

## （二）项目人员要求

服务单位需为本项目组建专业服务团队，包括：

1.实施小组

需配备不少于1名项目经理与用户接洽各项事宜。项目经理需具备不少于6年信息安全工作经验、具备同类项目管理经验，具有人力资源和社会保障部颁发的高级项目管理师证书，投标人需出具相关材料证明。

2.驻场团队

包含至少4人，其中3名网络安全运营驻场工程师、1名数据安全运营驻场工程师（如无法满足实际工作开展，需增派驻场人员，增派数量以满足实际需求为准）。

要求驻场工程师应具有不少于3年网络安全或数据安全工作经验，至少注册信息安全专业人员（CISP）、注册信息安全工程师（CISE）、信息安全保障人员（CISAW）、注册渗透测试工程师（CISP-PTE）等资质中的任意一个。

如因各种原因造成服务期内驻场人员离岗，投标人需提供同等资质或以上的工程师进行更换，工作交接时长不得短于2个月。投标人应严格管控驻场团队，严禁出现驻场团队同时离岗的情况。

3.安全审计团队

人员数量不限，可由驻场人员兼任，也可独立设置。要求执行此项工作人员或团队服务期内具有稳定性，具有不少于2年或以上相关工作从业经验，具备国际信息系统审计师（CISA）资质。

4.攻防演习防守团队

至少1名安全专家和2名高级安全工程师（应根据实际攻防展开情况，进行酌情增派），按需自行配备所需专业工具。其中安全专家具有注册信息系统安全专家（CISSP）、注册渗透测试工程师（CISP-PTE）、注册渗透测试专家（CISP-PTS）等资质之一，或者拥有超过3年以上省部级以上攻防演习成功防守案例。高级安全工程师必须至少具有注册信息安全专业人员（CISP）、注册信息安全工程师（CISE）、注册渗透测试工程师（CISP-PTE）、注册渗透测试专家（CISP-PTS）等资质中的任意一个。

要求防守团队/安全专家具备以下能力：（1）能够进行资产攻击面分析；（2）能够进行服务器被攻击行为检测；（3）能够进行非常规服务分析；（4）能够进行数据库危险操作分析；（5）能够进行服务器失陷预测分析；（6）能够进行账户风险分析；（7）能够进行WEB安全分析；（8）能够对受害目标及攻击源头进行精准定位，对入侵途径及攻击者背景的研判与溯源。

5.安全检测团队

人员数量不限，内部扫描可由驻场人员兼任也可独立设置，外部挖掘需有独立团队担任。团队人员需经过正规的法律培训，需经过实名认证，认证信息与公安部的公民身份信息一致，且无不良记录。

6.应急支撑团队

至少5人，包括应急服务人员若干和应急安全专家若干。其中应急服务人员中，部分成员可由驻场团队兼任，保证至少有1人能在1小时能到现场；应急安全专家中，保证在2小时到现场。应急安全专家必须具有注册信息系统安全专家（CISSP）、注册渗透测试工程师（CISP-PTE）、注册渗透测试专家（CISP-PTS）等资质之一。应急服务人员应具有注册信息安全专业人员（CISP）、注册信息安全工程师（CISE）、信息安全保障人员（CISAW）、注册渗透测试工程师（CISP-PTE）、注册渗透测试专家（CISP-PTS）等资质中的任意一个。

7.重保服务团队

包括现场保障人员9名，远程保障人员及安全应急保障响应小组。此部分人员可与攻防演习防守团队、应急支撑团队复用，资质要求与6相同，但不得由驻场团队成员兼任。

## （三）其它要求

1.安全服务配套工具

服务单位需为本项目提供相关安全服务配套工具，应包括但不限于天津税务提出的相关产品。各类设备实际部署数量应根据具体覆盖范围进行调整，并且不局限于某一厂商某一品牌，以满足天津税务实际安全防护需求为原则。

此外服务单位需根据对天津税务安全现状分析后，额外提供基于新技术的相关安全产品，需提供详细的说明，涉及安全需要、实现方式及预期效果等内容。

2.保密要求

服务单位提供的各安全服务团队的组成人员必须遵守国家税务总局天津市税务局内部各项规章制度和内部操作规程，履行保密义务，签署保密协议，未经批准不得以任何理由泄露任何保密信息和内部资料。

3.能力测试

国家税务总局天津市税务局有权对服务单位提供的团队人员的业务能力进行测试。如果不能满足本项目安全服务的要求，或国家税务总局天津市税务局认为其不适合从事本项工作，甲方有权要求更换。更换后安全的服务驻场人员资质和工作经验应达到本项目的工作要求。

4.履约要求

如因投标方人员未完全履行服务约定对甲方网络安全工作造成重大影响或引发舆情的，根据影响情况最多扣减项目合同金额的20%。

五、项目验收要求

## （一）项目交付成果

1.按招标文件技术部分要求对服务进行验收，服务单位应在验收时提供相关周期性服务报告。

2.项目服务期内如果因运维人员问题，出现安全设备运行故障，导致税务系统相关应用系统出现30分钟以上系统服务中断的情况时，按合同中违约条款追究责任。

## （二）项目验收文档

|  |  |  |
| --- | --- | --- |
| 产出物 | 频率 | 数量 |
| 安全运营项目周报 | 每周 | 48 |
| 安全运营项目月报 | 每月 | 12 |
| 安全日志分析报告 | 每周 | 48 |
| 数据库审计报告 | 每月 | 12 |
| 漏洞扫描报告 | 每月 | 12 |
| 网络攻防演习相关报告 | 按需 | 按需 |
| 重要时期保障服务相关报告 | 按需 | 按需 |
| 互联网暴露面发现报告 | 每季度 | ≥4 |
| 互联网渗透测试报告 | 每季度 | ≥4 |
| 数据安全风险评估报告 | 按需 | ≥14 |
| 应急响应报告 | 按需 | 按需 |
| 资产清单 | 每月 | 12 |
| 内网失陷主机报告 | 每月 | 12 |
| 弱口令清单 | 每月 | 12 |
| 互联网安全监控汇总报告 | 每月 | 12 |

项目验收过程中，验收组成员将按照合同内容和工作要求对该项目进行审核，要求服务单位确保合同中涉及内容均已阶段性完成，完整提供交付文档和验收文档等。

六、税收信息化项目开发和应用管理工作要求

（一）失信认定

甲方遵照《税务系统信息化服务商失信行为记录名单制度（试行)》对乙方失信行为进行认定，并追究乙方相关责任。

（二）安全和保密要求

１.乙方应严格落实国家税务总局天津市税务局网络安全保密管理要求，承担技术支持人员的安全和保密管理责任。按甲方要求签订乙方保密协议书和技术支持人员保密承诺书。

２.乙方承担派驻技术支持人员背景审查，提供其身份证明、履历、家庭成员及主要社会关系、无犯罪记录证明等材料，提交信息备案表。

３.乙方负责派驻技术支持人员工作胜任、资格条件、以及网络安全能力评估，对技术支持人员承担的工作进行安全保密风险分析，明确技术支持人员工作范围和边界，重点防范设备和资料失窃、误操作导致的软硬件故障、敏感信息泄露、信息系统越权访问和网络攻击等风险。

４.乙方负责派驻技术支持人员的网络和数据安全管理、网络安全意识、保密意识、网络安全法律法规、网络安全技能以及网络安全警示教育等培训，上岗前确保考核合格。

５.对“安全和保密责任”落实不严格、不到位，造成重大安全事件或产生负面影响的，按照合同中“其他终止合同情况”条款执行，并依照相关法律等规定进行追责。

（三）运行维护保障要求

１.乙方在运行维护中出现运行故障（不可抗力因素除外）或发现违规操作，30分钟内未主动上报甲方的，给予警告，并按次扣除合同总价款1‰的金额；合同生效期间累计扣除不超过合同总价款5%的金额。

２.乙方在运行维护中出现巡检不及时、不到位的，按次扣除合同总价款1‰的金额；合同生效期间累计扣除不超过合同总价款的5%。

３.乙方在运行维护中发现运行故障（不可抗力因素除外）、业务系统可用性低于50%或业务功能阻断等问题的，甲方将根据乙方处理时间（持续时间判定以甲方通报为准）扣除合同总价款一定比例的金额。运行故障0.5小时≤持续时间＜4小时的，按次扣除合同总价款5‰的金额；运行故障4小时≤持续时间＜8小时的，按次扣除合同总价款1%的金额；运行故障持续时间≥8小时的，按次扣除合同总价款5%的金额。

（四）其他专项要求

１.禁止乙方另行开发合同业务需求范围内供纳税人、缴费人使用的软件，对违反合约专门条款的，纳入失信名单。

２.乙方在本项目实施过程中发生违反安全规定的行为，造成数据失窃或丢失、敏感信息泄露、主要业务系统瘫痪等不良后果的，自甲方或甲方主管机关做出认定结果之日起三年内，税务系统各单位可以拒绝乙方参与税务系统政府采购活动。

３.乙方应建立防止违法违规聘用离职税务人员的风险控制制度，出现违法违规聘用离职税务人员行为的，甲方将采取包括但不限于要求其限期改正、支付违约金、解除合同、三年内限制参加所聘人员原单位及下属单位信息化项目政府采购活动等措施。

４.禁止乙方采取馈赠礼品礼金、邀请娱乐旅游消费、提供便利条件等非正常交往手段“围猎”相关税务人员及亲属。一经发现，自发现之日起三年内，税务系统各单位可以拒绝乙方参与税务系统政府采购活动。

七、其他要求

1.承担相关技术支持人员的安全和保密管理责任，服务单位必须签订《国家税务总局天津市税务局保密协议书》，技术支持人员必须签订《国家税务总局天津市税务局保密承诺书》。

2.对技术支持人员承担的工作应进行安全保密风险分析，明确技术支持人员工作范围和边界，重点防范设备和资料失窃、误操作导致的软硬件故障、敏感信息泄露、对信息系统的越权操作和恶意攻击等风险，严格按照有关部门和招标人相关安全保密管理要求实施管理。

3.严格控制技术支持人员处理内部文件、获取税务数据的范围和权限，包括不得随意将携带的电脑和移动存储介质接入税务专网。

4.严格内外网管理，未经允许，不得擅自从内网拷贝并向外携带办公区数据、文档、程序等信息资源，确因工作需要，须填写申请，报主管应用系统负责人审批，并经运维支持中心备案后，方可实施相关操作。外网的数据进入内网，必须在指定计算机上，并进行严格检查杀毒后，方可进入内网，避免将病毒或木马等带入。

5.办公区计算机设备使用和安全要求严格遵循天津市相关规范。未经允许不得在公用计算机上保留各类工作文档及数据。办公区外网计算机需安装指定系统及防毒软件等必要软件，严禁接入办公区内网，不得保留与工作有关的文档、图片等电子文件，因工作需要上传下载的文件须及时删除。外网计算机统一配发使用账号，使用后需注销用户。

6.服务单位派驻国家税务总局天津市税务局的人员必须与服务单位签订正式劳动合同和信息系统安全保密协议。

**第二包：**

一、项目背景

为全面落实《国家税务总局网络安全和信息化领导小组办公室关于落实网络安全等级保护制度和关键信息基础设施安全保护制度相关工作的通知》（税总信息办便函〔2021〕37号）中对信息系统合规性检查的相关工作要求，需要对信息系统进行等级保护测评、关键基础设施风险评估。

二、项目内容

购买14个三级信息系统、5个二级信息系统的等级保护测评服务和2个系统的关键基础设施风险评估服务。在规定时间内完成测评工作并出具测评报告，对测评中发现的问题出具整改建议书，并针对整改结果进行复查。

三、项目需求

## （一）等保测评及风险评估

在合同期内完成以下14个三级信息系统、5个二级信息系统的等级保护测评服务。在规定时间内完成测评工作并出具测评报告，对测评中发现的问题出具整改建议书，提出有针对性的加强完善信息系统安全管理和防护意见，并针对整改结果进行复查。

在合同期内完成以下2个系统的关键基础设施风险评估服务。围绕关键基础设施承载的核心业务，通过关键属性的识别和分析，对每个关键属性的具体描述内容的安全性逐一进行风险分析，给出风险分析的结果，最终根据风险分析的结果定性分析出整体安全状况。

|  |  |  |
| --- | --- | --- |
| **等保级别** | **信息系统** | **备注** |
| 三级 | 金税三期征收管理系统 | / |
| 金税三期社保费征管信息系统 | 关键信息基础设施风险评估 |
| 国家税务总局天津市税务局网站 | / |
| 增值税发票管理系统 | / |
| 国家税务总局天津市电子税务局 | 关键信息基础设施风险评估 |
| 超融合大数据平台系统 | / |
| 国家税务总局天津市税务局纳税服务平台 | / |
| 个税专门系统 | / |
| 自然人电子税务局 | / |
| 安全支撑运行平台 | / |
| 电子发票服务平台 | / |
| 税智撑平台 | / |
| 统一身份管理平台 | / |
| 云平台 | / |
| 二级 | 稽查视频指挥平台 | / |
| 财务管理系统 | / |
| 绩效管理信息系统 | / |
| 大企业税收服务与管理平台 | / |
| 天津税务综合监控系统 | / |

## （二）互联网安全检测部分

1.互联网暴露面检测

按照实际需要每年提供不少于4次，结合服务工具和人工分析，通过数据挖掘和调研的方式确定资产范围，基于网络扫描、搜索引擎、互联网基础数据引擎对暴露在互联网上的公网IP和端口等进行主动探测发现。采用 web 漏洞扫描技术、系统漏洞扫描技术、操作系统的探测技术、端口的探测技术、服务探测技术、 Web 爬虫技术等各类探测技术精准识别未报备的公网IP和端口，提前发现可能存在的安全隐患。

2.外部漏洞挖掘

按照每季度一次的频率，采用各种手段模拟真实的安全攻击，从而发现黑客入侵信息系统的潜在可能途径，要求测试方式以人工渗透为主，扫描工具为辅。评估内容包含外部威胁（包括但不限于 web 应用安全风险、业务安全风险、安全设备绕过等）与内部威胁（包括但不限于配置不当、弱口令、社工库利用、内部人员泄密[如源代码、文档、敏感文件、邮件]等）所带来的风险。发现黑客入侵互联网网站和各互联网信息系统的潜在可能途径，并出具相关漏洞报告及整改建议，跟进后续漏洞修复检验等。范围包含:向互联网提供服务 40个左右的各种业务系统、网站（动态交互式网站）、APP（安卓、IOS）、API 接口（服务器接口) 微信公众号/服务号等。

3.敏感信息泄露检查

按照实际需要每年开展不少于2次的外网敏感信息泄露检查，通过对涉及对Github 信息、百度网盘、百度文库、CSDN、暗网信息等监测，对天津税务泄露在外的系统源代码、邮件配置信息、数据库配置信息、FTP配置信息等各类信息以及涉及天津税务的关键岗位的个人信息、业务数据信息等进行过滤，消除潜在安全隐患，发现问题第一时间形成《互联网敏感信息泄露检查专项报告》提交。

四、项目实施要求

## （一）项目总体要求

服务单位需充分了解天津市税务局现有三级信息系统建设情况和项目需求，提出初步实施方案，在实施前提条件满足的情况下，根据国家税务总局天津市税务局确定的工作时间计划，合理组织和协调相关人员，在项目执行过程中，服务单位对被测试系统部署的相关配置信息负有保密责任。

## （二）项目实施要求

1.在项目实施过程中，应提交项目实施计划表。

2.每周服务单位需提交工作周报，内容应包括本周工作和下周工作安排等内容。

3.等保测评及风险评估工作应严格按照双方确认的工作方案开展，如遇任何变动，需在工作周报中及时提出，经甲方批准后方可变更。

4.服务单位需提供一名项目经理，主要负责人力资源调度、项目总体计划、与项目单位的实施协调和验收管理等工作。

5.项目实施过程中严格遵守保密协议约定，任何数据不得用于本次项目以外的其他用途。

6.项目实施过程中应控制风险，防止对应用系统运行造成影响。

7.项目经理具有工业和信息化部教育与考试中心颁发的高级信息安全管理工程师证书和网络安全等级测评高级测评师证书，实施小组人员具备网络安全等级测评中级测评师证书，实施小组人员中2名安全技术人员具备信息安全保障人员认证（CISAW）证书，同时具备注册信息安全专业人员-注册渗透测试工程师（CISP-PTE）证书。

五、项目验收要求

在服务期限内，服务单位按期提交相关工作成果，出具信息系统等级保护测评报告。提交报告数量、质量及国家税务总局天津市税务局出具的评价意见作为验收依据。服务单位需按照国家税务总局天津市税务局验收程序要求，提供相应验收材料。由天津市税务局召开验收工作会，验收合格后按规定进入付款流程。

六、项目技术支持服务要求

项目组应明确项目经理和项目组成员，如相关成员无法参加本项目，由同等资质人员替换，并由服务单位出具人员替换说明，且提供相应人员的资质证书。

1.在项目实施过程开始，应提交项目实施计划表。

2.每周实施方需提交工作周报，内容应包括本周工作内容和下周工作安排等内容。

3.等保测评、风险评估工作应严格按照双方确认的工作方案开展，如遇任何变动，须在工作周报中及时提出，经委托方批准后方可变更。

4.项目实施过程中严格遵守保密协议约定，任何数据不得用于本次项目以外的其他用途。

5.项目实施过程中应控制风险，防止对应用系统运行造成影响。

6.针对工具测试等环节需要做好相应的应急预案以及操作规范。

7.项目实施应具有完善的测评方案，包括物理安全、主机安全、网络安全、应用安全、数据备份与恢复，管理安全等。

七、税收信息化项目开发和应用管理工作要求

项目验收过程中，验收组成员将按照合同内容和工作要求对该项目进行审核，要求服务单位确保合同中涉及内容均已阶段性完成，完整提供交付文档和验收文档等。

遵照税务总局信息化服务单位失信行为记录名单制度(试行)相关规定，按照相关流程对服务单位失信行为进行认定和修复，出现服务单位严重失信行为立即终止合同，并追究服务单位相关责任。

八、其他要求

1.承担相关技术支持人员的安全和保密管理责任，服务单位必须签订《国家税务总局天津市税务局保密协议书》，技术支持人员必须签订《国家税务总局天津市税务局保密承诺书》。

2.对技术支持人员承担的工作应进行安全保密风险分析，明确技术支持人员工作范围和边界，重点防范设备和资料失窃、误操作导致的软硬件故障、敏感信息泄露、对信息系统的越权操作和恶意攻击等风险，严格按照有关部门和招标人相关安全保密管理要求实施管理。

3.严格控制技术支持人员处理内部文件、获取税务数据的范围和权限，包括不得随意将携带的电脑和移动存储介质接入税务专网。

4.严格内外网管理，未经允许，不得擅自从内网拷贝并向外携带办公区数据、文档、程序等信息资源，确因工作需要，须填写申请，报主管应用系统负责人审批，并经运维支持中心备案后，方可实施相关操作。外网的数据进入内网，必须在指定计算机上，并进行严格检查杀毒后，方可进入内网，避免将病毒或木马等带入。

5.办公区计算机设备使用和安全要求严格遵循天津市相关规范。未经允许不得在公用计算机上保留各类工作文档及数据。办公区外网计算机需安装指定系统及防毒软件等必要软件，严禁接入办公区内网，不得保留与工作有关的文档、图片等电子文件，因工作需要上传下载的文件须及时删除。外网计算机统一配发使用账号，使用后需注销用户。

6.服务单位派驻国家税务总局天津市税务局的人员必须与服务单位签订正式劳动合同和信息系统安全保密协议。

**第三包：**

一、项目背景

为全面落实《中华人民共和国密码法》和《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》中对密码应用与安全性评估要求的要求，拟对三级信息系统开展密码应用安全性评估，评估我局现有的三级信息系统的应用是否合规、正确、有效，并通过测评发现应用系统存在的安全隐患和风险，出具密码应用安全性评估报告，并提出有针对性的加强完善密码安全管理和防护意见，对系统密码应用方案及改进后的被测系统提供咨询、评估服务。

二、项目内容

购买14个三级信息系统的密码应用安全性评估服务。分析整个被测信息系统及其涉及的业务应用系统，进行现场测评，协助用户认清风险，查找漏洞，找出差距，提出有针对性的加强完善密码安全管理和防护建议。

三、项目需求

1.在合同期内完成以下14个三级信息系统的密码应用安全性评估服务，出具密码应用安全性评估报告，并提出有针对性的加强完善密码安全管理和防护意见，对系统密码应用方案及改进后的被测系统提供咨询、评估服务。

|  |  |
| --- | --- |
| 序号 | 系统名称 |
| 1 | 金税三期征收管理系统 |
| 2 | 国家税务总局天津市税务局纳税服务平台 |
| 3 | 金税三期社保费征管信息系统 |
| 4 | 国家税务总局天津市税务局网站 |
| 5 | 增值税发票管理系统 |
| 6 | 国家税务总局天津市电子税务局 |
| 7 | 超融合大数据平台系统 |
| 8 | 个税专门系统 |
| 9 | 自然人电子税务局 |
| 10 | 安全支撑运行平台 |
| 11 | 电子发票服务平台 |
| 12 | 统一身份管理平台 |
| 13 | 云平台 |
| 14 | 税智撑平台 |

2.提供商用密码应用培训。从国家政策法规、国家密码标准、密码行业标准、密码要求规范等方面对甲方进行培训主要包括商用密码应用安全性评估的目的和意义、商用密码应用要求、商用密码测评要求等。

四、项目实施要求

## （一）项目总体要求

服务单位需充分了解天津市税务局现有三级信息系统建设情况和项目需求，提出初步实施方案，在实施前提条件满足的情况下，根据国家税务总局天津市税务局确定的工作时间计划，合理组织和协调相关人员，在项目执行过程中，服务单位对被测试系统部署的相关配置信息负有保密责任。

## （二）项目实施要求

1.制定测评实施方案。服务单位应结合制定测评实施方案，包括但不限于技术方案、项目组织、工作质量、保密措施、进度安排和应急响应等。测评实施方案应做到内容详实，服务流程清晰，实施进度安排详细合理，有完善的项目进度和质量管控制度。

2.制定培训方案。服务单位提供的培训方案应做到全面合理有效，具有详细的培训计划、培训师资力量、培训内容。供应商应安排具备相应资质和经验的技术人员，对天津市税务局的相关人员进行全流程使用培训，确保熟练掌握密评要求和密码知识。

3. 人员要求。服务单位需提供一名项目经理，主要负责人力资源调度、项目总体计划、与项目单位的实施协调和验收管理等工作。项目经理具备注册网络安全渗透评估专业人员（NSATP-A）证书、信息安全保障人员认证（CISAW）证书、信息系统安全认证专业人员（CISSP）证书，项目经理及测评技术人员应为本单位正式在职员工且均通过国家密码管理局组织的商用密码应用安全性评估人员测评能力考核，测评技术人员不得少于 4 人。

4.项目实施过程中严格遵守保密协议约定，任何数据不得用于本次项目以外的其他用途。

5.项目实施过程中应控制风险，防止对应用系统运行造成影响。

五、项目验收要求

在服务期限内，服务单位按期提交相关工作成果，交付《密码应用安全性评估实施方案》，出具《密码应用安全性评估报告》。提交报告数量、质量及国家税务总局天津市税务局出具的评价意见作为验收依据。服务单位需按照国家税务总局天津市税务局验收程序要求，提供相应验收材料。由天津市税务局召开验收工作会，验收合格后按规定进入付款流程。

六、项目技术支持服务要求

项目组应明确项目经理和项目组成员，如相关成员无法参加本项目，由同等资质人员替换，并由服务单位出具人员替换说明，且提供相应人员的资质证书。

七、税收信息化项目开发和应用管理工作要求

（一）失信认定

采购单位遵照《税务系统信息化服务商失信行为记录名单制度（试行)》对中标单位失信行为进行认定，并追究中标单位相关责任。

（二）安全和保密要求

１.中标单位应严格落实国家税务总局天津市税务局网络安全保密管理要求，承担技术支持人员的安全和保密管理责任。按采购单位要求签订中标单位保密协议书和技术支持人员保密承诺书。

２.中标单位承担派驻技术支持人员背景审查，提供其身份证明、履历、家庭成员及主要社会关系、无犯罪记录证明等材料，提交信息备案表。

３.中标单位负责派驻技术支持人员工作胜任、资格条件、以及网络安全能力评估，对技术支持人员承担的工作进行安全保密风险分析，明确技术支持人员工作范围和边界，重点防范设备和资料失窃、误操作导致的软硬件故障、敏感信息泄露、信息系统越权访问和网络攻击等风险。

４.中标单位负责派驻技术支持人员的网络和数据安全管理、网络安全意识、保密意识、网络安全法律法规、网络安全技能以及网络安全警示教育等培训，上岗前确保考核合格。

５.对“安全和保密责任”落实不严格、不到位，造成重大安全事件或产生负面影响的，按照合同中“其他终止合同情况”条款执行，并依照相关法律等规定进行追责。

（三）运行维护保障要求

１.中标单位在运行维护中出现运行故障（不可抗力因素除外）或发现违规操作，30分钟内未主动上报采购单位的，给予警告，并按次扣除合同总价款1‰的金额；合同生效期间累计扣除不超过合同总价款5%的金额。

２.中标单位在运行维护中出现巡检不及时、不到位的，按次扣除合同总价款1‰的金额；合同生效期间累计扣除不超过合同总价款的5%。

３.中标单位在运行维护中发现运行故障（不可抗力因素除外）、业务系统可用性低于50%或业务功能阻断等问题的，采购单位将根据中标单位处理时间（持续时间判定以采购单位通报为准）扣除合同总价款一定比例的金额。运行故障0.5小时≤持续时间＜4小时的，按次扣除合同总价款5‰的金额；运行故障4小时≤持续时间＜8小时的，按次扣除合同总价款1%的金额；运行故障持续时间≥8小时的，按次扣除合同总价款5%的金额。

（四）其他专项要求

１.禁止中标单位另行开发合同业务需求范围内供纳税人、缴费人使用的软件，对违反合约专门条款的，纳入失信名单。

２.中标单位在本项目实施过程中发生违反安全规定的行为，造成数据失窃或丢失、敏感信息泄露、主要业务系统瘫痪等不良后果的，自采购单位或采购单位主管机关做出认定结果之日起三年内，税务系统各单位可以拒绝中标单位参与税务系统政府采购活动。

３.中标单位应建立防止违法违规聘用离职税务人员的风险控制制度，出现违法违规聘用离职税务人员行为的，采购单位将采取包括但不限于要求其限期改正、支付违约金、解除合同、三年内限制参加所聘人员原单位及下属单位信息化项目政府采购活动等措施。

４.禁止中标单位采取馈赠礼品礼金、邀请娱乐旅游消费、提供便利条件等非正常交往手段“围猎”相关税务人员及亲属。一经发现，自发现之日起三年内，税务系统各单位可以拒绝中标单位参与税务系统政府采购活动。

八、其他要求

1.对技术支持人员承担的工作应进行安全保密风险分析，明确技术支持人员工作范围和边界，重点防范设备和资料失窃、误操作导致的软硬件故障、敏感信息泄露、对信息系统的越权操作和恶意攻击等风险，严格按照有关部门和招标人相关安全保密管理要求实施管理。

2.严格控制技术支持人员处理内部文件、获取税务数据的范围和权限，包括不得随意将携带的电脑和移动存储介质接入税务专网。

3.严格内外网管理，未经允许，不得擅自从内网拷贝并向外携带办公区数据、文档、程序等信息资源，确因工作需要，须填写申请，报主管应用系统负责人审批，并经运维支持中心备案后，方可实施相关操作。外网的数据进入内网，必须在指定计算机上，并进行严格检查杀毒后，方可进入内网，避免将病毒或木马等带入。

4.办公区计算机设备使用和安全要求严格遵循天津市相关规范。未经允许不得在公用计算机上保留各类工作文档及数据。办公区外网计算机需安装指定系统及防毒软件等必要软件，严禁接入办公区内网，不得保留与工作有关的文档、图片等电子文件，因工作需要上传下载的文件须及时删除。外网计算机统一配发使用账号，使用后需注销用户。

5.服务单位派驻国家税务总局天津市税务局的人员必须与服务单位签订正式劳动合同和信息系统安全保密协议。

**第四包：**

一、项目背景

由于税务总局垂直下发的密码组件目前存在密码应用不足、应用集成难、支持场景少等问题，无法满足我局当前的安全建设需求，因此，需要进一步完善现有密码组件的服务能力，解决各类密评中出现的问题。

二、项目内容

购买具有差异化、个性化的密码服务，如国密门禁身份鉴别服务、国密门禁数据完整性保护服务、通道加解密服务、高安全性身份鉴别服务等，进一步完善现有密码组件的服务能力，解决各类密评中出现的问题，梳理物理层、网络层、应用层和密码组件等四大密码服务提升场景，针对性解决现有的“卡脖子”问题，进一步实现业务系统的安全加固。

三、项目需求

1. 密码应用基础服务

**国密门禁身份鉴别服务：**使用采用国密算法的智能IC卡，基于国密SM4对称密码算法和密钥分散机制等密码技术对重要区域进入人员进行身份鉴别。

**国密门禁数据完整性保护服务：**基于PCI-E密码卡采用HMAC-SM3的消息鉴别码（MAC）机制对电子门禁系统进出记录数据进行存储完整性保护。

**通道加解密服务：**提供系统之间交互数据使用的传输加密，为系统与用户之间建立加密通道。支持SSL或IPSEC协议接入服务，支持国密算法。

**个人数字证书服务：**遵循国内相关标准颁发，用来证明个人在互联网上的数字身份。通过采用国产密码技术，采用SM2算法支撑客户端数字签名与签名认证等。

**设备数字证书服务：**遵循国内相关标准颁发，用来证明密码设备在互联网上的数字身份。

**磁盘级加解密服务：**采用透明化方式，对于重要的数据、文件等采用代码零改造的磁盘级加密存储技术，在无需修改应用程序的前提下，实现应用程序的可信存储环境，为应用程序提供透明、安全、高效、密评合规的存储加密功能。

### 密钥管理服务：密钥管理对于保证密钥全生存周期的安全性是至关重要的,可以保证密钥(除公钥外)不被非授权的访问、使用、泄露、修改和替换,可以保证公钥不被非授权的修改和替换。《中华人民共和国密码法》和《商用密码管理条例》等政策都要求商用密码的应用和管理应保障密钥管理的安全性。基于此，依据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，在密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等全生命周期进行安全管理。

**密码方案编制及更新服务：**梳理用户现状（包含系统使用单位情况、信息系统情况、软硬件信息情况、网络拓扑、信息资源分析、密码应用情况），形成符合国家、行业和用户要求的密码应用方案，并根据FAQ持续更新密码方案，使方案落地可行。

**密码咨询及改造服务：**根据税务实际场景，提供前期密码设计咨询服务以及后期密码集成对接及改造工作。

**安全管理制度编制服务：**制定密码应用安全管理制度，建立密码操作流程，设置密钥管理规则等。

**密码人员管理制度编制服务：**建立密码应用岗位责任制度，上岗人员培训制度，关键岗位人员保密制度及调离制度等。

**密码应用应急处置制度编制服务：**制定密码应用应急策略、应急处置方案等。

1. 密码应用提升服务

**高安全性身份鉴别服务：**增加基于SM2算法的国密数字证书认证登录方式，向用户USBKey配置基于SM2算法的国密数字证书，保证用户身份唯一性标识及身份信息的安全存储。

**增强级访问控制服务：**实现增强级访问控制，对访问控制信息做HMAC-SM3完整性保护。

**细粒度数据安全存储服务：**字段级细粒度的重要数据加解密，实现磁盘级安全服务上移，真正做到“数据可用不可见”。

**网络优化设计服务：**与税局网络安全组共同设计金三与金四的内网区、运维区，实现金三金四内网区、运维区互联互通。

**网络故障风险点优化评估服务：**调研应用负载均衡与VPN的功能差异，评估优化的可行性。

**网络层VPN统筹完善服务：**根据最新网络情况，重新设计VPN的部署方案，灵活调整VPN部署数量及位置。

**国密门禁-动力环境监控系统对接联调服务：**将国密门禁接入动力环境监控系统，实现动力对国密门禁的统一监控。

**国密视频监控-动力环境监控系统对接联调服务：**将国密视频监控接入动力环境监控系统，实现动力对国密视频监控的统一监控。

**物理智能设备密码改造支持服务：**对物理智能设备国产密码建设提供咨询、指导服务。

**密码组件调研评估服务：**深入细粒度调研密码机、签名验签服务器等密码组件的部署情况，评估复用粒度。

**密码组件对接改造服务：**将可复用的密码组件进一步对接改造，纳管到现有统一密码服务中，实现弹性扩容。

四、项目实施要求

## （一）项目总体要求

在工作开展中，通过提供差异化、个性化的密码服务，如国密门禁身份鉴别服务、国密门禁数据完整性保护服务、通道加解密服务、高安全性身份鉴别服务等，对现有的天津市税务信息系统进行改造，解决各类密评中出现的问题，进一步实现业务系统的安全加固。

## （二）项目人员要求

安排项目经理一名，要求从事密码服务工作3年以上，具有信息系统项目管理师（高级）、网络安全服务能力评价证书（CCSS-CM）；具体技术人员按照高级、中级技术人员合理分配，具备CISP注册信息安全工程师、软件设计师、数据库认证专家、售后服务管理师、信息系统项目管理师等证书，均要求有1年以上密码服务的工作经验。

五、项目验收要求

## （一）项目交付成果

1.按招标文件技术部分要求对服务进行验收，服务单位应在验收时提供相关周期性服务报告。

2.项目服务期内如果因技术人员问题，出现等保三级的信息系统密评不通过的情况时，按合同中违约条款追究责任。

## （二）项目验收文档

|  |  |  |
| --- | --- | --- |
| 产出物 | 频率 | 数量 |
| 国密门禁身份鉴别服务工作报告 | 按需 | 按需 |
| 国密门禁数据完整性保护服务工作报告 | 按需 | 按需 |
| 通道加解密服务工作报告 | 按需 | 按需 |
| 个人数字证书服务工作报告 | 按需 | 按需 |
| 设备数字证书服务工作报告 | 按需 | 按需 |
| 磁盘级加解密服务工作报告 | 按需 | 按需 |
| 密码方案编制及更新服务工作报告 | 按需 | 按需 |
| 密码咨询及改造服务工作报告 | 按需 | 按需 |
| 安全管理制度编制服务工作报告 | 按需 | 按需 |
| 密码人员管理制度编制服务工作报告 | 按需 | 按需 |
| 密码应用应急处置制度编制服务工作报告 | 按需 | 按需 |
| 高安全性身份鉴别服务工作报告 | 按需 | 按需 |
| 增强级访问控制服务工作报告 | 按需 | 按需 |
| 细粒度数据安全存储服务工作报告 | 按需 | 按需 |
| 网络优化设计服务工作报告 | 按需 | 按需 |
| 网络故障风险点优化评估服务工作报告 | 按需 | 按需 |
| 网络层VPN统筹完善服务工作报告 | 按需 | 按需 |
| 国密门禁-动力环境监控系统对接联调服务工作报告 | 按需 | 按需 |
| 国密视频监控-动力环境监控系统对接联调服务工作报告 | 按需 | 按需 |
| 物理智能设备密码改造支持服务工作报告 | 按需 | 按需 |
| 密码组件调研评估服务工作报告 | 按需 | 按需 |
| 密码组件对接改造服务工作报告 | 按需 | 按需 |

项目验收过程中，验收组成员将按照合同内容和工作要求对该项目进行审核，要求服务单位确保合同中涉及内容均已阶段性完成，完整提供交付文档和验收文档等。

六、税收信息化项目开发和应用管理工作要求

（一）失信认定

甲方遵照《税务系统信息化服务商失信行为记录名单制度（试行)》对乙方失信行为进行认定，并追究乙方相关责任。

（二）安全和保密要求

１.乙方应严格落实国家税务总局天津市税务局网络安全保密管理要求，承担技术支持人员的安全和保密管理责任。按甲方要求签订乙方保密协议书和技术支持人员保密承诺书。

２.乙方承担派驻技术支持人员背景审查，提供其身份证明、履历、家庭成员及主要社会关系、无犯罪记录证明等材料，提交信息备案表。

３.乙方负责派驻技术支持人员工作胜任、资格条件、以及网络安全能力评估，对技术支持人员承担的工作进行安全保密风险分析，明确技术支持人员工作范围和边界，重点防范设备和资料失窃、误操作导致的软硬件故障、敏感信息泄露、信息系统越权访问和网络攻击等风险。

４.乙方负责派驻技术支持人员的网络和数据安全管理、网络安全意识、保密意识、网络安全法律法规、网络安全技能以及网络安全警示教育等培训，上岗前确保考核合格。

５.对“安全和保密责任”落实不严格、不到位，造成重大安全事件或产生负面影响的，按照合同中“其他终止合同情况”条款执行，并依照相关法律等规定进行追责。

（三）其他专项要求

１.禁止乙方另行开发合同业务需求范围内供纳税人、缴费人使用的软件，对违反合约专门条款的，纳入失信名单。

２.乙方在本项目实施过程中发生违反安全规定的行为，造成数据失窃或丢失、敏感信息泄露、主要业务系统瘫痪等不良后果的，自甲方或甲方主管机关做出认定结果之日起三年内，税务系统各单位可以拒绝乙方参与税务系统政府采购活动。

３.乙方应建立防止违法违规聘用离职税务人员的风险控制制度，出现违法违规聘用离职税务人员行为的，甲方将采取包括但不限于要求其限期改正、支付违约金、解除合同、三年内限制参加所聘人员原单位及下属单位信息化项目政府采购活动等措施。

４.禁止乙方采取馈赠礼品礼金、邀请娱乐旅游消费、提供便利条件等非正常交往手段“围猎”相关税务人员及亲属。一经发现，自发现之日起三年内，税务系统各单位可以拒绝乙方参与税务系统政府采购活动。

七、其他要求

1.承担相关技术支持人员的安全和保密管理责任，服务单位必须签订《国家税务总局天津市税务局保密协议书》，技术支持人员必须签订《国家税务总局天津市税务局保密承诺书》。

2.对技术支持人员承担的工作应进行安全保密风险分析，明确技术支持人员工作范围和边界，重点防范设备和资料失窃、误操作导致的软硬件故障、敏感信息泄露、对信息系统的越权操作和恶意攻击等风险，严格按照有关部门和招标人相关安全保密管理要求实施管理。

3.严格控制技术支持人员处理内部文件、获取税务数据的范围和权限，包括不得随意将携带的电脑和移动存储介质接入税务专网。

4.严格内外网管理，未经允许，不得擅自从内网拷贝并向外携带办公区数据、文档、程序等信息资源，确因工作需要，须填写申请，报主管应用系统负责人审批，并经运维支持中心备案后，方可实施相关操作。外网的数据进入内网，必须在指定计算机上，并进行严格检查杀毒后，方可进入内网，避免将病毒或木马等带入。

5.办公区计算机设备使用和安全要求严格遵循天津市相关规范。未经允许不得在公用计算机上保留各类工作文档及数据。办公区外网计算机需安装指定系统及防毒软件等必要软件，严禁接入办公区内网，不得保留与工作有关的文档、图片等电子文件，因工作需要上传下载的文件须及时删除。外网计算机统一配发使用账号，使用后需注销用户。

6.服务单位派驻国家税务总局天津市税务局的人员必须与服务单位签订正式劳动合同和信息系统安全保密协议。

第三部分 投标须知

A 说明

1. 概述

1.1 根据《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》《中华人民共和国招标投标法》等有关法律、法规和规章的规定，本采购项目已具备招标条件。

1.2 本招标文件仅适用于投标邀请函中所叙述项目货物和服务的采购。

1.3 参与招标投标活动的所有各方，对在参与招标投标过程中获悉的国家、商业和技术秘密以及其它依法应当保密的内容，均负有保密义务，违者应对由此造成的后果承担全部法律责任。

2. 定义

2.1 “采购人”和“招标人”系指本次招标活动的采购单位。“采购代理机构”系指组织本次招标活动的机构，即“天津市政府采购中心”。

2.2 “投标人”系指响应招标、参加投标竞争的法人、其他组织或者自然人。

2.3 “服务”系指招标文件规定的投标人为完成采购项目所需承担的全部义务。

3. 解释权

3.1 本次招投标的最终解释权归为采购人、采购代理机构。

3.2 本文件未作须知明示，而又有相关法律、法规规定的，采购人、采购代理机构将对此解释为依据有关法律、法规的规定。

4. 合格的投标人

4.1 符合《中华人民共和国政府采购法》第二十二条供应商参加政府采购活动应当具备的条件及其他有关法律、法规关于供应商的有关规定，有能力提供招标采购服务的供应商。

4.2 符合《投标邀请函》中关于供应商资格要求（实质性要求）的规定。

4.3 关于联合体投标

若《投标邀请函》接受联合体投标的：

（1）两个以上的自然人、法人或者其他组织可以组成一个联合体，以一个供应商的身份共同参加政府采购。

（2）联合体各方均应当符合《政府采购法》第二十二条第一款规定的条件，根据采购项目的特殊要求规定投标人特定条件的，联合体各方中至少应当有一方符合《投标邀请函》规定的供应商资格条件（实质性要求）。

（3）联合体各方之间应当签订共同投标协议并在投标文件内提交，明确约定联合体主体及联合体各方承担的工作和相应的责任。联合体各方签订共同投标协议后，不得再以自己名义单独在同一合同项下投标，也不得组成新的联合体参加同一合同项下的投标。

（4）下载招标文件时，应以联合体协议中确定的主体方名义下载。

（5）联合体投标的，应以主体方名义提交投标保证金（如有），对联合体各方均具有约束力。

（6）由同一专业的单位组成的联合体，按照同一项资质等级较低的单位确定资质等级。业绩等有关打分内容根据共同投标协议约定的各方承担的工作和相应责任，确定一方打分，不累加打分；评审标准无明确或难以明确对应哪一方的打分内容按主体方打分。

（7）联合体中任意一方为中小企业的，该方应提供《中小企业声明函》。

（8）联合体各方应当共同与采购人签订采购合同，就采购合同约定的事项对采购人承担连带责任。

4.4 关于关联企业

除联合体外，法定代表人或单位负责人为同一个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投标。如同时参加，则评审时将同时被拒绝。

4.5 关于中小微企业参与投标

中小微企业是指符合《政府采购促进中小企业发展管理办法》（财库[2020]46号）规定的供应商。中小微企业参与投标应提供《中小企业声明函》。

根据财库〔2014〕68号《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》，监狱企业视同小微企业。监狱企业是指由司法部认定的为罪犯、戒毒人员提供生产项目和劳动对象，且全部产权属于司法部监狱管理局、戒毒管理局、直属煤矿管理局，各省、自治区、直辖市监狱管理局、戒毒管理局，各地(设区的市)监狱、强制隔离戒毒所、戒毒康复所，以及新疆生产建设兵团监狱管理局、戒毒管理局的企业。监狱企业投标时，提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件，不再提供《中小企业声明函》。

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，残疾人福利性单位视同为小型、微型企业。

4.6 关于分公司投标

分公司作为投标人参与本项目政府采购活动的，应提供具有法人资格的总公司的营业执照副本扫描件及法人企业授权书，法人企业授权书须加盖总公司公章。总公司可就本项目或此类项目在一定范围或时间内出具法人企业授权书。已由总公司授权的，总公司取得的相关资质证书对分公司有效，法律法规或者行业另有规定的除外。

4.7 关于提供前期服务的供应商

为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加该采购项目的其他采购活动。

5. 合格的服务

5.1 投标人所提供的服务应当没有侵犯任何第三方的知识产权、技术秘密等合法权利。

5.2 投标人提供的服务应当符合招标文件的要求，并且其质量完全符合国家标准、行业标准或地方标准。

5.3 系统软件、通用软件必须是具有在中国境内的合法使用权或版权的正版软件，涉及到第三方提出侵权或知识产权的起诉及支付版税等费用由投标人承担所有责任及费用。

6. 投标费用

无论投标过程中的做法和结果如何，投标人自行承担所有与参加投标有关的费用。

7. 信息发布

本项目需要公开的有关信息，包括招标公告、更正公告、中标公告、终止公告等与招标活动有关的通知，采购人、采购代理机构均将通过“中国政府采购网（http://www.ccgp.gov.cn/）”和“天津政府采购中心网（http://tjgpc.zwfwb.tj.gov.cn）”公开发布。投标人在参与本采购项目招投标活动期间，请及时关注上述媒体和天津市政府采购中心招投标系统“查看项目文件”的相关信息。因没有及时关注而未能如期获取相关信息，投标人自行承担由此可能产生的风险。

8. 询问与质疑

8.1 根据《政府采购质疑和投诉办法》（财政部令第94号）、《天津市财政局关于转发<财政部关于进一步加强政府采购需求和履约验收管理的指导意见>的通知》（津财采[2017]4号）的要求及委托代理协议的授权范围，针对采购文件的询问、质疑应当向采购人提出；针对采购过程、采购结果的询问、质疑应当向天津市政府采购中心提出。

8.2 询问

（1）询问可以采取电话、当面或书面等形式。

（2）采购人应当自收到供应商询问之日起3个工作日内作出答复，但答复的内容不得涉及商业秘密或者依法应当保密的内容。

8.3 质疑

（1）提出质疑的供应商应当是参与所质疑项目采购活动的供应商。

（2）供应商认为采购文件、采购过程和采购结果使自己的权益受到损害的，可以在知道或者应知其权益受到损害之日起七个工作日内，以书面原件形式针对同一采购程序环节一次性向采购人提出质疑，否则不予受理。

（3）质疑函应当符合《政府采购质疑和投诉办法》（财政部令第94号）第十二条的规定，并按照统一格式提出（具体格式可参照天津市政府采购网（http://tjgp.cz.tj.gov.cn）“下载专区”中的“质疑函格式文本”）。质疑函应当明确阐述采购文件、采购过程、采购结果使自己的合法权益受到损害的法律依据、事实依据、相关证明材料及证据来源，以便于有关单位调查、答复和处理。

（4）供应商质疑应当有明确的请求和必要的证明材料。质疑内容不得含有虚假、恶意成份。依照谁主张谁举证的原则，提出质疑者必须同时提交相关确凿的证据材料和注明证据的确切来源，证据来源必须合法，采购人或天津市政府采购中心有权将质疑函转发质疑事项各关联方，请其作出解释说明。对捏造事实、滥用维权扰乱采购秩序的恶意质疑者，将上报天津市财政局政府采购处依法处理。

8.4 针对询问或质疑的答复内容需要修改采购文件的，其修改内容应当以政府采购网发布的更正公告为准。

9. 其他

本《投标须知》的条款如与《投标邀请函》、《招标项目需求》就同一内容的表述不一致的，以《投标邀请函》、《招标项目需求》中规定的内容为准。

B 招标文件说明

10. 招标文件的构成

10.1招标文件由下述部分组成：

（1）投标邀请函

（2）招标项目需求

（3）投标须知

（4）合同条款

（5）投标文件格式

（6）本项目招标文件的更正公告内容（如有）

10.2 除非有特殊要求，招标文件不单独提供招标项目使用地的自然环境、气候条件、公用设施等情况，投标人被视为熟悉上述与履行合同有关的一切情况。

10.3 加注“★”号条款为实质性条款，不得出现负偏离，发生负偏离即做无效标处理。

10.4 招标文件中涉及的参照品牌、型号仅起说明作用，并没有任何限制性，投标人在投标中可以选用其他替代品牌或型号，但这些替代要实质上优于或相当于招标要求。

11. 招标文件的澄清和修改

11.1 投标截止前，采购人、采购代理机构需要对招标文件进行补充或修改的，采购人、采购代理机构将会通过“中国政府采购网”、“天津市政府采购中心网”以更正公告形式发布。

11.2 更正公告一经在“中国政府采购网”、“天津市政府采购中心网”发布，天津市政府采购中心招投标系统将自动发送通知至已获取招标文件供应商的“查看项目文件”，视同已书面通知所有招标文件的收受人。请参与项目的供应商及时关注更正公告，由此导致的风险由投标人自行承担，采购人、采购代理机构不承担任何责任。

11.3 更正公告的内容为招标文件的组成部分。当招标文件与更正公告就同一内容的表述不一致时，以最后发出的更正公告内容为准。

11.4 招标文件的澄清、答复、修改或补充都应由采购代理机构以更正公告形式发布，除此以外的其他任何澄清、修改方式及澄清、修改内容均属无效，不得作为投标的依据，由此导致的风险由投标人自行承担，采购人、采购代理机构不承担任何责任。

12. 答疑会和踏勘现场

12.1 采购人、采购代理机构召开答疑会的，所有投标人应按《投标邀请函》规定的时间、地点参加答疑会。投标人如不参加，其风险由投标人自行承担，采购人、采购代理机构不承担任何责任。

12.2 采购人、采购代理机构组织踏勘现场的，所有投标人按《投标邀请函》规定的时间、地点参加踏勘现场活动。投标人如不参加，其风险由投标人自行承担，采购人、采购代理机构不承担任何责任。

12.3 采购人、采购代理机构在答疑会或踏勘现场中口头介绍的情况，除经“中国政府采购网”、“天津市政府采购中心网”以更正公告的形式发布外，不构成对招标文件的修改，不作为投标人编制投标文件的依据。

C 投标文件的编制

13. 要求

13.1 投标人应仔细阅读招标文件的所有内容，按招标文件要求编制投标文件，以使其投标对招标文件做出实质性响应。否则，其投标文件可能被拒绝，投标人须自行承担由此引起的风险和责任。

13.2 投标人应根据招标项目需求和投标文件格式编制投标文件，保证其真实有效，并承担相应的法律责任。

13.3 投标人应对投标文件所提供的全部资料的真实性承担法律责任，并无条件接受采购人、采购代理机构对其中任何资料进行核实（核对原件）的要求。采购人、采购代理机构核对发现有不一致或供应商无正当理由不按时提供原件的，按有关规定执行。

14. 投标语言及计量单位

14.1 投标人和采购代理机构就投标交换的文件和来往信件，应以中文书写，全部辅助材料及证明材料均应有中文文本，并以中文文本为准。外文资料必须提供中文译文，并保证与原文内容一致，否则投标人将承担相应法律责任。除签名、盖章、专用名称等特殊情形外，以中文以外的文字表述的投标文件，评标委员会有权拒绝其投标。

14.2 除在招标文件中另有规定，投标文件所使用的计量单位均应使用中华人民共和国法定计量单位。

15. 投标文件格式

15.1 投标人应按招标文件中提供的投标文件格式完整填写。因不按要求编制而引起系统无法检索、读取相关信息时，其后果由投标人自行承担。

15.2 投标人可对本招标文件“招标项目要求”所列的所有服务进行投标，也可只对其中一包或几包的服务投标；若无特殊说明，每一包的内容不得分项投标，原则上按照整包确定中标供应商。

15.3 投标人根据招标文件的规定和采购项目的实际情况，拟在中标后将中标项目的非主体、非关键性工作分包的，应当在投标文件中载明分包承担主体，分包承担主体应当具备相应资质条件且不得再次分包。

15.4 如投标多个包的，要求按包分别独立制作投标文件。

15.5 投标文件（包括封面和目录）的每一页，从封面开始按阿拉伯数字1、2、3…顺序编制页码。

16. 投标报价

16.1 投标书、开标一览表等各表中的报价，若无特殊说明应采用人民币填报。

16.2 投标报价是为完成招标文件规定的一切工作所需的全部费用的最终优惠价格。

16.3 除《招标项目需求》中说明并允许外，投标的每一个货物、服务的单项报价以及采购项目的投标总价均只允许有一个报价，任何有选择的报价，采购人、采购代理机构均将予以拒绝。

17. 投标人资格证明文件

投标人必须提交证明其有资格进行投标和有能力履行合同的文件，作为投标文件的一部分。

（1）《投标邀请函》中规定的供应商资格要求（实质性要求）证明文件；

（2）若国家及行业对投标项目有特殊资格要求的，还须提供特殊资格证明文件；

（3）涉及本须知中“4. 合格的投标人”相关要求的，按其要求执行。

18. 技术响应文件

18.1 投标人须提交证明其拟提供的服务符合招标文件规定的技术响应文件，作为投标文件的一部分。

18.2 上述技术响应文件可以是文字资料、图纸或数据，其内容应包括但不限于人力、物力等资源的投入以及服务内容、方式、手段、措施、质量保证及建议等。

19. 投标保证金

19.1 按照《招标项目要求》要求执行。

19.2 符合《政府采购货物和服务招标投标管理办法》和《政府采购法实施条例》相关规定。

20. 投标有效期

20.1 投标有效期为提交投标文件的截止之日起60天。投标书中规定的有效期短于招标文件规定的，其投标将被拒绝。

20.2 特殊情况下，采购代理机构可于投标有效期满之前，向投标人提出延长投标有效期的要求。答复应以书面形式进行。投标人可以拒绝上述要求，但不被没收投标保证金。对于同意该要求的投标人，既不要求也不允许其修改投标文件，但将要求其延长投标保证金的有效期。

21. 投标文件的签署及规定

21.1 投标文件应按《招标项目要求》和《投标文件格式》如实编写，未尽事宜可自行补充。投标文件内容不完整、格式不符合导致投标文件被误读、漏读或者查找不到相关内容的，投标人自行承担由此产生的风险。

21.2 投标人按照《投标邀请函》的要求提交网上应答并上传加盖投标人电子签章的PDF格式电子投标文件（以通过天津公共资源电子签章客户端正确读取签章信息为准）。

21.3 若有修改须于规定时间内重新提交电子投标文件。投标文件因模糊不清或表达不清所引起的后果由投标人自负。

D 投标文件的网上应答和提交

22. 投标人须按《投标邀请函》规定提交网上应答并上传加盖投标人电子签章的PDF格式电子投标文件（以通过天津公共资源电子签章客户端正确读取签章信息为准）。具体方式：使用天津数字认证有限公司发出的CA数字证书（原天津市电子认证中心发出尚在有效期内的CA数字证书仍可使用）登陆天津市政府采购中心网（网址：http://tjgpc.zwfwb.tj.gov.cn）-”网上招投标”-“供应商登录”-“市级集采机构入口”提交网上应答并上传加盖投标人电子签章的PDF格式电子投标文件（以通过天津公共资源电子签章客户端正确读取签章信息为准）。如有需要，投标人可于工作时间且在招标文件规定的截止时间前到天津市河东区红星路79号天津市政府采购中心窗口完成上述操作。

23. 制作和上传电子投标文件要求

23.1 投标人须下载天津市政府采购中心网-下载中心-《天津公共资源电子签章客户端安装包及使用说明》。

23.2 投标人须按照招标文件的规定制作电子投标文件，对所需提供的一切纸质材料进行扫描后加入电子投标文件，按照《天津公共资源电子签章客户端安装包及使用说明》规定的要求制作加盖投标人电子签章的PDF格式电子投标文件（以通过天津公共资源电子签章客户端正确读取签章信息为准），并于投标截止时间前上传至天津市政府采购中心招投标系统。

特别提醒：

（1）由于投标人网络接入速率不可控等网络传输风险，建议投标人在网上应答上传加盖电子签章的PDF文件后，对上传文件进行下载，核对文件完整性，如是否缺页少页、图片是否显示完整、签章是否有效等，并按照《天津公共资源电子签章客户端安装包及使用说明》要求的文件检查方法进行检查，确保投标文件上传准确、有效。

（2）投标人应当按照天津公共资源电子签章客户端使用说明的要求使用电子签章客户端软件。不按本使用说明使用电子签章客户端软件，或使用word等其它软件进行签章工作，将会造成天津公共资源电子签章客户端无法读取签章信息，并导致投标无效。

23.3 投标人须保证电子投标文件清晰，便于识别，如因上传、扫描、格式等原因导致评审时受到影响，由投标人自行承担相应责任。

24. 投标人须承诺接受电子投标的方式，并自行承担由此带来的废标、无效投标的风险。

25. 未按招标文件的规定提交网上应答和上传加盖投标人电子签章的PDF格式电子投标文件（以通过天津公共资源电子签章客户端正确读取签章信息为准）的投标将被拒绝。

E 开标和评标

26. 开标解密和资格审查

26.1 投标人须于《投标邀请函》中规定的时间内使用天津数字认证有限公司发出的CA数字证书（原天津市电子认证中心发出尚在有效期内的CA数字证书仍可使用）登陆天津市政府采购中心网（网址：http://tjgpc.zwfwb.tj.gov.cn）-”网上招投标”-“供应商登录”-“市级集采机构入口”完成开标解密。

26.2 由于投标人原因，没有在规定时间内进行网上开标解密，视为无效投标。

26.3 开标解密后，对开标结果进行网上公示，投标人报价为空、为零的将被视为无效投标。

26.4 开标解密后，投标代表人应保持电话畅通并具备相应的网络环境，随时准备接受评委的网上询标。

26.5 投标人须于规定时间内通过天津市政府采购中心招投标系统“询标解答”对评委的网上询标予以解答。如投标代表人被要求到评审现场答疑时，须携带身份证等有效证件原件，以备查验。

26.6 投标截止时间后，投标人不足3家的，不得开标。

26.7 开标解密后，采购人或采购代理机构应当依法对投标人的资格进行审查。资格审查合格的投标人不足3家的，不得评标。

27. 评标委员会

27.1 评标委员会成员由采购人代表和评审专家组成，成员人数应当为5人以上单数，其中评审专家不得少于成员总数的三分之二。

27.2 评标委员会负责审查投标文件是否符合招标文件的要求，并进行审查、询标、评估和比较。评标委员会认为必要时，可向投标人进行询标。

27.3 出现符合专业条件的供应商或者对招标文件作实质性响应的供应商不足三家，或投标人的报价均超过了采购预算，采购人不能支付的情况时，或出现影响采购公正的违法、违规行为时，评标委员会有权宣布废标。

27.4 评标委员会负责完成全部评标工作，向采购人提出经评标委员会签字的书面评标报告。

28. 对投标文件的审查和响应性的确定

28.1 符合性检查。评标委员会依据法律法规和招标文件的规定，对投标文件的内容是否完整、有无计算错误、要求的保证金是否已提供、文件签署是否正确、实质性要求等进行审查，确定每份投标文件是否实质上响应了招标文件的要求。

28.2 投标截止时间后，除评标委员会要求提供外，不接受投标人及与投标人有关的任何一方递交的材料。

28.3 实质上没有响应招标文件要求的投标文件，将被拒绝。投标人不得通过修改或撤回不符合要求的重大偏离而使其投标成为响应性的投标。如出现下列情况之一的，其投标将被拒绝或中标无效：

（1）投标文件未按招标文件的要求加盖电子签章的；

（2）投标有效期短于招标文件要求的；

（3）投标文件中提供虚假材料的；

（4）不能满足招标文件中任何一条实质性要求或加注“★”号条款出现负偏离或经评标委员会认定未实质性响应招标文件要求的或投标内容不符合相关强制性规定的；

（5）未按时进行网上解密或电子投标文件损坏、无效的；

（6）投标报价超出采购预算或最高限价；

（7）存在串通情形的；

（8）单位负责人或法定代表人为同一人，或者存在控股、管理关系的不同供应商，参加同一合同项下投标的，相关投标均无效；

（9）其他法定投标无效的情形。

28.4 评标委员会对确定为实质上响应的投标进行审核，投标文件报价出现前后不一致的，修改错误的原则如下：

（1）投标文件中开标一览表（报价表）内容与投标文件中相应内容不一致的，以开标一览表（报价表）为准；

（2）大写金额和小写金额不一致的，以大写金额为准；

（3）单价金额小数点或者百分比有明显错位的，以开标一览表的总价为准，并修改单价；

（4）总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。

（5）同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的报价经投标人确认后产生约束力，投标人不确认的，其投标无效。

28.5 评标委员会将要求投标人按上述修改错误的方法调整投标报价，投标人同意后，调整后的报价对投标人起约束作用。如果投标人不接受修改后的报价，其投标将被拒绝。

29. 投标文件的澄清

29.1 澄清有关问题。为了有助于对投标文件进行审查、评估和比较，评标委员会有权要求投标人对投标文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容作出必要的澄清、说明或者纠正。投标人有义务按照评标委员会通知的时间、地点指派投标代表人就相关问题进行澄清。

29.2 投标人澄清、说明、答复或者补充的内容须为PDF格式并加盖电子签章后上传至天津市政府采购中心招投标系统。

29.3 投标人的澄清、说明、答复或者补充应在规定的时间内完成，并不得超出投标文件的范围或对投标内容进行实质性的修改。

29.4 澄清文件将作为投标文件的一部分，与投标文件具有同等的法律效力。

30. 投标的评估和比较

评标委员会将根据招标文件确定的评标原则和评标方法对确定为实质上响应招标文件要求的投标进行评估和比较。

31. 评标原则和评标方法

31.1 评标原则

（1）评标委员会应当按照客观、公正、审慎的原则，根据招标文件规定的评审程序、评审方法和评审标准进行独立评审。

（2）评标委员会发现招标文件存在歧义、重大缺陷导致评标工作无法进行，或者招标文件内容违反国家有关强制性规定的，应当停止评标工作，与采购人或者采购代理机构沟通并作书面记录。采购人或者采购代理机构确认后，应当修改招标文件，重新组织采购活动。

（3）对招标文件中描述有歧义或前后不一致的地方，但不影响项目评审的，评标委员会有权进行评判，但对同一条款的评判应适用于每个投标人。

（4）评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。

31.2 评标方法

（1）采用“综合评分法”的评标方法，具体评审因素详见《招标项目需求》。评标采用百分制，各评委独立分别对实质上响应招标文件的投标进行逐项打分，对评标委员会各成员每一因素的打分汇总后取算术平均分，该平均分为供应商的得分。

（2）根据《中华人民共和国政府采购法实施条例》和《关于进一步规范政府采购评审工作有关问题的通知》（财库〔2012〕69号）的规定，评标委员会成员要依法独立评审，并对评审意见承担个人责任。评标委员会成员对需要共同认定的事项存在争议的，按照少数服从多数的原则做出结论。持不同意见的评标委员会成员应当在评审报告上签署不同意见并说明理由，否则视为同意。

（3）评标委员会审查产品资质或检测报告等相关文件符合性时，应综合考虑行业特点、交易习惯、采购需求最本质原义等情况，而不应以投标文件中产品名称与招标文件产品名称是否一致作为审查的标准。

（4）中标候选供应商产生办法：按得分由高到低顺序确定中标候选供应商；得分相同的，按投标报价由低到高顺序确定中标候选供应商；得分且投标报价相同的，按技术指标优劣顺序确定中标候选供应商，采购人或评标委员会经采购人授权后按中标候选供应商顺序确定中标供应商。

（5）根据《政府采购货物和服务招标投标管理办法》（财政部令第87号）第43条规定，如评审现场经财政部门批准本项目转为其他采购方式的，按相应采购方式程序执行。

32. 其他注意事项

32.1 在开标、投标期间，投标人不得向评标委员会成员或采购代理机构询问评标情况、施加任何影响，不得进行旨在影响评标结果的活动。

32.2 为保证定标的公正性，在评标过程中，评标委员会成员不得与投标人私下交换意见。在开、评标期间及招标工作结束后，凡与评标情况有接触的任何人不得透露审查、澄清、评价和比较等投标的有关资料以及授标建议等评标情况。

32. 3 本项目不接受赠品、回扣或者与采购无关的其他商品、服务。

F 授予合同

33. 中标供应商的产生

33.1 采购人可以事先授权评标委员会直接确定中标供应商。

33.2 采购人也可以按照《政府采购法》及其实施条例等法律法规的规定和招标文件的要求确认中标供应商。

34. 中标通知

34.1 中标公告发布同时，采购代理机构将通过天津市政府采购中心招投标系统以电子形式向中标供应商发出《中标通知书》（请使用天津数字认证有限公司发出的CA数字证书（原天津市电子认证中心发出尚在有效期内的CA数字证书仍可使用）登陆天津市政府采购中心网（网址：http://tjgpc.zwfwb.tj.gov.cn）-”网上招投标”-“供应商登录”-“市级集采机构入口”，并从“供应商系统”的“查看项目文件”中获取）。《中标通知书》一经发出即发生法律效力。

35. 投标人可使用天津数字认证有限公司发出的CA数字证书（原天津市电子认证中心发出尚在有效期内的CA数字证书仍可使用）登陆天津市政府采购中心网（网址：http://tjgpc.zwfwb.tj.gov.cn）-”网上招投标”-“供应商登录”-“市级集采机构入口”，并从“供应商系统”的“项目资审情况”中获取未通过资格审查的原因或从“供应商系统”的“查看排序和得分”中获取未中标人本人的评审得分与排序。

36. 签订合同

36.1 采购人与中标供应商应当在中标通知书发出之日起三十日内，按照招标文件确定的事项签订政府采购合同。合同文本请使用天津数字认证有限公司发出的CA数字证书（原天津市电子认证中心发出尚在有效期内的CA数字证书仍可使用）登陆天津市政府采购中心网（网址：http://tjgpc.zwfwb.tj.gov.cn）-”网上招投标”-“供应商登录”-“市级集采机构入口”，并从“供应商系统”的“合同”中获取。

36.2 招标文件、中标供应商的投标文件及其澄清文件等，均为签订合同的依据，且为合同的组成部分。

37. 履约保证金

37.1 若《招标项目要求》规定须提交履约保证金的，中标供应商须按照规定要求提交履约保证金。

37.2 中标供应商未能按合同规定履行其义务，采购人有权没收其履约保证金。

38. 中标供应商拒绝与采购人签订合同的，采购人可以按照评审报告推荐的中标候选人名单排序，确定下一候选人为中标供应商，也可以重新开展政府采购活动。

39. 合同分包

39.1 未经采购人同意，中标供应商不得分包合同。

39.2 政府采购合同分包履行的，中标供应商就采购项目和分包项目向采购人负责，分包供应商就分包项目承担责任。

第四部分 合同条款

**合同一般条款**

需方：

供方：

供、需双方根据 项目（项目编号：TGPC-201 - ）的政府采购结果和招标文件的要求，并经双方协商一致，达成 合同：

* 本合同为中小企业预留合同
* 本合同非中小企业预留合同

鉴于政府采购使用的合同文本的特殊性，本合同一般条款仅作为确立法律关系框架作用，具体合同的权利义务等内容以双方签订的专业合同为准，该合同作为本政府采购合同附件，与本合同具有同等法律效力，如附件合同没有而合同一般条款有的且涉及政府采购性质的内容，以合同一般条款内容为准。

一、采购内容： （详见附件）

合同总价款：人民币 元

大写：人民币 元整

二、质量要求及对质量负责条件和期限：见附件。

三、供方所提供的服务必须具有合法手续及相关文件。如涉及知识产权则必须是自己拥有或合法使用的。

四、服务时间、地点、方式：见附件。

五、供方应随服务向需方交付的相关资料。如果所提交文件是外文的，供方有义务为需方提供中文或译成中文文件。

六、验收工作由需方负责对合同进行验收。

七、货款支付方式：见附件。

供方开户银行（汉字全称）： ，

行号（数字代码）： ，

帐 号： 。

八、有关涉及本合同供方向天津市政府采购中心所提交的投标文件及有关澄清资料和服务承诺均视为本合同不可分割的部分，对供方具有约束力。

九、本合同一式 份，需方留存 份，供方留存 份，均具同等效力，签字盖章后生效。

|  |  |
| --- | --- |
| 供方（公章）： | 需方（公章）： |
| 地址： | 地址： |
| 法定代表人： | 法定代表人： |
| 委托代理人： | 委托代理人： |
| 电话： | 电话： |

时间：20 年 月 日

**合同特殊条款**

合同特殊条款是合同一般条款的补充和修改。如果两者之间有抵触，应以特殊条款为准。

合同特殊条款由供方和需方根据项目的具体情况协商拟订。

第五部分 投标文件格式

**投标文件封面格式**



投 标 文 件

**（加盖电子签章）**

**项目编号：**

**项目名称：**

**所投包号：**

**投标单位名称：**

**投标代表人姓名：**

**投标日期： 年 月 日**

**投标文件总目录**

**（投标人自行编制）**

**评分因素及评标标准页码检索**

**（需投标人按招标文件“评分因素及评标标准”中每个评分项逐项列明页码）**

**附件1**

**投标书**

致：天津市政府采购中心

根据贵方为天津市 项目（项目编号： ）的投标邀请，签字代表 （姓名/职务）经正式授权并代表我公司 （投标单位名称、地址）提交网上应答及上传加盖电子签章的投标文件。

据此函，签字代表宣布同意如下：

1. 所附投标报价表中规定的应提供和交付的服务投标总价为：

第一包，￥ 元（人民币），大写 。

第二包，￥ 元（人民币），大写 。

……

2. 我公司将按招标文件的规定履行合同责任和义务。

3. 我公司已详细审查全部招标文件，包括更正公告以及全部参考资料和所有附件。我们认为全部招标文件（包括更正公告以及全部参考资料和所有附件）公平公正，无倾向性和排他性，我们完全理解并同意放弃对这方面有不明及误解的权利。

4. 我公司的投标有效期为开标之日起60天。

5. 我公司同意按照招标方要求提供的与投标有关的一切数据或资料，并声明投标文件及所提供的一切资料均真实有效。由于我公司提供资料不实而造成的责任和后果由我公司自行承担。

6. 我公司保证所投产品来自合法的供货渠道，若中标，则有义务向采购人提供其需要的有效书面证明材料。如果提供非法渠道的商品，视为欺诈，并承担相关责任。

7. 我公司已熟知贵中心关于本项目电子招投标的要求和规定，我公司完全响应本次招投标通过网上应答进行的方式，我方承诺投标数据以应答截止时间贵中心网络服务器数据库的记录为准，一切因网络通信或我方操作失误造成的应答数据错误或缺失均与贵中心无关，我方愿承担因此出现的任何风险和责任。

8. 我公司承诺完全符合《政府采购法》、《政府采购法实施条例》等法律法规规定，并随时接受采购人、采购代理机构的检查验证。在整个招标过程中，我公司若有违规行为，我公司完全接受贵中心依照相关法律法规和招标文件的规定给予处罚。

9. 我公司承诺未列入“信用中国”网站（www.creditchina.gov.cn）失信被执行人、重大税收违法案件当事人名单，也未列入中国政府采购网（www.ccgp.gov.cn）政府采购严重违法失信行为记录名单，符合《中华人民共和国政府采购法》第二十二条规定的各项条件，具备履行合同所必需的设备和专业技术能力，投标截止日前3年在经营活动中没有重大违法记录。

10. 我公司若中标，本承诺将成为合同不可分割的一部分，与合同具有同等的法律效力。

11. 如违反上述承诺，我公司投标无效且接受相关部门依法作出的处罚，并承担通过相关媒体予以公布的任何风险和责任。

12. 我公司开票信息如下，**此信息与我公司在税务局注册的信息一致**：

纳税人识别号：

地址、电话：

开户行及账号：

开具发票类型：□增值税专用发票 □增值税普通发票

13. 我公司选择招标代理服务费发票领取方式（请自行选择以下任一方式并在相应□里划“√”）：

**□上门自取**

**□到付邮寄**

邮寄地址、邮编：

邮寄联系人、手机号码：

投标人名称：

日期： 年 月 日

**附件2**

**开标一览表**

项目名称：

项目编号：

包号：

单位：元

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 包号 | 服务名称 | 数量 | 投标总价 | 备注 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

投标人名称：

日期： 年 月 日

**附件3**

**开标分项一览表**

项目名称：

项目编号：

包 号：

单位：元

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **项号** | **服务名称** | **总价** | **数量** | **备注** |
| 1 |  |  | 1项 |  |
| 其中 | | | | |
| **分项名称** | | **价格** | **数量** | **备注** |
|  | |  |  |  |
|  | |  |  |  |
|  | |  |  |  |
|  | |  |  |  |
| 管理费、税费 | |  |  |  |
| …… | |  |  |  |
|  | |  |  |  |

注：1. 本表第一行填写本项目投标总价，须与附件2中投标总价保持一致。

2. 下面应填写分项价格及分项名称（分项名称可根据实际情况增减、修改），分项价格汇总应等于总价。

投标人名称：

日期： 年 月 日

**附件4**

**商务要求点对点应答表**

项目名称：

项目编号：

包号：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 招标要求 | 投标应答 | 偏离说明 | 备注 |
| （一）报价要求 | | | | |
|  |  |  |  |  |
| （二）服务要求 | | | | |
|  |  |  |  |  |
| （三）时间、地点要求 | | | | |
|  |  |  |  |  |
| （四）付款方式 | | | | |
|  |  |  |  |  |
| （五）投标保证金和履约保证金 | | | | |
|  |  |  |  |  |

注：

1. 不如实填写偏离情况的投标文件将视为虚假材料。

2. 招标要求指招标文件中规定的具体要求，投标应答指投标文件的具体内容。

4. 偏离说明指招标要求与投标应答之间的不同之处。

投标人名称：

日期： 年 月 日

**附件5**

**技术要求点对点应答表**

项目名称：

项目编号：

包号：

| 序号 | 招标要求 | 投标应答 | 偏离说明 | 备注 |
| --- | --- | --- | --- | --- |
| 1 | （一）投标人须承诺所提供的服务、人员及设备符合相关国家强制性规定。 |  |  |  |
| 2. 项目需求书要求 | | | | |
| 序号 | 招标要求 | 投标应答 | 偏离说明 | 备注 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

注：

1. 不如实填写偏离情况的投标文件将视为虚假材料。

2. 招标要求指招标文件中规定的具体要求，投标应答指投标文件的具体内容。

3. 偏离说明指招标要求与投标应答之间的不同之处。

4. 投标人在上表“项目需求书要求”的投标应答中必须列出具体数值或内容。如投标人未应答或只注明“符合”、“满足”等类似无具体内容的表述，将被视为不符合招标文件要求。投标人自行承担由此造成的一切后果。

投标人名称：

日期： 年 月 日

**附件6**

**主要相关项目业绩一览表**

项目名称：

项目编号：

包号：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 用户单位名称 | 项目内容 | 实施地点 | 用户联系人及联系方式 | 项目起止时间 | 合同金额 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

备注：若招标文件第二部分评分因素及评标标准中要求提供业绩的，投标人所列业绩应按其要求将证明材料按顺序附后。

投标人名称：

日期： 年 月 日

**附件7-1**

**专业人员组成及任务分配**

|  |  |  |  |
| --- | --- | --- | --- |
| **姓名** | **职位** | **学历** | **任务** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**注：列出所有参加本项目专业人员名单及在本项目中所承担职位和工作。**

**附件7-2**

**专业人员简历格式**

本项目岗位：

人员姓名：

学历、专业：

所获证书：

出生日期：

在此公司工作年限：

**关键资格条件：**

***（概述此人员与本任务最相关的经验，描述其在以前的有关任务中承担的责任，给出日期和地点。）***

**教育：**

*（概述此人员的大学和其他专业化教育和培训情况，给出学校的名称、入学日期、所获学位。）*

**所获证书：**

*（提供此人与本项目相关的证书扫描件）*

**工作简历：**

（从现任职位开始，倒叙列出自毕业后所任所有职务、日期、受雇单位名称、职位头衔、任务地点。近十年的经验应给出从事活动的类型和适当的用户信息。）

**注：关键岗位人员均需填写此表。**

**附件8**

**投标代表人授权书**

致：天津市政府采购中心

我单位授权委托本月/上月（本月尚未缴纳社保的，则填写上月）由我单位缴纳社会保险的在职职工\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_（姓名）（身份证号码：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_、联系电话：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_）作为投标代表人以我方的名义参加贵中心组织的\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_项目（项目编号：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_）的投标活动，并代表我方全权办理针对上述项目的投标、开标、投标文件澄清、签约等一切具体事务和签署相关文件。

我方对投标代表人的签名事项负全部责任。

本授权书至投标有效期结束前始终有效。

投标代表人无转委托权，特此委托。

年 月 日

|  |  |
| --- | --- |
| 投标代表人身份证正面 | 投标代表人身份证背面 |

**附件9-1**

**中小企业声明函（服务）**

本公司（联合体）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（联合体）参加 **（请填写项目名称）**采购活动，服务全部由符合政策要求的中小企业承接。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

1. （**请填写标的名称**），属于 软件和信息技术服务业 **（请填写本项目采购文件中明确的所属行业）**行业；承接企业为 （**请填写承接该标的企业名称**），从业人员 人，营业收入为 万元，资产总额为 万元，属于 （**请根据中小企业划分标准填写中型企业/小型企业/微型企业**）；

2. （**请填写标的名称**），属于 **（请填写本项目采购文件中明确的所属行业）**行业；承接企业为 （**请填写承接该标的企业名称**），从业人员 人，营业收入为 万元，资产总额为 万元，属于 （**请根据中小企业划分标准填写中型企业/小型企业/微型企业**）；

……

以上企业，不属于大型企业的分支机构，不存在控股股东为大型企业的情形，也不存在与大型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。

投标人名称：

日期：

**注：**

**1.标的名称须按照采购文件中明确的标的名称进行填写；所属行业须按照采购文件中明确的所属行业进行填写，否则不享受中小企业扶持政策。**

**2.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。除新成立企业外，上表填写不全的，不享受中小企业扶持政策。**

**3.中标（成交）供应商享受中小企业扶持政策的，将随中标（成交）结果同时公告其《中小企业声明函》，接受社会监督。**

**附件9-2**

**若不是残疾人福利性单位，投标文件中可不提供此声明函**

**残疾人福利性单位声明函**

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\_\_\_\_\_\_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。

投标人名称：

日 期：

注：

**中标供应商为残疾人福利性单位的，将随中标结果同时公告其《残疾人福利性单位声明函》，接受社会监督。**

**若不是残疾人福利性单位，投标文件中可不提供此声明函。**

**附件10**

**政府采购政策情况表**

项目名称：

项目编号：

包号：

单位：元

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 节能产品（非强制节能产品） | 产品名称 | 品牌型号 | | 制造商 | 节能认证证书编号 | 金额 |
|  |  | |  |  |  |
|  |  | |  |  |  |
| 节能产品（不包括强制节能产品）金额合计 | | | | |  |
| 比重（节能产品金额/投标所投包总价） | | | | | % |
| 节能产品证明材料见投标文件第 至 页。 | | | | | |
| 环境标志产品 | 产品名称 | 品牌型号 | 制造商 | | 环境标志认证证书编号 | 金额 |
|  |  |  | |  |  |
|  |  |  | |  |  |
| 环境标志产品金额合计 | | | | |  |
| 比重（环境标志产品金额/所投包投标总价） | | | | | % |
| 环境标志产品证明材料见投标文件第 至 页。 | | | | | |

填报要求：

1. 请投标人正确填写本表，所填内容将作为评分的依据。其内容或数据应与对应的证明资料相符，如果填写不完整或有误，不再享受上述政策优惠。

2. 节能产品是指财政部和国家发展改革委员会公布现行的《节能产品政府采购清单》中的产品；环境标志产品是指财政部、生态环境部发布现行的《环境标志产品政府采购清单》中的产品。请提供《清单》中相关内容页（并对相关内容作圈记）。

投标人名称：

日期：

**附件11：招标文件第一部分供应商资格要求的证件**

**附件12**

**书面声明**

参加政府采购活动前3年我单位在经营活动中没有重大违法记录。

我单位具备良好的商业信誉和健全的财务会计制度，依法缴纳税收和社会保障资金。

投标人名称：

日期：

**证明材料**

我单位具备履行本项目合同所必需的设备和专业技术能力。

投标人名称：

日期：

**附件13：招标文件评分因素及评标标准中要求的证明材料扫描件、方案等**

**附件14：投标人认为需要提供的其他资料**