网络安全服务项目

（项目编号：11000026210200163755-XM001）

第 2 标包：信息系统测评（标包名称）

投标文件

（第一册：资格分册）

投标人名称：中科信息安全共性技术国家工程研究中心有限公司（盖章）

法定代表人或其委托代理人：_____（签字或签章）

2026 年 3 月 24 日

目录

1.1. 资格分册目录

序号	文件名称	页码
1	投标人资格证明文件	5-48
2	投标标的符合性证明文件	49
3	其他文件	50-52

注：1. 该目录为方便资格审查人员查找相关证明文件及评审条件，应尽可能的详细、清晰，投标人可根据自身情况补充完善。

2. 投标文件的装订顺序应按此表顺序依次装订，并连续编排页码（电子文件可以采用页码机加盖页码）。

1.2. 资格审查索引

审查因素			投标响应情况	投标文件页码范围	说明或备注
招标文件获取			/	/	/
投标人名称			满足	6	/
符合《政府采购法》第二十二条的规定	具有独立承担民事责任的能力		满足	5	/
	具有良好的商业信誉和健全的财务会计制度		满足	7	/
	具有履行合同所必需的设备和专业技术能力		满足	40	/
	有依法缴纳税收和社会保障资金的良好记录	依法缴纳税收	满足	38	/
		依法缴纳社会保障资金	满足	39	/
	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		满足	41	/
	法律、行政法规规定的其他条件		满足	41	/
落实政府采购政策需满足的资格要求			满足	42	/
特定资格要求			无	/	/
联合体投标人			无	/	/
投标人不得存在的情形			无	/	/
投标标的的符合性			无	/	/
法定代表人身份证明			满足	50	/
法定代表人授权委托书			满足	51	/
投标保证金金额			满足	52	/
投标保证金形式			满足	52	/

注：本索引由投标人根据招标文件第三章“资格审查与评标办法”第 2.1 款规定的资格审查标准和投标人实际响应情况逐项填写。

1. 投标人资格证明文件

1.1. 独立承担民事责任能力的证明材料

统一社会信用代码

91110108791603851A

营业执照

(副 本)(3-1)

扫描市场主体身份码了解更多登记、备案、许可、监管信息，体验更多应用服务。

名　　称　中科信息安全共性技术国家工程研究中心有限公司

类　　型　其他有限责任公司

法定代表人　潘毅

经营范围　信息安全理论与标准研究、体系论证、大型信息安全系统设计、高性能信息安全产品开发、信息安全共性技术研究与应用、信息安全评测与管理；信息安全咨询；新技术引进与市场推广、技术转让与成果孵化；计算机软件生产与加工；计算机技术培训；会议服务；承办展览展示活动。（市场主体依法自主选择经营项目，开展经营活动；依法须经批准的项目，经相关部门批准后依批准的内容开展经营活动；不得从事国家和本市产业政策禁止和限制类项目的经营活动。）

注册资本　5000万元

成立日期　2006年08月09日

住　　所　北京市海淀区中关村大街19号16层B1601、B1602、B1603、B1605

登记机关

2023 年 09 月 26 日

国家企业信用信息公示系统网址：http://www.gsxt.gov.cn

市场主体应当于每年1月1日至6月30日通过国家企业信用信息公示系统报送公示年度报告。

国家市场监督管理总局监制

1.2. 投标人资格声明书

投标人资格声明书

致：国讯招标集团有限公司（*采购人或采购代理机构*）

在参与本次项目中，我方承诺：

序号	承诺项	具体情形（请进行勾选）
（一）	是否具有良好的商业信誉和健全的财务会计制度	☑具有 ☐不具有
（二）	是否有依法缴纳税收和社会保障资金的良好记录	☑具有 ☐不具有
（三）	是否具有履行合同所必需的设备和专业技术能力	☑具有 ☐不具有
（四）	参加政府采购活动前三年内，在经营活动中是否有重大违法记录 **注：**重大违法记录指因违法经营受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚，不包括因违法经营被禁止在一定期限内参加政府采购活动，但期限已经届满的情形。 其中：“较大数额罚款”以《关于<中华人民政府采购法实施条例>第十九条第一款“较大数额罚款”具体适用问题的意见》（财库〔2022〕3号）规定为准，具体为：200万元以上的罚款，法律、行政法规以及国务院有关部门明确相关领域“较大数额罚款”标准高于200万元的，从其规定。	☑无重大违法记录 ☐有重大违法记录 ☐因违法经营受到刑事处罚 ☐因违法经营受到责令停产停业的行政处罚 ☐因违法经营受到吊销许可证或执照的行政处罚 ☐因违法经营受到较大数额罚款的行政处罚
（五）	是否属于政府采购法律、行政法规规定的公益一类事业单位、或使用事业编制且由财政拨款保障的群团组织 **注：**如为政府购买服务项目应当填写，否则可不填写	☐属于 ☑不属于
（六）	是否存在为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务后，再参加该采购项目的其他采购活动的情形	☐存在 ☑不存在
（七）	与我单位存在“单位负责人为同一人或者存在直接控股、管理关系”的其他法人单位信息如下（如有，不论其是否参加同一合同项下的政府采购活动均应当填写）	

序号	单位名称	相互关系
	无	
……		

上述声明真实有效，否则我方负全部责任。

投标人名称（加盖公章）：中科信息安全共性技术国家工程研究中心有限公司

日期：2026年3月24日

1.2.1. 财务状况证明材料

1.2.1.1. 2024年度财务审计报告

中科信息安全共性技术国家工程研究中心有限公司

2024年度财务报表

审计报告书

中兴华会计师事务所(特殊普通合伙)

ZHONGXINHAU CERTIFIED PUBLIC ACCOUNTANTS LLP

地址：北京市丰台区丽泽路20号丽泽SOHO B座20层 邮编：100073

电话：(010) 51423818 传真：(010) 51423816

目　　录

中兴华会计师事务所（特殊普通合伙）
ZHONGXINGHUA CERTIFIED PUBLIC ACCOUNTANTS LLP
地址（location）：北京市丰台区丽泽路 20 号丽泽 SOHO B 座 20 层
20/F, Tower B, Lize SOHO, 20 Lize Road, Fengtai District, Beijing PR China
电话（tel）：010-51423818 传真（fax）：010-51423816

审 计 报 告

中兴华审字（2025）第 010215 号

中科信息安全共性技术国家工程研究中心有限公司全体股东：

一、审计意见

我们审计了中科信息安全共性技术国家工程研究中心有限公司（以下简称“中科信息”）财务报表，包括 2024 年 12 月 31 日的资产负债表，2024 年度的利润表、现金流量表、所有者权益变动表以及相关财务报表附注。

我们认为，后附的财务报表在所有重大方面按照企业会计准则的规定编制，公允反映了中科信息 2024 年 12 月 31 日的财务状况以及 2024 年度的经营成果和现金流量。

二、形成审计意见的基础

我们按照中国注册会计师审计准则的规定执行了审计工作。审计报告的“注册会计师对财务报表审计的责任”部分进一步阐述了我们在这些准则下的责任。按照中国注册会计师职业道德守则，我们独立于中科信息，并履行了职业道德方面的其他责任。我们相信，我们获取的审计证据是充分、适当的，为发表审计意见提供了基础。

三、管理层和治理层对财务报表的责任

管理层负责按照企业会计准则的规定编制财务报表，使其实现公允反映，并设计、执行和维护必要的内部控制，以使财务报表不存在由于舞弊或错误导致的重大错报。

在编制财务报表时，管理层负责评估中科信息的持续经营能力，披露与持续经营相关的事项（如适用），并运用持续经营假设，除非管理层计划清算中科信息、终止运营或别无其他现实的选择。

治理层负责监督中科信息的财务报告过程。

四、注册会计师对财务报表审计的责任

我们的目标是对财务报表整体是否不存在由于舞弊或错误导致的重大错报获取合理保证，并出具包含审计意见的审计报告。合理保证是高水平的保证，但并不能保证按照审计准则执行的审计在某一重大错报存在时总能发现。错报可能由舞弊或错误导致，如果合理预期错报单独或汇总起来可能影响财务报表使用者依据财务报表作出的经济决策，则通常认为错报是重大的。

在按照审计准则执行审计的过程中，我们运用了职业判断，保持了职业怀疑。同时，我们也执行以下工作：

（1）识别和评估由于舞弊或错误导致的财务报表重大错报风险，设计和实施审计程序以应对这些风险，并获取充分、适当的审计证据，作为发表审计意见的基础。由于舞弊可能涉及串通、伪造、故意遗漏、虚假陈述或凌驾于内部控制之上，未能发现由于舞弊导致的重大错报的风险高于未能发现由于错误导致的重大错报的风险。

（2）了解与审计相关的内部控制，以设计恰当的审计程序，但目的并非对内部控制的有效性发表意见。

（3）评价管理层选用会计政策的恰当性和作出会计估计及相关披露的合理性。

（4）对管理层使用持续经营假设的恰当性得出结论。同时，根据获取的审计证据，就可能导致对中科信息持续经营能力产生重大疑虑的事项或情况是否存在重大不确定性得出结论。如果我们得出结论认为存在重大不确定性，审计准则要求我们在审计报告中提请报表使用者注意财务报表中的相关披露；如果披露不充分，我们应当发表非无保留意见。我们的结论基于截至审计报告日可获得的信息。然而，未来的事项或情况可能导致中科信息不能持续经营。

（5）评价财务报表的总体列报、结构和内容，并评价财务报表是否公允反映相关交易和事项。

我们与治理层就计划的审计范围、时间安排和重大审计发现等事项进行沟通，包括沟通我们在审计中识别出的值得关注的内部控制缺陷。

（此页无正文，为《审计报告》（中兴华审字（2025）第 010215 号）之签字盖章页）

中兴华会计师事务所（特殊普通合伙）　　中国注册会计师：

中国·北京　　中国注册会计师：

2025 年 02 月 09 日

资产负债表

2024年12月31日

编制单位：中科信息安全共性技术国家工程研究中心有限公司　　金额单位：人民币元

项　目	注释	年末余额	上年年末余额
流动资产：			
货币资金	七、1	14,899,671.10	24,019,627.58
交易性金融资产			
以公允价值计量且其变动计入当期损益的金融资产			
衍生金融资产			
应收票据	七、2		1,510,000.00
应收账款	七、3	14,811,870.00	14,359,533.62
应收款项融资	七、4	320,000.00	440,000.00
预付款项			
其他应收款	七、5	12,958,285.06	2,801,391.36
存货	七、6	116,524.74	116,524.74
合同资产			
持有待售资产			
一年内到期的非流动资产			
其他流动资产			
流动资产合计		**43,106,350.90**	**43,247,077.30**
非流动资产：			
债权投资			
可供出售金融资产			
其他债权投资			
持有至到期投资			
长期应收款			
长期股权投资	七、7	400,000.00	400,000.00
其他权益工具投资			
其他非流动金融资产			
投资性房地产			
固定资产	七、8	3,650,025.74	3,876,435.39
在建工程			
生产性生物资产			
油气资产			
使用权资产			
无形资产	七、9		2,434,266.01
开发支出	七、10	46,408,322.29	41,988,385.42
商誉			
长期待摊费用			
递延所得税资产			
其他非流动资产			
非流动资产合计		**50,458,348.03**	**48,699,086.82**
资产总计		**93,564,698.93**	**91,946,164.12**

（后附财务报表附注是本财务报表的组成部分）

法定代表人：潘之印　　主管会计工作负责人：[illegible]　　会计机构负责人：[illegible]

（承上页）

资产负债表（续）

2024年12月31日

编制单位：中科信息安全共性技术国家工程研究中心有限公司　　金额单位：人民币元

项　目	注释	年末余额	上年年末余额
流动负债：			
短期借款			
交易性金融负债			
以公允价值计量且其变动计入当期损益的金融负债			
衍生金融负债			
应付票据			
应付账款	七、11	209,683.00	209,683.00
预收款项			
合同负债	七、12	1,059,859.26	978,350.00
应付职工薪酬	七、13	857,311.35	702,101.08
应交税费	七、14	1,481,716.93	1,107,909.63
其他应付款	七、15	858,900.50	927,645.05
持有待售负债			
一年内到期的非流动负债			
其他流动负债			
流动负债合计		**4,467,471.04**	**3,925,688.76**
非流动负债：			
长期借款			
应付债券			
其中：优先股			
永续债			
租赁负债			
长期应付款			
长期应付职工薪酬			
预计负债			
递延收益			
递延所得税负债			
其他非流动负债			
非流动负债合计			
负债合计		**4,467,471.04**	**3,925,688.76**
所有者权益：			
实收资本	七、16	50,000,000.00	50,000,000.00
其他权益工具			
其中：优先股			
永续债			
资本公积	七、17	27,237,353.57	27,237,353.57
减：库存股			
其他综合收益			
专项储备			
盈余公积	七、18	1,401,546.06	1,293,870.81
未分配利润	七、19	10,458,328.26	9,489,250.98
所有者权益合计		**89,097,227.89**	**88,020,475.36**
负债和所有者权益总计		**93,564,698.93**	**91,946,164.12**

（后附财务报表附注是本财务报表的组成部分）

法定代表人：潘毅之印　　主管会计工作负责人：　　会计机构负责人：

利润表

2024年12月31日

编制单位：中科信息安全共性技术国家工程研究中心有限公司　　金额单位：人民币元

项　目	注释	本年金额	上年金额
一、营业收入	七、20	84,177,823.97	68,764,469.89
减：营业成本	七、20	25,826,479.09	17,892,558.92
税金及附加	七、21	584,052.36	489,885.74
销售费用	七、22	14,481,003.39	12,553,614.73
管理费用	七、23	14,894,421.25	12,924,110.14
研发费用	七、24	26,623,606.11	25,107,528.84
财务费用	七、25	-3,791.45	-21,658.59
其中：利息费用			
利息收入	七、25	11,898.05	32,568.44
加：其他收益	七、26	119,003.48	814,518.92
投资收益（损失以“－”号填列）			
其中：对联营企业和合营企业的投资收益			
以摊余成本计量的金融资产终止确认收益			
净敞口套期收益（损失以“－”号填列）			
公允价值变动收益（损失以“－”号填列）			
信用减值损失（损失以“－”号填列）	七、27	-739,300.00	-28,500.00
资产减值损失（损失以“－”号填列）			
资产处置收益（损失以“－”号填列）			
二、营业利润（亏损以“－”号填列）		1,151,756.70	604,449.03
加：营业外收入	七、28	137,702.56	57,574.52
减：营业外支出	七、29	27,624.00	2,891.66
三、利润总额（亏损总额以“－”号填列）		1,261,835.26	659,131.89
减：所得税费用	七、30	185,082.73	98,869.78
四、净利润（净亏损以"－"号填列）		1,076,752.53	560,262.11
（一）持续经营净利润（净亏损以“-”号填列）			
（二）终止经营净利润（净亏损以“-”号填列）			
五、其他综合收益的税后净额			
（一）不能重分类进损益的其他综合收益			
1. 重新计量设定受益计划变动额			
2. 权益法下不能转损益的其他综合收益			
3. 其他权益工具投资公允价值变动			
4. 企业自身信用风险公允价值变动			
5. 其他			
（二）将重分类进损益的其他综合收益			
1. 权益法下可转损益的其他综合收益			
2. 其他债权投资公允价值变动			
3. 可供出售金融资产投资公允价值变动			
4. 金融资产重分类计入其他综合收益的金额			
5. 持有至到期投资重分类为可供出售金融资产损益			
6. 其他债权投资信用减值准备			
7. 现金流量套期储备			
8. 外币财务报表折算差额			
9. 其他			
六、综合收益总额		1,076,752.53	560,262.11

（后附财务报表附注是本财务报表的组成部分）　6

法定代表人：潘之毅印　　主管会计工作负责人：夏坤　　会计机构负责人：

现金流量表

2024年12月31日

编制单位：中科信息安全共性技术国家工程研究中心有限公司　　金额单位：人民币元

项　目	注释	本年金额	上年金额
一、经营活动产生的现金流量：			
销售商品、提供劳务收到的现金		92,540,740.82	72,994,720.63
收到的税费返还			26,757.46
收到其他与经营活动有关的现金		1,668,239.18	3,168,115.02
经营活动现金流入小计		**94,208,980.00**	**76,189,593.11**
购买商品、接受劳务支付的现金		26,272,055.34	18,464,103.04
支付给职工以及为职工支付的现金		48,441,868.15	39,171,397.35
支付的各项税费		3,973,376.72	3,891,372.67
支付其他与经营活动有关的现金		23,980,431.95	12,243,702.89
经营活动现金流出小计		**102,667,732.16**	**73,770,575.95**
经营活动产生的现金流量净额		**-8,458,752.16**	**2,419,017.16**
二、投资活动产生的现金流量：			
收回投资收到的现金			
取得投资收益收到的现金			
处置固定资产、无形资产和其他长期资产收回的现金净额		27,000.00	
收到其他与投资活动有关的现金			
投资活动现金流入小计		**27,000.00**	
购建固定资产、无形资产和其他长期资产支付的现金		801,514.32	380,559.77
投资支付的现金			
支付其他与投资活动有关的现金			
投资活动现金流出小计		**801,514.32**	**380,559.77**
投资活动产生的现金流量净额		**-774,514.32**	**-380,559.77**
三、筹资活动产生的现金流量：			
吸收投资收到的现金			
取得借款收到的现金		300,000.00	
收到其他与筹资活动有关的现金			
筹资活动现金流入小计		**300,000.00**	
偿还债务支付的现金		300,000.00	
分配股利、利润或偿付利息支付的现金			
支付其他与筹资活动有关的现金			
筹资活动现金流出小计		**300,000.00**	
筹资活动产生的现金流量净额			
四、汇率变动对现金及现金等价物的影响			
五、现金及现金等价物净增加额		-9,233,266.48	2,038,457.39
加：期初现金及现金等价物余额		23,892,627.58	21,854,170.19
六、期末现金及现金等价物余额		**14,659,361.10**	**23,892,627.58**

（后附财务报表附注是本财务报表的组成部分）

法定代表人：潘之毅印　　主管会计工作负责人：[illegible]　　会计机构负责人：[illegible]

所有者权益变动表

2024年12月31日

编制单位：中西信息安全技术国家工程研究中心有限公司　　金额单位：人民币元

项目	本年金额										
	实收资本	其他权益工具			资本公积	减：库存股	其他综合收益	专项储备	盈余公积	未分配利润	所有者权益合计
		优先股	永续债	其他							
一、上年年末余额	50,000,000.00				27,237,353.57				1,293,870.81	9,489,250.98	88,020,475.36
加：会计政策变更											
前期差错更正											
其他											
二、本年年初余额	50,000,000.00				27,237,353.57				1,293,870.81	9,489,250.98	88,020,475.36
三、本期增减变动金额（减少以"-"号填列）									107,675.25	969,077.28	1,076,752.53
（一）综合收益总额										1,076,752.53	1,076,752.53
（二）所有者投入和减少资本											
1、所有者投入资本											
2、其他权益工具持有者投入资本											
3、股份支付计入所有者权益的金额											
4、其他											
（三）利润分配									107,675.25	-107,675.25	
1、提取盈余公积									107,675.25	-107,675.25	
2、提取一般风险准备											
3、对所有者（或合伙人）的分配											
4、其他											
（四）所有者权益内部结转											
1、资本公积转增资本											
2、盈余公积转增资本											
3、盈余公积弥补亏损											
4、设定受益计划变动额结转留存收益											
5、其他综合收益结转留存收益											
6、其他											
（五）专项储备											
1、本期提取											
2、本期使用											
（六）其他											
四、本年年末余额	50,000,000.00				27,237,353.57				1,401,546.06	10,458,328.26	89,097,227.89

（后附财务报表附注是本财务报表的组成部分）

法定代表人：　　主管会计工作负责人：　　会计机构负责人：

所有者权益变动表（续）

2024年12月31日

编制单位：中科信息安全共性技术国家工程研究中心有限公司　　金额单位：人民币元

项目	上年金额										
	实收资本	其他权益工具			资本公积	减：库存股	其他综合收益	专项储备	盈余公积	未分配利润	所有者权益合计
		优先股	永续债	其他							
一、上年年末余额	50,000,000.00				27,237,353.57				1,237,844.60	8,985,015.08	**87,460,213.25**
加：会计政策变更											
前期差错更正											
其他											
二、本年年初余额	50,000,000.00				27,237,353.57				1,237,844.60	8,985,015.08	**87,460,213.25**
三、本期增减变动金额（减少以“-”号填列）									56,026.21	504,235.90	**560,262.11**
（一）综合收益总额										560,262.11	**560,262.11**
（二）所有者投入和减少资本											
1、所有者投入资本											
2、其他权益工具持有者投入资本											
3、股份支付计入所有者权益的金额											
4、其他											
（三）利润分配									56,026.21	-56,026.21	
1、提取盈余公积									56,026.21	-56,026.21	
2、提取一般风险准备											
3、对所有者（或合伙人）的分配											
4、其他											
（四）所有者权益内部结转											
1、资本公积转增资本（或股本）											
2、盈余公积转增资本（或股本）											
3、盈余公积弥补亏损											
4、设定受益计划变动额结转留存收益											
5、其他综合收益结转留存收益											
6、其他											
（五）专项储备											
1、本期提取											
2、本期使用											
（六）其他											
四、本年年末余额	50,000,000.00				27,237,353.57				1,293,870.81	9,489,250.98	**88,020,475.36**

（后附财务报表附注是本财务报表的组成部分）

法定代表人：　　主管会计工作负责人：　　会计机构负责人：

中科信息安全共性技术国家工程研究中心有限公司

财务报表附注(供参考以客户实际情况为准)

截止 2024 年 12 月 31 日

（除特别说明外，金额以人民币元表述）

一、 公司基本情况

（一）企业注册地：北京市海淀区中关村大街 19 号 16 层 B1601、B1602、B1603、B1605；

（二）企业的业务性质和主要经营活动：本公司经批准的经营范围：信息安全理论与标准研究、体系论证、大型信息安全系统设计、高性能信息安全产品开发、信息安全基础设施研究与应用、信息安全评测与管理；信息安全咨询与服务、技术引进与市场推广、技术转让与成果孵化；计算机软件生产与加工；计算机技术培训；会议服务；承办展览展示活动。公司主要产品是信息安全咨询与服务、计算机软件生产与加工等；

（三）财务报告批准报出日：2025 年 2 月 9 日；

（四）中科信息安全共性技术国家工程研究中心有限公司（以下简称“本公司”）系于 2006 年 8 月 9 日在北京市工商行政管理局办理了工商登记，营业执照号为：110000009838727，且于 2016 年 12 月 29 日变更为统一社会信用代码 91110108791603851A。注册资本为人民币 5000 万元。公司法定代表人为潘毅。

二、 财务报表的编制基础

本公司财务报表以持续经营假设为基础，根据实际发生的交易和事项，按照财政部发布的《企业会计准则——基本准则》（财政部令第 33 号发布、财政部令第 76 号修订）、于 2006 年 2 月 15 日及其后颁布和修订的 41 项具体会计准则、企业会计准则应用指南、企业会计准则解释及其他相关规定（以下合称“企业会计准则”）编制。

三、 遵循企业会计准则的声明

本财务报表符合企业会计准则的要求，真实、完整地反映了本公司 2024 年 12 月 31 日的财务状况及 2024 年度的经营成果和现金流量等有关信息。

四、 重要会计政策、会计估计的说明

1、会计期间

本公司会计年度采用公历年度，即每年自 1 月 1 日起至 12 月 31 日止。

2、记账本位币

本公司以人民币为记账本位币。本公司编制本财务报表时所采用的货币为人民币。

3、记账基础和计价原则

根据企业会计准则的相关规定，本公司会计核算以权责发生制为基础。除某些金融工具外，本财务报表均以历史成本为计量基础，资产如果发生减值，则按照相关规定计提相应的减值准备。

4、现金及现金等价物的确定标准

本公司现金及现金等价物包括库存现金、可以随时用于支付的存款以及本公司持有的期限短（一般为从购买日起，三个月内到期）、流动性强、易于转换为已知金额的现金、价值变动风险很小的投资。

5、应收款项

应收款项包括应收账款、其他应收款等。

（1）减值准备的确认方法

本公司以预期信用损失为基础，对上述各项目按照其适用的预期信用损失计量方法（一般方法或简化方法）计提减值准备并确认信用减值损失。

信用损失，是指本公司按照原实际利率折现的、根据合同应收的所有合同现金流量与预期收取的所有现金流量之间的差额，即全部现金短缺的现值。其中，对于购买或源生的已发生信用减值的金融资产，本公司按照该金融资产经信用调整的实际利率折现。

预期信用损失计量的一般方法是指，本公司在每个资产负债表日评估金融资产的信用风险自初始确认后是否已经显著增加，如果信用风险自初始确认后已显著增加，本公司按照相当于整个存续期内预期信用损失的金额计量损失准备；如果信用风险自初始确认后未显著增加，本公司按照相当于未来 12 个月内预期信用损失的金额计量损失准备。本公司在评估预期信用损失时，考虑所有合理且有依据的信息，包括前瞻性信息。

对于在资产负债表日具有较低信用风险的金融工具，本公司假设其信用风险自初始确认后并未显著增加，选择按照未来 12 个月内的预期信用损失计量损失准备。

（2）信用风险自初始确认后是否显著增加的判断标准

如果某项金融资产在资产负债表日确定的预计存续期内的违约概率显著高于在初始确认时确定

的预计存续期内的违约概率，则表明该项金融资产的信用风险显著增加。除特殊情况外，本公司采用未来 12 个月内发生的违约风险的变化作为整个存续期内发生违约风险变化的合理估计，来确定自初始确认后信用风险是否显著增加。

（3）已发生信用减值的金融资产的判断标准

当对金融资产预期未来现金流量具有不利影响的一项或多项事件发生时，该金融资产成为已发生信用减值的金融资产。金融资产已发生信用减值的证据包括下列可观察信息：

1）发行方或债务人发生重大财务困难；

2）债务人违反合同，如偿付利息或本金违约或逾期等；

3）债权人出于与债务人财务困难有关的经济或合同考虑，给予债务人在任何其他情况下都不会做出的让步；

4）债务人很可能破产或进行其他财务重组；

5）发行方或债务人财务困难导致该金融资产的活跃市场消失；

6）以大幅折扣购买或源生一项金融资产，该折扣反映了发生信用损失的事实。

金融资产发生信用减值，有可能是多个事件的共同作用所致，未必是可单独识别的事件所致。

（4）以组合为基础评估预期信用风险的组合方法

本公司对信用风险显著不同的金融资产单项评价信用风险，如：应收关联方款项；与对方存在争议或涉及诉讼、仲裁的应收款项；已有明显迹象表明债务人很可能无法履行还款义务的应收款项等，进行单项评价信用风险。

（5）金融资产减值的会计处理方法

期末，本公司计算各类金融资产的预计信用损失，如果该预计信用损失大于其当前减值准备的账面金额，将其差额确认为减值损失；如果小于当前减值准备的账面金额，则将差额确认为减值利得。

6、 固定资产

（1）固定资产确认条件

固定资产指为生产商品、提供劳务、出租或经营管理而持有的使用寿命超过一年的房屋建筑物、机器设备、运输工具及其它与经营有关的工器具等。与该固定资产有关的经济利益很可能流入企业，以及该固定资产的成本能够可靠地计量时予以确认。

（2）固定资产的计价

固定资产按成本进行初始计量。购买固定资产的价款超过正常信用条件延期支付，实质上具有融资性质的，固定资产的成本以购买价款的现值为基础确定。实际支付的价款与购买价款的现值之间的差额，除应予资本化的以外，在信用期间内计入当期损益。

（3）固定资产后续计量

公司对所有固定资产计提折旧，除对已提足折旧仍继续使用的固定资产外，与固定资产有关的后续支出，符合固定资产确认条件的，计入固定资产成本；不符合固定资产确认条件的，在发生时计入当期损益。

（4）固定资产折旧方法：

公司对除已经提足折旧仍继续使用的固定资产和单独计价入账的土地外的所有固定资产按规定采用平均年限法计算折旧，并按分类折旧率计提折旧，预计残值率为 5%，分类、估计经济折旧年限及折旧率如下：

固定资产类别	折旧年限（年）	残值率（%）	年折旧率（%）
房屋、建筑物	20 年	5%	4.75%
机器设备	5 年	5%	19%
运输工具	5 年	5%	19%
办公设备及其他设备	5 年	5%	19%
房屋、建筑物	20 年	5%	4.75%

已全额计提减值准备的固定资产，不再计提折旧，部分计提减值准备的固定资产按照扣除已提取减值准备后的余额计提折旧。

（5）固定资产减值测试方法及减值准备计提方法

期末，对单项固定资产由于市价持续下跌，或技术陈旧、损坏、长期闲置等原因，导致其可收回金额低于账面价值的，并且这种降低的价值在可预计的将来期间内不能恢复时，按可收回金额低于其账面价值的差额，计提固定资产减值准备。预计的固定资产减值损失计入当期损益类账项。对存在下列情况之一的固定资产，按固定资产单项项目全额计提减值准备：

①长期闲置不用，在可预见的未来不会再使用，且已无转让价值的固定资产；

②由于技术进步等原因，已不可使用的固定资产；

③虽然固定资产尚可使用，但使用后产生大量不合格品的固定资产；

④已遭毁损，以至于不再具有使用价值和转让价值的固定资产；

⑤他实质上已经不能再给公司带来经济利益的固定资产。

固定资产减值损失一经确认,在以后会计期间不得转回。

7、职工薪酬

职工薪酬，是指企业为获得职工提供的服务或解除劳动关系而给予的各种形式的报酬或补偿。职工薪酬包括短期薪酬、离职后福利、辞退福利和其他长期职工福利。

本公司职工薪酬主要包括短期职工薪酬、离职后福利、辞退福利以及其他长期职工福利。其中：

短期薪酬主要包括工资、奖金、津贴和补贴、职工福利费、医疗保险费、生育保险费、工伤保险费、住房公积金、工会经费和职工教育经费、非货币性福利等。本公司在职工为本公司提供服务的会计期间将实际发生的短期职工薪酬确认为负债，并计入当期损益或相关资产成本。其中非货币性福利按公允价值计量。

8、收入确认原则

公司按以下规定确认营业收入实现，并按已实现的收入记账，计入当期损益。

销售商品，本公司已将商品所有权上的主要风险和报酬转换给购货方，公司不再对该商品实施继续管理权和实际控制权，相关的收入已经收到或取得了收款的证据，并且与销售该商品有关的成本能够可靠地计量时，确认营业收入的实现。

提供劳务（不包括长期合同），①劳务在同一年度内开始并完成的，在劳务已经提供，收到价款或取得收取款项的证据时，确认劳务收入；②劳务的开始和完成分属不同会计年度的，在劳务合同的总收入、劳务的完成程度能够可靠地确定，与交易相关的价款能够流入，已经发生的成本和完成劳务将要发生的成本能够可靠计量时，按完工百分比法确认劳务收入。

让渡资产使用权收入，按有关合同、协议规定的收费时间和方法计算确认营业收入的实现。

9、企业所得税的会计处理方法

所得税的会计处理采用应付税款法，按照当期计算的应缴所得税额确认为当期所得税费用方法。

汇算清缴的方式：季度预缴，年终汇算清缴。

五、 会计政策、会计估计变更以及差错更正的说明

1、会计政策变更

本公司 2024 年度无应披露的会计政策变更。

2、会计估计变更

本公司 2024 年度无应披露的会计估计变更事项。

3、重要前期差错更正

本公司 2024 年度无应披露的重要前期差错更正。

六、 税项

1、主要税种及税率

税种	具体税率情况
增值税	按增值额计缴。

城市维护建设税	按实际缴纳的流转税的7%计缴。
教育费附加	按实际缴纳的流转税的3%计缴。
地方教育费附加	按实际缴纳的流转税的2%计缴。
企业所得税	按计税基础的15%计缴。
个人所得税	代扣代缴。

七、 财务报表重要项目的说明

下列所披露的财务报表数据，除特别注明之外，“年初”系指 2023 年 12 月 31 日，“年末”系指 2024 年 12 月 31 日，“本年”系指 2024 年 1 月 1 日至 12 月 31 日，“上年”系指 2023 年 1 月 1 日至 12 月 31 日，货币单位为人民币元。

1、货币资金

项　目	年末余额	年初余额
现金	134,911.37	153,050.19
银行存款	14,524,449.73	23,739,577.39
其他货币资金	240,310.00	127,000.00
合　计	**14,899,671.10**	**24,019,627.58**

其中受限货币资金为银行履约保函 127,000.00 元

2、应收票据

项　目	年末余额	年初余额
银行承兑汇票		1,510,000.00
合　计		**1,510,000.00**

3、应收账款

（1）账龄分析

账龄	年末余额		年初余额	
	账面余额	比例（%）	账面余额	比例（%）
1 年以内	9,166,528.00	61.89	7,365,341.62	51.07
1-2 年	1,226,400.00	8.28	3,153,750.00	21.87
2-3 年	1,404,500.00	9.48	638,400.00	4.43
3-4 年	570,900.00	3.85	3,183,542.00	22.08
4-5 年	2,443,542.00	16.50	80,000.00	0.55
5 年以上				
小　计	14,811,870.00		14,421,033.62	
减：坏账准备			61,500.00	
合　计	**14,811,870.00**	**100.00**	**14,359,533.62**	**100.00**

（2）按坏账计提方法列示

类别	期末余额				
	账面余额		坏账准备		账面价值
	金额	比例（%）	金额	计提比例（%）	
单项计提坏账准备的应收账款					
按组合计提坏账准备的应收账款	14,811,870.00	100.00			14,811,870.00
其中：预期信用损失组合	14,811,870.00	100.00			14,811,870.00
合计	14,811,870.00	100.00			14,811,870.00

4、应收款项融资

项　目	年末余额	年初余额
银行承兑汇票	320,000.00	440,000.00
合　计	**320,000.00**	**440,000.00**

5、其他应收款

（1）账龄分析

账　龄	年末余额			年初余额		
	账面余额	比例（%）	坏账准备	账面余额	比例（%）	坏账准备
1 年以内	11,673,886.15	90.09		2,369,068.05	84.57	
1 至 2 年	946,698.91	7.31		142,260.31	5.08	
2 至 3 年	49,500.00	0.38		1,863.00	0.07	
3 至 4 年						
4 至 5 年				288,200.00	10.29	
5 年以上	288,200.00	2.22				
合　计	**12,958,285.06**	**100.00**		**2,801,391.36**	**100.00**	

6、存货

项目	年末余额			年初余额		
	金额	跌价准备	账面价值	金额	跌价准备	账面价值
原材料	116,524.74		116,524.74	116,524.74		116,524.74
合计	**116,524.74**		**116,524.74**	**116,524.74**		**116,524.74**

7、长期股权投资

项目	年末余额	年初余额
长期股权投资	400,000.00	400,000.00

项目	年末余额	年初余额
合　计	400,000.00	400,000.00

8、固定资产

项　　目	年初余额	本年增加额	本年减少额	年末余额
一、原价合计	**20,766,798.33**	**801,514.32**	**628,213.18**	**20,940,099.47**
其中：房屋、建筑物	15,944,650.20			15,944,650.20
运输设备	826,086.44	198,486.73	581,661.44	442,911.73
电子设备	2,651,393.56	548,007.79		3,199,401.35
办公设备及其他	1,344,668.13	55,019.80	46,551.74	1,353,136.19
二、累计折旧合计	**16,890,362.94**	**996,513.31**	**596,802.52**	**17,290,073.73**
其中：房屋、建筑物	12,966,124.89	756,093.12		13,722,218.01
运输设备	784,782.12		552,578.37	232,203.75
电子设备	2,222,719.84	138,254.58		2,360,974.42
办公设备及其他	916,736.09	102,165.61	44,224.15	974,677.55
三、固定资产减值准备累计金额合计				
其中：房屋、建筑物				
运输设备				
电子设备				
办公设备及其他				
四、固定资产账面价值合计	**3,876,435.39**			**3,650,025.74**
其中：房屋、建筑物	2,978,525.31			2,222,432.19
运输设备	41,304.32			210,707.98
电子设备	428,673.72			838,426.93
办公设备及其他	427,932.04			378,458.64

9、无形资产

项目	年初余额	本年增加	本年减少	年末余额
一、原价合计	**34,379,655.75**			**34,379,655.75**
非专利技术	34,342,685.75			34,342,685.75
软件	36,970.00			36,970.00
二、累计摊销额合计	**31,945,389.74**	**2,434,266.01**		**34,379,655.75**
非专利技术	31,908,419.74	2,434,266.01		34,342,685.75
软件	36,970.00			36,970.00
三、无形资产减值准备合计				
非专利技术				
软件				
四、无形资产账面价值合计	2,434,266.01			
非专利技术	2,434,266.01			

软件				

10、开发支出

项目	年末余额	年初余额
开发支出	46,408,322.29	41,988,385.42
合计	**46,408,322.29**	**41,988,385.42**

11、应付账款

（1）应付账款账龄情况

账龄	年末余额	年初余额
1 年以内		
1 至 2 年		
2 至 3 年		23,940.00
3 至 4 年	23,940.00	59,813.00
4 至 5 年	59,813.00	81,270.00
5 年以上	125,930.00	44,660.00
合　计	**209,683.00**	**209,683.00**

12、合同负债

（1）合同负债账龄情况

账龄	年末余额	年初余额
1 年以内	543,009.26	463,100.00
1 至 2 年	46,600.00	77,000.00
2 至 3 年	77,000.00	109,250.00
3 至 4 年	64,250.00	175,000.00
4 至 5 年	175,000.00	6,000.00
5 年以上	154,000.00	148,000.00
合　计	**1,059,859.26**	**978,350.00**

13、应付职工薪酬

项目	年初余额	本年增加额	本年减少额	年末余额
一、短期薪酬				
1、工资、奖金、津贴和补贴	16,298.42	35,336,953.67	35,336,953.67	16,298.42
2、职工福利费		314,590.58	314,590.58	
其中：非货币性福利				
3、基本医疗保险费	203,943.61	2,966,111.91	2,916,300.82	253,754.70
4、补充医疗保险费		100,747.26	100,747.26	
5、工伤保险费	3,809.33	55,793.24	54,770.80	4,831.77
6、生育保险费	15,237.51	205,991.47	201,901.50	19,327.48

项目	年初余额	本年增加额	本年减少额	年末余额
7、住房公积金		2,703,873.20	2,703,873.20	
8、工会经费和职工教育经费		124,322.18	124,322.18	
二、离职后福利				
1、基本养老保险费	443,987.04	6,487,383.80	6,390,594.00	540,776.84
2、年金缴费（补充养老保险）				
3、失业保险费	18,825.17	269,724.45	266,227.48	22,322.14
三、辞退福利及内退补偿		31,586.66	31,586.66	
其中：1.因解除劳动关系给予的补偿		31,586.66	31,586.66	
2.预计内退人员支出				
四、其他福利				
合　计	**702,101.08**	**48,597,078.42**	**48,441,868.15**	**857,311.35**

14、应交税费

项目	年末余额	年初余额
增值税	962,741.99	744,331.10
企业所得税	139,529.52	104,583.24
城建税	67,692.28	51,520.07
个人所得税	263,491.51	170,675.17
教育费附加	29,010.98	22,080.03
地方教育费附加	19,250.65	14,720.02
合　计	**1,481,716.93**	**1,107,909.63**

15、其他应付款

项目	年末余额	年初余额
应付利息		
应付股利		
其他应付款	858,900.50	927,645.05
合计	**858,900.50**	**927,645.05**

（1）按款项性质列示的其他应付款

项目	年末余额	年初余额
保证金	854,900.00	922,873.00
保险公积金		771.55
关联方往来款	4,000.50	4,000.50
合计	**858,900.50**	**927,645.05**

16、实收资本

投资者名称	年末余额		年初余额	
	投资金额	所占比例	投资金额	所占比例

投资者名称	年末余额		年初余额	
	投资金额	所占比例	投资金额	所占比例
中国科学院信息工程研究所	12,500,000.00	25%	12,500,000.00	25%
长春吉大正元信息技术股份有限公司	11,000,000.00	22%	11,000,000.00	22%
航天信息股份有限公司	11,000,000.00	22%	11,000,000.00	22%
吉林省伟孚科技有限公司	10,500,000.00	21%	10,500,000.00	21%
北京中科正阳信息安全技术有限公司	5,000,000.00	10%	5,000,000.00	10%
合计	**50,000,000.00**	100%	**50,000,000.00**	100%

17、资本公积

项目	年初余额	本年增加	本年减少	年末余额
资本溢价	27,200,000.00			27,200,000.00
其他资本公积	37,353.57			37,353.57
合计	**27,237,353.57**			**27,237,353.57**

18、盈余公积

项目	年末余额	年初余额
法定盈余公积	1,401,546.06	1,293,870.81
合计	**1,401,546.06**	**1,293,870.81**

19、未分配利润

项目	本年金额	上年金额
调整前上年末未分配利润	9,489,250.98	8,985,015.08
调整年初未分配利润合计数（调增+，调减-）		
调整后年初未分配利润	9,489,250.98	8,985,015.08
加：本期归属于母公司所有者的净利润	1,076,752.53	560,262.11
减：提取法定盈余公积	-107,675.25	-56,026.21
提取任意盈余公积		
提取专项储备		
应付普通股股利		
转作股本的普通股股利		
其他减少		
期末未分配利润	10,458,328.26	9,489,250.98

20、 营业收入和营业成本

项目	本年发生额		上年发生额	
	收入	成本	收入	成本
1.主营业务小计	84,177,823.97	25,826,479.09	68,764,469.89	17,892,558.92
主营业务收入	84,177,823.97	25,826,479.09	68,764,469.89	17,892,558.92

2.其他业务小计				
其他				
合　计	84,177,823.97	25,826,479.09	68,764,469.89	17,892,558.92

21、税金及附加

项目	本年发生额	上年发生额
城市建设维护税	244,266.65	190,651.37
教育费附加	104,685.69	81,707.70
地方教育费附加	69,700.45	54,471.82
房产税	124,327.40	124,327.40
印花税	38,948.56	35,137.17
土地使用税	1,340.28	1,340.28
车船税	783.33	2,250.00
合计	**584,052.36**	**489,885.74**

22、销售费用

项目	本年发生额	上年发生额
工资	8,543,432.46	6,770,477.52
差旅费	476,757.38	552,931.57
业务招待费	2,539,141.67	2,858,790.27
交通费	379,089.01	383,423.97
通讯费	139,097.90	125,193.27
社会保险费	1,534,705.36	1,237,770.25
住房公积金	315,815.20	204,908.00
福利费	23,474.80	31,872.25
办公费	251,544.42	173,631.25
会议费	17,400.00	98,363.79
其他	218,207.55	
广告宣传费	42,337.64	116,252.59
合　计	**14,481,003.39**	**12,553,614.73**

23、管理费用

项目	本年发生额	上年发生额
工资	5,292,508.43	4,780,263.22
社会保险费	957,702.54	847,328.50
住房公积金	272,576.00	214,240.00
福利费	249,472.58	237,436.73
职工教育经费	124,322.18	100,121.79
无形资产摊销	2,434,266.01	2,434,268.88
办公费用	546,967.96	368,008.04
交通费	361,559.81	350,661.09

项目	本年发生额	上年发生额
通讯费	51,399.20	58,690.20
资料费	1,445.18	2,183.72
物业管理费	316,263.03	438,674.20
折旧费用	980,073.92	955,567.23
业务招待费	1,354,334.00	948,467.08
差旅费	137,935.20	146,710.25
固定电话费	7,462.62	7,655.06
水电费	24,528.18	29,106.27
残疾人保证金		5,255.28
公车维护费	78,897.22	97,565.93
房租	366,481.84	172,007.72
中介费	97,735.85	162,017.67
保密管理经费	166,925.54	35,583.14
离职补偿金	31,586.66	241,940.83
资质申请维护费	662,314.63	171,209.77
其他	109,080.68	87,313.63
广告宣传费	100,228.97	3,141.59
咨询费	123,781.52	22,277.23
会议费	44,571.50	6,415.09
合 计	**14,894,421.25**	**12,924,110.14**

24、研发费用

项目	本年发生额	上年发生额
工资	17,653,525.09	17,379,542.95
社会保险费	3,731,042.47	3,574,720.90
住房公积金	624,194.00	488,258.00
福利费	41,643.20	44,601.25
通讯费	228,453.49	185,765.18
交通费	510,208.25	466,243.90
产品检验费		120,000.00
折旧费	16,439.39	19,666.27
咨询费	4,600.00	3,550.00
委托开发费		81,000.00
耗材		1,196.98
差旅费	1,782,418.73	758,609.08
资质申请费		23,000.00
办公费用	13,449.05	49,254.28
燃料动力费	52,838.22	76,637.92
软件费	43,508.67	124,091.50

知识产权费	144,920.75	115,841.59
试验费	300,000.00	300,000.00
配件研发	1,858.41	13,588.00
服务费	837,736.19	795,807.19
其他	636,770.20	486,153.85
合计	**26,623,606.11**	**25,107,528.84**

25、财务费用

项目	本年发生额	上年发生额
利息支出		
减：利息收入	11,898.05	30,794.26
利息净支出		
汇兑损失		
减：汇兑收益		
汇兑净损失		
银行手续费	8,106.60	9,135.67
其他		
合计	**-3,791.45**	**-21,658.59**

26、其他收益

项目	本年发生额	上年发生额
国家项目补助收入	119,003.48	814,518.92
合计	**119,003.48**	**814,518.92**

（1）2024 年度政府补助明细

项目名称	本年发生额	上年发生额
政府补贴	84,000.00	720,000.00
软件产品退税		11,390.13
增值税加计抵减	8,330.04	57,885.90
个税返还	26,673.44	25,242.89
合计	**119,003.48**	**814,518.92**

27、信用减值损失

项目	本年发生额	上年发生额
应收账款坏账准备	739,300.00	28,500.00
合计	**739,300.00**	**28,500.00**

28、营业外收入

项目	本年发生额	上年发生额
其他	137,702.56	57,574.52
合　计	**137,702.56**	**57,574.52**

29、营业外支出

项目	本年发生额	上年发生额
其他	27,624.00	2,891.66
合　计	**27,624.00**	**2,891.66**

30、所得税费用

项目	本年发生额	上年发生额
当期所得税费用	185,082.73	98,869.78
合计	**185,082.73**	**98,869.78**

31、现金流量情况

（1）采用间接法将净利润调节为经营活动现金流量的信息：

补充资料	本年发生额	上年发生额
1．将净利润调节为经营活动现金流量：		
净利润	1,076,752.53	560,262.11
加：信用减值准备	739,300.00	28,500.00
固定资产折旧	996,513.31	975,233.50
无形资产摊销	2,434,266.01	2,434,268.88
长期待摊费用摊销		
待摊费用减少（减：增加）		
待摊费用增加（减：减少）		
处置固定资产、无形资产和其他长期资产的损失（收益以“－”号填列）		
固定资产报废损失（收益以“－”号填列）	4,410.66	
财务费用（收益以“－”号填列）		
投资损失（收益以“－”号填列）		
递延所得税资产减少（增加以“－”号填列）		
递延所得税负债增加（减少以“－”号填列）		
存货的减少（增加以“－”号填列）		
经营性应收项目的减少（增加以“－”号填列）	-14,251,776.95	-1,311,517.78
经营性应付项目的增加（减少以“－”号填列）	541,782.28	-267,729.55
其他		
经营活动产生的现金流量净额	-8,458,752.16	2,419,017.16
2、不涉及现金收支的重大投资和筹资活动：		
债务转为资本		
一年内到期的可转换公司债券		
融资租入固定资产		
3、现金及现金等价物净变动情况：		
现金的期末余额	14,659,361.10	23,892,627.58

补充资料	本年发生额	上年发生额
3、现金的年初余额	23,892,627.58	21,854,170.19
加：现金等价物的期末余额		
减：现金等价物的年初余额		
现金及现金等价物净增加额	-9,233,266.48	2,038,457.39

（2）现金和现金等价物的有关信息

项目	本年余额	上年余额
一、现金	14,659,361.10	23,892,627.58
其中：库存现金	134,911.37	153,050.19
可随时用于支付的银行存款	14,524,449.73	23,739,577.39
可随时用于支付的其他货币资金		
可用于支付的存放中央银行款项		
存放同业款项		
拆放同业款项		
二、现金等价物	240,310.00	127,000.00
其中：银行履约保函	240,310.00	127,000.00
三、期末现金及现金等价物余额	14,899,671.10	24,019,627.58
其中：母公司或集团内子公司使用受限制的现金和现金等价物	240,310.00	127,000.00

八、 关联方关系

1、关联方的认定标准

由本公司控制、共同控制或施加重大影响的另一方，或者能对本公司实施控制、共同控制或重大影响的一方；或者同受一方控制、共同控制或重大影响的另一企业，被界定为本公司的关联方。

2、 关联方关系

（1）存在控制关系的关联方

本公司不存在最终控制方。

（2）不存在控制关系的关联方

关联方名称	与本公司之关系
中国科学院信息工程研究所	本公司之股东
长春吉大正元信息技术股份有限公司	本公司之股东
航天信息股份有限公司	本公司之股东
吉林省伟孚科技有限公司	本公司之股东
北京中科正阳信息安全技术有限公司	本公司之股东

九、 或有事项的说明

本公司不存在应披露的未决诉讼、对外担保等或有事项。

十、资产负债表日后调整事项

截至 2024 年 12 月 31 日，本公司不存在应披露的资产负债表日后事项。

十一、按照有关财务会计制度应披露的其他内容

本公司不存在应披露的其他内容。

十二、财务报表的批准

本财务报表经本公司董事会于 2025 年 2 月 9 日批准。

公司名称：中科信息安全共性技术国家工程研究中心有限公司

统一社会信用代码

91110102082881146K

营业执照

(副 本)(5-1)

扫描市场主体身份码了解更多登记、备案、许可、监管信息，体验更多应用服务。

名　　称　中兴华会计师事务所（特殊普通合伙）

出 资 额　8506 万元

类　　型　特殊普通合伙企业

成立日期　2013 年 11 月 04 日

执行事务合伙人　李尊农、乔久华

主要经营场所　北京市丰台区丽泽路 20 号院 1 号楼南楼 20 层

经营范围　一般项目：工程造价咨询业务；工程管理服务；资产评估。（除依法须经批准的项目外，凭营业执照依法自主开展经营活动）许可项目：注册会计师业务；代理记账。（依法须经批准的项目，经相关部门批准后方可开展经营活动，具体经营项目以相关部门批准文件或许可证件为准）（不得从事国家和本市产业政策禁止和限制类项目的经营活动。）

登记机关　北京市丰台区市场监督管理局

2024 年 09 月 29 日

国家企业信用信息公示系统网址：http://www.gsxt.gov.cn

市场主体应当于每年 1 月 1 日至 6 月 30 日通过国家企业信息公示系统报送公示年度报告。

国家市场监督管理总局监制

会计师事务所

执业证书

名　　称：中兴华会计师事务所（特殊普通合伙）

首席合伙人：李尊农

主任会计师：

经营场所：北京市丰台区丽泽路20号院1号楼南楼20层

组织形式：特殊普通合伙

执业证书编号：11000167

批准执业文号：京财会许可〔2013〕0066号

批准执业日期：2013年10月25日

证书序号：0014686

说　明

1、《会计师事务所执业证书》是证明持有人经财政部门依法审批，准予执行注册会计师法定业务的凭证。

2、《会计师事务所执业证书》记载事项发生变动的，应当向财政部门申请换发。

3、《会计师事务所执业证书》不得伪造、涂改、出租、出借、转让。

4、会计师事务所终止或执业许可注销的，应当向财政部门交回《会计师事务所执业证书》。

发证机关：北京市财政局

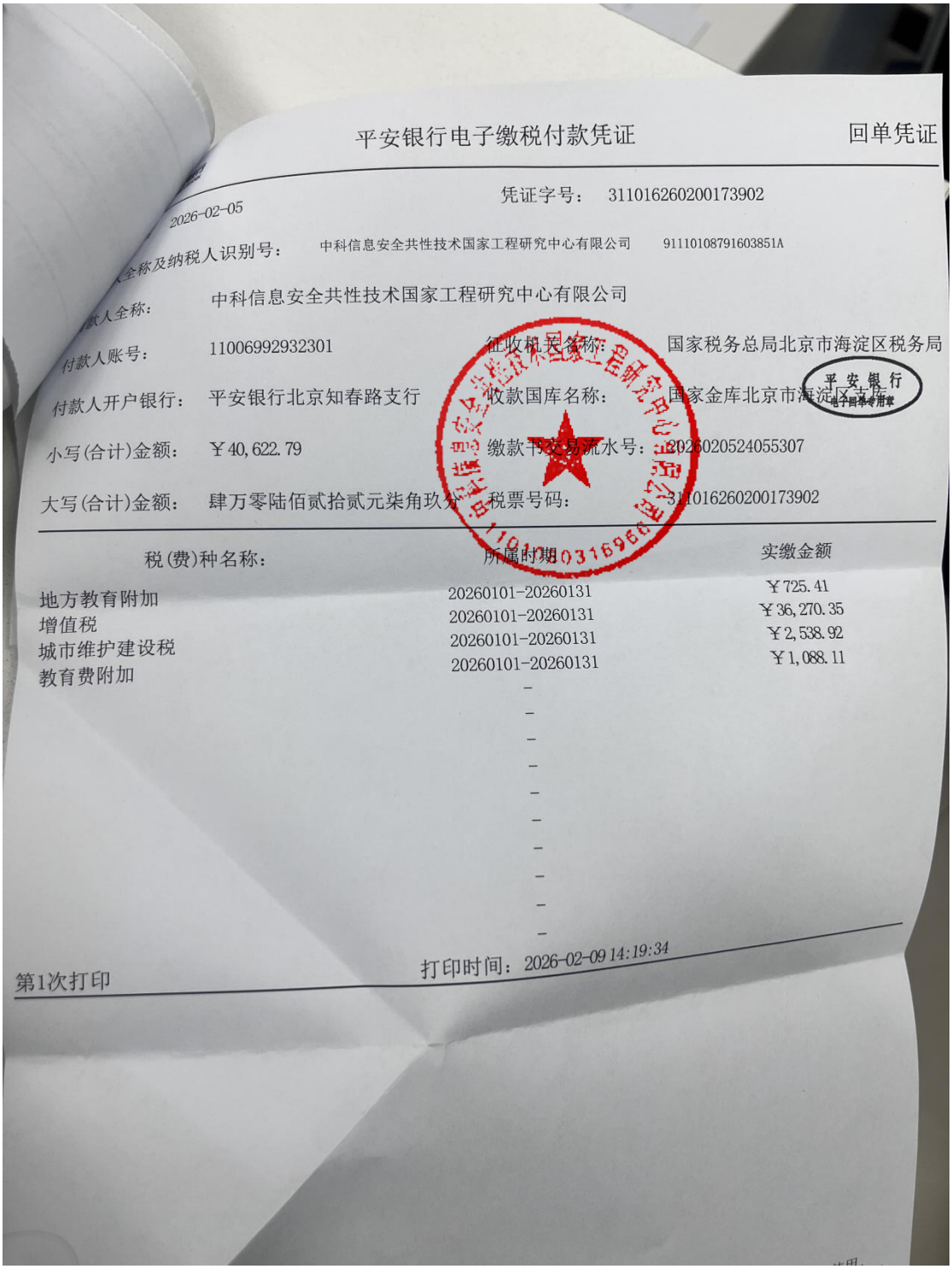
二〇二一年八月十七日

中华人民共和国财政部制

1.2.2. 依法缴纳税收和社会保障资金的良好记录

1.2.2.1. 依法缴纳税收证明材料

1.2.2.1.1. 2026年1月纳税



平安银行电子缴税付款凭证　　回单凭证

凭证字号：311016260200173902

2026-02-05

纳税人全称及纳税人识别号：中科信息安全共性技术国家工程研究中心有限公司　91110108791603851A

付款人全称：中科信息安全共性技术国家工程研究中心有限公司

付款人账号：11006992932301　　征收机关名称：国家税务总局北京市海淀区税务局

付款人开户银行：平安银行北京知春路支行　　收款国库名称：国家金库北京市海淀区支库

小写(合计)金额：￥40,622.79　　缴款书交易流水号：20260205240553O7

大写(合计)金额：肆万零陆佰贰拾贰元柒角玖分　　税票号码：311016260200173902

税(费)种名称：	所属时期	实缴金额
地方教育附加	20260101-20260131	￥725.41
增值税	20260101-20260131	￥36,270.35
城市维护建设税	20260101-20260131	￥2,538.92
教育费附加	20260101-20260131	￥1,088.11

第1次打印　　打印时间：2026-02-09 14:19:34

1.2.2.2. 依法缴纳社会保障资金证明材料

1.2.2.2.1. 2026 年 1 月社保

平安银行电子缴税付款凭证　　回单凭证

2026-02-10　　凭证字号：411016260200317656

纳税人识别号：　中科信息安全共性技术国家工程研究中心有限公司　911101087916038 51A

付款人全称：　中科信息安全共性技术国家工程研究中心有限公司

付款人账号：　11006992932301　　征收机关名称：　国家税务总局北京市海淀区税务局

付款人开户银行：　平安银行北京知春路支行　　收款国库名称：　国家金库北京市海淀区支库

小写(合计)金额：　￥1,004,334.74　　缴款书交易流水号：　202602102481155 6

大写(合计)金额：　壹佰万肆仟叁佰叁拾肆元柒角肆分　　税票号码：　411016260200317656

税(费)种名称：	所属时期	实缴金额
失业保险费	20260101-20260131	￥27,125.90
基本医疗保险费	20260101-20260131	￥238,707.57
企业职工基本养老保险费	20260101-20260131	￥651,019.92
工伤保险费	20260101-20260131	￥5,467.86
基本医疗保险费	20260101-20260131	￥54,251.66
基本医疗保险费	20260101-20260131	￥27,761.83

第2次打印　　打印时间：2026-02-11 14:07:43

1.2.3. 具有履行合同所必需的设备和专业技术能力

致：北京市文化和旅游局宣传中心（北京市旅游运行监测中心）

我单位具备履行合同所必需的设备和专业技术能力

投标人名称：中科信息安全共性技术国家工程研究中心有限公司

日期：2026 年 3 月 24 日

1.2.4. 承诺函

致：北京市文化和旅游局宣传中心（北京市旅游运行监测中心）

我单位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（重大违法记录指因违法经营受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚，不包括因违法经营被禁止在一定期限内参加政府采购活动，但期限已经届满的情形）等情况

我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：中科信息安全共性技术国家工程研究中心有限公司

日期：2026 年 3 月 24 日

1.3. 落实政府采购政策需满足的资格要求

1.3.1. 中小企业证明材料

1.3.1.1. 中小企业声明函

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）参加北京市文化和旅游局宣传中心（北京市旅游运行监测中心）***（单位名称）***的网络安全服务项目***（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．信息系统测评***（标的名称）***，属于软件和信息技术服务业***（采购文件中明确的所属行业）***行业；制造商为中科信息安全共性技术国家工程研究中心有限公司***（企业名称）***，从业人员 188 人，营业收入为 6110.33 万元，资产总额为 9149.49 万元，属于中型企业***（中型企业、小型企业、微型企业）***；

2．_____***（标的名称）***，属于_____***（采购文件中明确的所属行业）***行业；制造商为_____***（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。

企业名称（盖章）：中科信息安全共性技术国家工程研究中心有限公司

日期：2026 年 3 月 24 日

1.3.1.2. 残疾人福利性单位声明函

我公司非残疾人福利性单位

1.3.1.3. 监狱企业证明文件

我公司非监狱企业

1.3.2. 拟分包情况说明

不适用

1.3.3. 其它落实政府采购政策的资格要求

无

1.4 联合体协议书

不适用

1.5. 特定资格证书

无

2. 投标标的符合性证明文件

无

3. 其他文件

3.1. 法定代表人身份证明

法定代表人身份证明

单位名称：中科信息安全共性技术国家工程研究中心有限公司

单位性质：其他有限责任公司

地　　址：北京市海淀区中关村大街 19 号 16 层 B1601、B1602、B1603、B1605

成立时间：2006 年 8 月 9 日

经营期限：2006 年 08 月 09 日至 2036 年 08 月 08 日

潘毅（*法定的代表人姓名*）系中科信息安全共性技术国家工程研究中心有限公司（*投标人名称*）的法定代表人，本人相关信息如下：

性别：男

年龄：47

职务：董事长

特此证明。

附：法定代表人身份证：

投标人名称：中科信息安全共性技术国家工程研究中心有限公司（盖章）

日　　期：2026 年 3 月 24 日

3.2. 法定代表人授权委托书

法定代表人授权委托书

本人潘毅（姓名）系中科信息安全共性技术国家工程研究中心有限公司（投标人名称）的法定代表人，现委托 解淳皓 （姓名）为我方代理人。代理人根据授权，以我方名义签署、澄清、说明、补正、提交、撤回、修改网络安全服务项目（项目名称）1100002621020016375 5-XM001（项目编号）包 2（标包号、标包名称）投标文件和 / （其他授权委托事项）并处理有关事宜，其法律后果由我方承担。

本授权书于 2026 年 3 月 24 日生效，委托期限：90 天（**特别提醒：**其中委托期限可短于投标有效期，但生效日期或授权书委托期限的开始日期不得晚于投标文件其他相关文件中委托代理人的签署日期，截止日期不得早于开标日期）。

代理人证件类型：身份证，证件号码：211281200102172010。

代理人无转委托权。

投标人名称：中科信息安全共性技术国家工程研究中心有限公司（盖章）

法定代表人（签字或签章）：潘毅

签发日期：2026 年 3 月 24 日

承　　诺

以上授权委托书系法定代表人签字签发，如有不实，代理人愿意承担法律责任。

附：代理人身份证：

代理人（签字或签章）解淳皓

日　期：2026 年 3 月 24 日

3.3. 投标保证金提交证明

3.3.1. 投标保证金

平安银行 收付款业务回单 回单凭证

记账日期：2026-03-16　回单号：26031603100010000146　验证码：816725

付款人名称：中科信息安全共性技术国家工程研究中心有限公司　收款人名称：国讯招标集团有限公司

付款人账号：11006992932301　收款人账号：110932339510101

付款人开户行：平安银行北京知春路支行　收款人开户行：招商银行股份有限公司北京丽泽商务区支行

币种：人民币　大写金额：壹万元整　小写：10,000.00

备注：11000026210200163755-XM001(网银)

平安银行 电子回单专用章

已打印次数：1　打印时间：2026-03-16 17:35:03　设备编号：0000

打印方式：网银　柜员号：0000　网点号：

温馨提示：1、每笔业务回单对应唯一的回单号，回单号相同即为同一笔业务；2、凭回单号+验证码可在我行柜台、自助终端、平安数字口袋App（登录-快速查询区-电子回单查询）验证回单信息。

3.3.2. 投标保证金信息表

序号	类别	具体信息		
1	项目名称	网络安全服务项目		
2	项目编号	11000026210200163755-XM001	标包号	包 2
3	投标人名称	中科信息安全共性技术国家工程研究中心有限公司		
4	保证金情况	金额	10000 元	
		形式	□支票☑汇票□本票□转账（汇款）□其他：____（请注明）	
5	承 诺 书	致：国讯招标集团有限公司（采购代理机构） 我方在你方组织的 网络安全服务项目 项目（项目编号：11000026210200163755-XM001）中若获得中标资格，保证在领取中标通知书时按招标文件的规定向你方一次性支付招标代理服务费，你方按下栏发票信息向我公司开具发票，因发票信息填写有误而导致的一切后果我方自行承担。 退还保证金时请按下栏退款账户信息划入我方账户（需与保证金凭证上所载的账户信息一致）。若因内容不全、错误、字迹潦草模糊、或开户名称和/或开户行和/或账号与划款时所用不一致而导致该项目保证金未能及时退还或退还过程中发生错误，我方将承担全部责任和损失。 特此承诺！		

6	发票信息	发票类型	☑增值税普通发票 ☐增值税专用发票（应附增值税一般纳税人证明材料）
		名　　称	中科信息安全共性技术国家工程研究中心有限公司
		纳税人识别号	91110108791603851A
		地　　址	北京市海淀区中关村大街 19 号 16 层 B1601、B1602、B1603、B1605
		电　　话	010-82486161
		开 户 行	平安银行北京知春路支行
		账　　号	11006992932301
		发票领取	电子发票接收人邮箱：xiech@nercis.ac.cn
7	退款账户	开户名称	中科信息安全共性技术国家工程研究中心有限公司
		开户银行	平安银行北京知春路支行
		银行账号	11006992932301

投标人名称：中科信息安全共性技术国家工程研究中心有限公司（盖章）

法定代表人或其委托代理人（签字或签章）：

日　　期：2026 年 3 月 24 日

网络安全服务项目

（项目编号：11000026210200163755-XM001）

第 2 标包：信息系统测评（标包名称）

投标文件

（第二册：商务技术分册）

投标人名称：中科信息安全共性技术国家工程研究中心有限公司（盖章）

法定代表人或其委托代理人：（签字或签章）

2026 年 3 月 24 日

1.1. 商务技术分册目录

注：1．该目录为方便评标委员会查找相关证明文件及评审条件，应尽可能的详细、清晰，投标人可根据自身情况补充完善。

2．投标文件的装订顺序应按此表顺序依次装订，并连续编排页码（电子文件可以采用页码机加盖页码）。

1.2. 评标索引

1.2.1. 符合性审查索引

审查因素	投标响应情况	投标文件页码范围	说明或备注
进口产品（如有）	不适用	/	/
投标范围	我方完全响应招标文件里的投标范围，无偏离	6	/
其他说明（要求）	无	/	/
合同分包	不适用	/	/
合同条款偏离	无偏离	25	/
采购需求偏离	无偏离	82	/
报价方式		6-7	/
报价货币	人民币	6-7	/
报价要求	按照招标文件要求进行报价，无偏离	6-8	/
最高限价	我方不超过最高限价，无偏离	6-8	/
投标有效期	满足招标文件	6	/
备选方案	不适用	/	/
投标文件签字盖章	/	/	/

注：本索引由投标人根据招标文件第三章“资格审查与评标办法”第 6.1 款规定的符合性审查标准和投标人实际响应情况逐项填写。

1.2.2. 评分索引

1.2.2.1. 商务部分评分索引

序号	评分因素	投标响应情况	投标文件页码范围	说明或备注
1	具有公安部第三研究所颁发的网络安全等级测评与检测评估机构服务认证证书	满足	69	
2	具有国家密码管理局颁发得商用密码检测机构资质证书	满足	70	
3	具有中国合格评定国家认可委员会颁发的有效的CNAS检验机构认可证书，且同时具有有效的CNAS实验室认可证书	满足	71-72	
4	国家信息安全漏洞库（CNNVD）技术支撑单位三级	满足	73	
5	信息安全风险评估（一级）	满足	错误！未定义书签。	
6	管理体系资质	我单位满足4项资质	74-77	
7	项目业绩	满足	27-64	
8	信息安全国家标准制定项目经验	满足	78-81	

注：本索引由投标人根据招标文件第三章“资格审查与评标办法”第6.3.4款规定的商务部分评分标准和投标人实际响应情况逐项填写

1.2.2.2. 技术部分评分索引

序号	评分因素	投标响应情况	投标文件页码范围	说明或备注
1	整体测评方案	满足	82-274	/
2	安全风险管理方案	满足	231	/
3	项目团队方案评价	满足	243	/
4	售后服务方案	满足	224	/
5	工具保障	满足	102	/
6	技术团队能力	满足	243-274	/

注：本索引由投标人根据招标文件第三章“资格审查与评标办法”第 6.3.5 款规定的技术部分评分标准和投标人实际响应情况逐项填写。

1. 价格部分

1.1. 投标函

投标函

致：北京市文化和旅游局宣传中心（北京市旅游运行监测中心）*（采购人名称）*

根据你方项目编号为 1100002621020016375 5-XM001 的网络安全服务项目（*项目名称*）包 2/信息系统测评（*标包号/标包名称*）的招标文件，投标人中科信息安全共性技术国家工程研究中心有限公司（*投标人名称、地址*）提交下述文件正本 1 份及副本/份。

据此，我方同意如下内容：

1. 我方愿意以报价 534000 元整；伍拾叁万肆仟元整*（注明币种，并用文字和数字表示的投标总价）*元人民币承包上述项目（标包）。

2. 我方按招标文件的规定，以电汇*（投标保证金形式）*提交人民币 10000.00*（用数字表示的具体金额）*元人民币的投标保证金，并同意招标文件第二章“投标人须知”第 17.5 款关于投标保证金不予退还的规定。

3. 我方已详细审核并确认全部招标文件，包括修改文件及有关附件。我们完全理解并同意放弃对这方面有不明及误解的权力。

4. 本投标有效期为自开标日起 90*（有效期日数）*日历日。

5. 我方将按招标文件的规定履行合同责任和义务。

6. 我方在此声明，所提交的投标文件及有关资料内容完整、真实和准确，且不存在招标文件第二章“投标人须知”第 6.2.5 款载明的任何一种情形。

7. 我方同意提供按照你方可能要求的与其投标有关的一切数据或资料，完全理解你方不一定接受最低价的投标。

8. 其他承诺：/*（如有）*。

9. 与本投标有关的一切正式信函请寄：

联系人：解淳皓　　电子邮件：xiech@nercis.ac.cn

地　址：北京市海淀区中关村大街 19 号 16 层 B1601、B1602、B1603、B1605

电　话：010-82486161

邮　编：100080　　传　真：010-82486355

投标人名称：中科信息安全共性技术国家工程研究中心有限公司（盖章）

法定代表人或其委托代理人（签字或签章）：

日　　期：2026 年 3 月 24 日

1.2. 开标一览表

开标一览表

项目名称：网络安全服务项目

项目编号：11000026210200163755-XM001　　标包号：2

序号	项目	内容
1	投标报价	大写：人民币**伍拾叁万肆仟元整** 小写：**¥534000 元整**
2	交付时间/实施时间	**2026 年 4 月 1 日至 2026 年 12 月 31 日。**
3	交付地点/实施地点	**采购人指定地点**
4	投标保证金	☑提　交 金额：人民币壹万元整（¥10000.00） 形式：电汇 ☐未提交
5	……	

投标人名称：中科信息安全共性技术国家工程研究中心有限公司（盖章）

法定代表人或其委托代理人（签字或签章）：

日　　期：2026年3月24日

1.3. 分项报价表

分项报价表

项目名称：网络安全服务项目

项目编号：11000026210200163755-XM001　　标包号：2

序号	服务名称	服务范围	服务要求	服务时间	服务标准	单价(元)	小计
1	北京智慧文旅平台-文旅数据中心系统	等保测评	三级复测评	2026年4月1日-12月31日	出具等保测评报告	85200	
2	北京智慧文旅平台一政府监管平台系统	等保测评	三级复测评	2026年4月1日-12月31日	出具等保测评报告	85200	
3	北京市旅游团队电子行程单（二期）和电子合同项目	等保测评	三级复测评	2026年4月1日-12月31日	出具等保测评报告	85200	
4	北京市文化和旅游局财务内控综合管理信息平台	等保测评	二级复测评	2026年4月1日-12月31日	出具等保测评报告	50000	
5	北京市文化和旅游局办公系统	等保测评	二级复测评	2026年4月1日-12月31日	出具等保测评报告	50000	
6	北京智慧文旅平台-文旅数据中心系统	密码应用安全性评估	三级	2026年4月1日-12月31日	出具密码测评报告	89200	
7	北京智慧文旅平台一政	密码应用安全性评估	三级	2026年4月1日-12月31	出具密码测评报告	89200	

	府监管平台系统			日			
						534000	
合计（投标报价）：伍拾叁万肆仟元整							

投标人名称：中科信息安全共性技术国家工程研究中心有限公司（盖章）

法定代表人或其委托代理人（签字或签章）：

日　　期：2026年3月24日

1.3.1. 中小企业证明材料

1.3.1.1. 中小企业声明函

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）参加北京市文化和旅游局宣传中心（北京市旅游运行监测中心）***（单位名称）***的网络安全服务项目 ***（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．信息系统测评 ***（标的名称）***，属于软件和信息技术服务业 ***（采购文件中明确的所属行业）***行业；制造商为中科信息安全共性技术国家工程研究中心有限公司 ***（企业名称）***，从业人员 188 人，营业收入为 6110.33 万元，资产总额为 9149.49 万元，属于中型企业 ***（中型企业、小型企业、微型企业）***；

2．____ ***（标的名称）***，属于_____ ***（采购文件中明确的所属行业）***行业；制造商为____ ***（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。

企业名称（盖章）：中科信息安全共性技术国家工程研究中心有限公司

日期：2026 年 3 月 24 日

1.3.1.2. 残疾人福利性单位声明函

我公司非残疾人福利性单位

1.3.1.3. 监狱企业证明文件

我公司非监狱企业

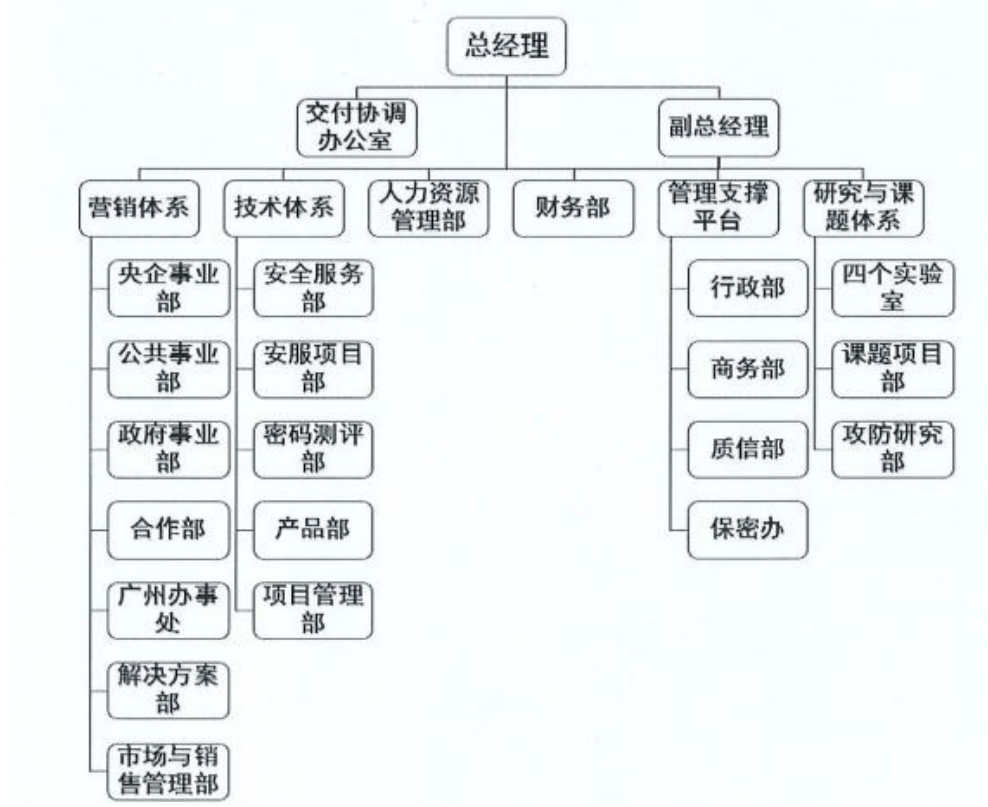
1.4. 拟分包情况说明

本项目不适用。

2. 商务部分

2.1. 投标人基本情况表

投标人名称	中科信息安全共性技术国家工程研究中心有限公司	统一社会信用代码	91110108791603851A
注册地址	北京市海淀区中关村大街 19 号 16 层 B1601、B1602、B1603、B1605		
联系人	解淳皓	联系电话	15042087476
投标人规模	☐大型企业 ☑中型企业 ☐小微企业 ☐其他	投标人特殊性	☐监狱企业 ☑其他 ☐残疾人福利性单位
投资类型	☐外商投资（☐外商单独投资 ☐外商部分投资） ☑内资		
投资国别	☐欧资企业 ☐美资企业 ☐日资企业 ☑其他		
投标人所属性别	☐女 ☑男（指拥有投标人 51%以上绝对所有权的性别；绝对所有权拥有者可以是一个人，也可以多人合计计算。）		
成立日期	2006 年 8 月 9 日	法定代表人	潘毅
注册资金	5000 万元	电话	010-82486161
传真	010-82486355	邮箱	xiech@nercis.ac.cn
网址	http://www.nercis.ac.cn		
主管单位	无		
经营范围	信息安全理论与标准研究、体系论证、大型信息安全系统设计、高性能信息安全产品开发、信息安全基础设施研究与应用、信息安全评测与管理；信息安全咨询与服务、技术引进与市场推广、技术转让与成果孵化；计算机软件生产与加工；计算机技术培训；会议服务；承办展览展示活动（企业依法自主选择经营项目，开展经营活动，依法须经批准的项目，经相关部门批准后依批准的内容开展经营活动；不得从事本市产业政策禁止和限制类项目的经营活动）		
资质等级	网络安全等级测评与检测评估机构服务认证证书 信息安全服务资质证书-安全工程类二级 信息安全应急处理二级服务资质 中国合格评定国家认可委员会 CNAS 检验机构认可证书 中国合格评定国家认可委员会 CNAS 检测实验室认可证书 质量管理体系认证证书（ISO 9001） 信息安全管理体系认证证书（ISO/IEC27001）		

<table>
<tr><td></td><td colspan="4">IT 服务管理体系认证证书（ISO/IEC20000-1）
环境管理体系认证证书（ISO 14001）
业务连续性管理体系证书（ISO 22301）
职业健康安全管理体系认证证书（ISO 45001）
企业信用评级证书（AAA）</td></tr>
<tr><td rowspan="3">员工总数</td><td rowspan="3">188 人，其中：</td><td>高级职称</td><td>中级职称</td><td>初级职称</td></tr>
<tr><td>1 人</td><td>20 人</td><td>30 人</td></tr>
<tr><td>管理人员</td><td>技术人员</td><td>其他人员</td></tr>
<tr><td>信用等级</td><td>AAA</td><td>上年度营业额</td><td colspan="2">6110.33 万元</td></tr>
<tr><td>组织结构框图</td><td colspan="4"> 
</td></tr>
<tr><td colspan="5">下属单位或分支机构情况</td></tr>
<tr><td>序号</td><td>名称</td><td>地址</td><td>主要负责人</td><td>联系方式</td><td>其他说明</td></tr>
<tr><td></td><td>无</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

2.2. 投标人简介

2.2.1. 企业信息

企业名称：中科信息安全共性技术国家工程研究中心有限公司

注册地址：北京市海淀区中关村大街19号16层B1601、B1602、B1603、B1605

联系地址：北京市海淀区中关村大街19号新中关大厦B座北翼16层

成立时间：2006年8月9日

经营期限：2006年08月09日至2036年08月08日

主管部门：无

营业执照注册号：911101087916038 51A

注册资本：5000万元

企业类型：其他有限责任公司

批准登记机关：北京市海淀区市场监督管理局

公司电话：010-82486161

传真：010-82486355

邮箱：xiech@nercis.ac.cn

邮编：100080

网站：http://www.nercis.ac.cn

2.2.2. 公司主营业务

主营业务：信息安全理论与标准研究、体系论证、大型信息安全系统设计、高性能信息安全产品开发、信息安全基础设施研究与应用、信息安全评测与管理；信息安全咨询与服务、技术引进与市场推广、技术转让与成果孵化；计算机软件生产与加工；计算机技术培训；会议服务；承办展览展示活动（企业依法自主选择经营项目，开展经营活动，依法须经批准的项目，经相关部门批准后依批准的内容开展经营活动；不得从事本市产业政策禁止和限制类项目的经营活动）

2.2.3. 企业简介

信息安全共性技术国家工程研究中心是国家发展和改革委员会批示（发改高技[2004]1551 号文件）成立的国家级工程研究中心，其依托法人实体单位是中科信息安全共性技术国家工程研究中心有限公司（以下简称“工程中心”），注册资金 5000 万元。

工程中心由中国科学院信息工程研究所等单位投资组建，工程中心的技术依托单位包括中国人民解放军总参第五十一研究所、北京电子科技学院和信息安全国家重点实验室。

工程中心总部位于北京市中关村核心区，研发基地位于中科院信息工程研究所。工程中心以增强我国信息安全产业核心竞争力为目标，开展信息安全保障体系相关的国家信息安全战略、安全体系结构、核心技术、产业标准、系统测评等共性支撑技术的研究、开发、服务与培训工作，加速我国信息安全领域科研成果向现实生产力的转化，推动我国信息安全产业的整体发展，满足国家信息安全战略的需求。

一、主要职能

- **标准制定验证**

参与信息安全国家标准、行业应用标准及规范的研究与制定工作。

● **关键技术研究**

以网络安全技术为核心的信息安全共性关键技术的研发与攻关，重点关注认证、网络安全防护、保密技术、等级保护、信息安全工程化技术等。

● **科技成果转化**

为信息安全科研成果提供转化和产业化平台，重点集中于国家信息安全保障体系建设所急需的信息安全共性构件、信息安全基础平台和高端核心产品。

● **信息安全服务**

为政府、央企、大型事业单位等各级组织机构提供信息安全整体咨询、风险评估、软件测试、信息安全规划与建设、渗透测试与加固、等级保护测评、源代码安全审计和安全运维等安全服务。

二、工程中心业务

◆ **关键技术研发**

根据国内信息安全保障实际需求和未来技术发展趋势，跟踪国际信息安全技术发展，有针对性地进行信息安全技术研究，并不断创新，以满足国家信息安全保障体系建设的需求。目前，公司重点关注以密码为核心的信息安全共性关键技术的研发与攻关，具体包括高强度认证技术、高性能网络安全防护技术、高安全等级系统软件、安全芯片技术、信息安全工程化技术等。

◆ **成果转化**

作为一个成果转化和产业化平台，具备信息安全工程化所需的全套软硬件环境，能够为信息安全科研成果的产业化提供必要的支撑条件，将有效加速信息安全科研成果的转化，全面拉近企业与科研单位的联系。近期成果转化的重点集中于国家信息安全保障体系建设所急需的信息安全共性构件、信息安全基础平台和高端核心产品。

◆ **标准制定与验证**

依据国家需求，进行信息安全国家标准、行业标准，特殊行业应用标准及规

范的研究与制订工作。一方面为国家及行业制定信息安全标准、法规和决策提供依据和技术支持；另一方面也为标准、协议的应用单位提供技术支撑环境。目前的重点是 PKI/PMI/KMI 标准、密码算法与应用标准、安全协议标准、密码应用接口标准、各种安全业务标准等。另外，公司还将陆续提供各种安全标准实现的一致性验证工具、手段和基本环境。

◆ **安全测评**

研究、开发针对信息系统和信息安全产品的安全测评技术、工具及手段，建立技术先进、客观公正的信息安全测评环境，依据统一的测评标准及流程规范，为包括政府、军队、大型企事业单位在内的各级组织以及信息安全产品开发商提供信息系统及信息安全产品的测评服务，测试、评估、验证信息系统及信息安全产品的安全性，为信息系统及信息安全产品的安全认证提供依据。

◆ **安全服务**

依照国际国内信息安全相关标准指南及最佳实践，为包括政府、军队、大型企事业单位在内的各级组织提供安全体系咨询规划服务、等级测评服务、风险评估与合规性检测服务、渗透服务与加固服务、安全解决方案设计服务、信息化密码保障基础甚是工程监理服务、安全运维服务、等级保护建设整改服务和远程网站安全事件主动预警监控服务。

◆ **人才培养**

依托下属三个实验室的技术力量，面向全社会个人及组织机构，提供面向不同层次需求及目标对象的信息安全专业培训及认证培训，普及信息安全理念及安全知识，提高信息安全管理及开发能力，保障组织信息安全建设及管理工作的顺利开展。

◆ **安全服务**

■ 风险评估与合规性检测服务

■ 安全运维服务

- 等级保护建设整改服务
- 渗透测试与加固服务
- 安全体系咨询规划服务
- 安全解决方案设计服务
- 等级保护测评服务
- 网站（互联网应用）远程安全监测服务
- 源代码安全检测审计服务
- ……

三、中心优势

1）实验室联盟

依托中关村开放实验室联盟，工程中心建立了信息安全产品合作机制，建设了技术验证平台，整合我国信息安全保障体系建设需要的关键技术和产品，提供“自主可控”的信息安全整体解决方案。

2）权威的技术专家团

工程中心专家委员会由院士和国内权威专家组成，为中心的重大决策和计划提供技术指导和咨询。

3）技术资源的有机整合

工程中心由国内优势的科研机构和企业组建，均是我国信息安全技术研究与工程建设的主力军，在信息安全领域具有各自的优势，并形成了有机整合。

4）强有力的研发后盾

工程中心依托中科院信息工程研究所和信息安全国家重点实验室，具有一批国内外知名的密码学专家和信息安全专家，以及一支以年轻博士为主体的 300 多人科研团队的支持。

5）人才优势

工程中心依托中科院信息工程研究所的人才储备优势，技术队伍强大，人员

结构合理。

四、发展历程

2004 年，工程中心建设项目通过发改委的立项审批（发改高技 [2004]1551 号文件），并依据批复要求，于 2006 年 8 月 9 日组建法人依托单位中科信息安全共性技术国家工程研究中心有限公司，进行中心的市场化建设与运营。

2007 年，发改委对工程中心的建设任务和目标进行批复（发改办高技 [2007] 2820 号），中心的建设实施方案确定，进入运行建设期。

2011 年 5 月，工程中心顺利完成发改委批复的所有建设任务，并正式通过北京市发改委组织的验收（京发改[2011]1085 号文）。

2012 年 11 月 16 日，国家发展和改革委员会会同科技部、财政部、海关总署、国家税务总局等部门，对工程中心进行授牌。

五、用户列表

- 中共中央办公厅
- 中国人民政治协商会议全国委员会
- 国家保密局
- 中华人民共和国文化和旅游部
- 国家广播电视总局
- 国家林业局
- 国家知识产权局
- 国家档案局
- 中国科学院
- 中国农业科学院
- 中国电力科学研究院
- 中国民用航空局

- 国家外国专家局
- 国家电力监管委员会
- 国家电网
- 中石油
- 中石化
- 中国烟草
- 中国移动
- 中国通用技术集团
- 中国投资担保公司
- 中国国际期货有限公司
- 中粮期货有限公司
- ……

六、工程中心荣誉

- 2019 年度石景山区网络安全工作-优秀技术支持单位
- 信息与网络安全保卫工作-技术保障单位
- 公安部组织专项行动-表扬信
- 《“一带一路”网络安全合作需求、风险与路径研究》-优秀奖
- 2019 年全国两会-第二届一带一路国际高峰论坛感谢信
- 国家重大活动网络安全保卫-技术支持单位
- 2017 年度网络安全重大问题联合研究协作机制优秀软课题-优秀奖
- 党的十九大网上安保工作-优秀团队
- 2017 年度全国网络安全等级保护测评机构先进单位
- 中国共产党第十九次全国代表大会-等保感谢信 2017\
- 一带一路国际合作高峰论坛网络安全保卫组感谢信-2017
- 2016 年度全国网络安全等级保护测评机构先进单位
- 等保办公室感谢信 2015 北京世界田径锦标赛
- 反法西斯 70 周年 2015 田径锦标赛-技术支持单位
- 等保办公室感谢信 2014

- 信息化办公室感谢信 2008
- ……

七、工程中心资质

- 网络安全等级测评与检测评估机构服务认证证书
- 信息安全服务资质证书-安全工程类二级
- 信息安全应急处理二级服务资质
- 中国合格评定国家认可委员会 CNAS 检验机构认可证书
- 中国合格评定国家认可委员会 CNAS 检测实验室认可证书
- 质量管理体系认证证书（ISO 9001）
- 信息安全管理体系认证证书（ISO/IEC27001）
- IT 服务管理体系认证证书（ISO/IEC20000-1）
- 环境管理体系认证证书（ISO 14001）
- 业务连续性管理体系证书（ISO 22301）
- 职业健康安全管理体系认证证书（ISO 45001）
- 企业信用评级证书（AAA）
- 信息系统工程监理服务标准贯标证书-丙级单位
- ……

2.3. 合同条款偏离表

序号	合同条目号	招标文件要求合同条款	投标文件响应	说明
/	/	/	所有合同条款及格式均满足，无偏离	

注：1．本表所列内容应符合招标文件第二章“投标人须知”第 11.2 款和第 14.3.5 款规定。

2．投标人应对招标文件第四章“合同条款及格式”所提出各项要求进行逐条逐项答复、说明和解释，首先对实现或满足程度明确作出“满足”、“不满足”、“部分满足”等应答，然后作出具体、详细的说明。**回答“部分满足”应说明哪部分满足或哪部分不满足，不得使用“明白”、“理解”等词语。**在答复中，要求明确满足的程度，凡采用“详见”、“参见”方式说明的，应指明参见文档的具体章节或页码。**如果所有条款无偏离，则无需逐条应答，可在表内填写“所有合同条款及格式均满足或优于招标文件要求，无偏离”。**

3．以上表格仅供参考，投标人可以根据情况自行编制偏离文件。

2.4. 类似项目一览表

序号	项目名称	合同对方主体全称	合同时间		投资额	合同金额	证明人及电话	备注
			签订时间	实施周期				
1	2023 年第三方网络安全服务采购项目	中国人民银行征信中心	2023. 11	2025. 5. 31	30 万元	30 万元	赵伟臣 021-20679443	
2	诚通财务 2024 年度信息系统等级保护测评服务项目	诚通财务有限责任公司	2024. 11	2025. 11	24. 3 万元	24. 3 万元	010-83278134	
3	2024 年等级保护测评服务项目	中银三星人寿保险有限公司	2024. 7	2025. 7	31. 6039 万元	31. 6039 万元	刘佳锐 13321189972	
4	金谷信托网络安全等级保护定级备案、测评服务项目	中国金谷国际信托有限责任公司	2024. 9	/	31. 9 万元	31. 9 万元	010-88088276	
5	综合信息系统安全等级保护测评合同	北京住房公积金管理中心	2024. 7	/	34 万元	34 万元	宁老师 010-82486161	
6	网络安全等级保护测评服务合同	中邮人寿保险股份有限公司	2023. 7	/	90 万元	90 万元	于老师 010-6885-6880	

2.4.1. 中国人民银行征信中心2023年第三方网络安全服务采购项目

中国人民银行征信中心2023年第三方网络安全服务采购项目合同

合同编号：ZXZX-2023-0200****

甲方：中国人民银行征信中心

乙方：中科信息安全共性技术国家工程研究中心有限公司

二〇二三 年 十一 月

签订地点：上海

甲　　方：中国人民银行征信中心
法定代表人：陈建华
地址：上海市浦东新区繁昌路 298 号
邮政编码：201201
联系人：赵伟臣
联系电话：021-20679443
传真号码：021-20675438
开户银行：中信银行上海分行营业部
银行账号：8110201013601575758

乙　　方：中科信息安全共性技术国家工程研究中心有限公司
法定代表人：潘毅
地址：北京市海淀区中关村大街 19 号新中关大厦 B 座北翼 16 层
邮政编码：100080
联系人：高朋朋
联系电话：010-82486161
传真号码：010-82486161
开户银行：平安银行北京知春路支行
银行账号：11006992932301

甲乙双方依据“中国人民银行征信中心2023年第三方网络安全服务采购项目二次采购”（项目编号：JS2023007）项目采购的结果，本着自愿、平等、互利、诚实信用的原则，通过友好协商，现授权各自代表按照下述条款签署本合同。

1、合同的组成

1.1下述文件是构成本合同不可分割的部分：

（1）本合同条款及其所有附件；

（2）甲方的谈判文件及澄清文件；

（3）乙方的响应文件及质疑解答文件；

（4）成交通知书；

（5）法定代表人授权书；

（6）双方与合同有关的往来信函、传真，经双方法定代表人或其授权代表签字并加盖单位公章确认后，视为本合同的组成部分；

（7）经双方法定代表人或其授权代表签字并加盖单位公章或合同专用章确认的补充协议。

1.2 如果乙方的响应文件及质疑解答文件内容违背或低于甲方谈判文件要求或任何可能导致影响当次采购目的的情形，均应当被视为乙方自动放弃响应文件及质疑解答文件中相应部分而同意以谈判文件相应内容为准。如果乙方的响应文件及质疑解答文件内容高于甲方谈判文件要求，则以乙方的响应文件及质疑解答文件内容为准。如果合同条款与合同附件有矛盾之处，以合同条款内容为准。如果合同附件之间有矛盾之处，以有利于甲方的附件内容为准。

1.3 上述合同文件应能够相互解释、相互说明。如合同文件之间出现不一致，除本合同另有约定外，第1.1款第（1）项至（6）项的排列顺序就是合同文件的优先解释顺序；对于第（7）项中双方达成的补充协议与原合同（包括第1.1款（1）-（6）项中所列的所有文件）存在不一致，以签订日期在后的补充协议为准。

2、服务时间、地点和内容

2.1 项目服务实施时间：

项目服务实施地点：中国人民银行征信中心上海、天津和北京各数据及灾备中心，具体以甲方指定地点为准。

2.2、项目服务内容

2.2.1 乙方为甲方提供第三方网络安全服务。

2.2.2 乙方保证为甲方提供优质的第三方网络安全服务，服务的各方式和标准项均能符合本合同规定的要求。服务期内，乙方保证提供甲方在《业务需求及技术规范》（附件三）中要求的全部服务，甲方下发《项目任务表》（附件六）按需采购。

2.2.3 第三方网络安全服务期限：自合同签订起两年。

3、各方的责任和义务

3.1 甲方向乙方提供第三方网络安全服务所需的有关资料，并就乙方开展工作提供力所能及的协助，特别是甲方应在适当时候指定一名总代表以便能随时予以联系。

3.2 甲方应尽合理努力协助乙方向有关机构取得工作许可和乙方要求的其它文件，以使乙方能进入相关现场开展本合同项下的工作，但所有费用由乙方独自负担。

3.3 乙方应提供足够数量的称职的专业人员来履行本合同规定的义务。乙方应对其所雇用的履行合同的专业人员负完全责任，并使甲方免受其专业人员因执行合同任务所引起的一切损害。服务项目实施期间，未经甲方书面认可，乙方不得变更项目服务人员。但在发生不可预测事件或不可抗力而导致必须更换人员的情况时，例如项目服务人员患病、离职或死亡，乙方有权更换与被更换人员技能、资历相当的人员，但应事先通知甲方、取得甲方书面同意并通过甲方面试。

3.4 乙方在提供服务期间，如果对甲方运行正常的硬件、软件或其他财产造成损坏或损害，乙方应负责对其及时修复及更换，并确保甲方正常使用上述硬件、软件或有关财产，以避免甲方的经营活动遭受任何不利影响。

3.5 乙方人员在甲方现场工作期间，应严格遵守甲方的有关规章管理制度。

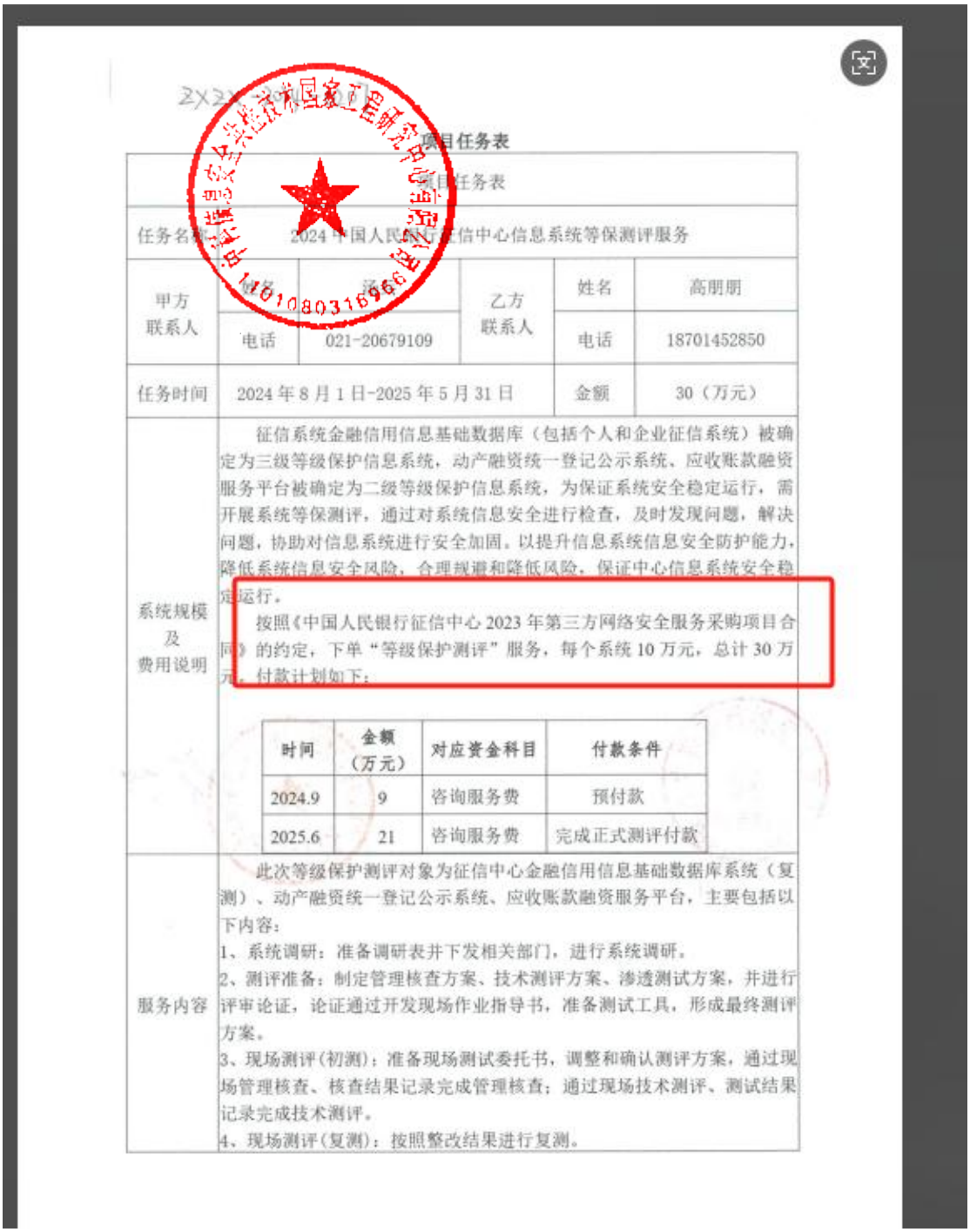
3.6 附件三对第三方网络安全服务另有规定的，乙方应当严格遵守。

3.7 甲方有权督促乙方依据合同约定履行义务。

4、验收

4.1 乙方完成阶段性工作后应当按照附件三的规定向甲方交付工作成果。

4.2 乙方应当在完成服务项目任务后，向甲方提交验收评估表。甲方应当在



项目任务表

项目任务表					
任务名称	2024 中国人民银行征信中心信息系统等保测评服务				
甲方联系人	姓名	张	乙方联系人	姓名	高朋朋
	电话	021-20679109		电话	18701452850
任务时间	2024 年 8 月 1 日-2025 年 5 月 31 日			金额	30（万元）
系统规模及费用说明	征信系统金融信用信息基础数据库（包括个人和企业征信系统）被确定为三级等级保护信息系统，动产融资统一登记公示系统、应收账款融资服务平台被确定为二级等级保护信息系统，为保证系统安全稳定运行，需开展系统等保测评，通过对系统信息安全进行检查，及时发现问题，解决问题，协助对信息系统进行安全加固。以提升信息系统信息安全防护能力，降低系统信息安全风险，合理规避和降低风险，保证中心信息系统安全稳定运行。 按照《中国人民银行征信中心 2023 年第三方网络安全服务采购项目合同》的约定，下单“等级保护测评”服务，每个系统 10 万元，总计 30 万元，付款计划如下：				
服务内容	此次等级保护测评对象为征信中心金融信用信息基础数据库系统（复测）、动产融资统一登记公示系统、应收账款融资服务平台，主要包括以下内容： 1、系统调研：准备调研表并下发相关部门，进行系统调研。 2、测评准备：制定管理核查方案、技术测评方案、渗透测试方案，并进行评审论证，论证通过开发现场作业指导书，准备测试工具，形成最终测评方案。 3、现场测评(初测)：准备现场测试委托书，调整和确认测评方案，通过现场管理核查、核查结果记录完成管理核查；通过现场技术测评、测试结果记录完成技术测评。 4、现场测评(复测)：按照整改结果进行复测。				

时间	金额（万元）	对应资金科目	付款条件
2024.9	9	咨询服务费	预付款
2025.6	21	咨询服务费	完成正式测评付款

	5、出具报告：依据测评结果，出具等级测评报告。 报告包括：征信系统金融信用信息基础数据库（个人和企业征信系统）、动产融资统一登记公示系统、应收账款融资服务平台等保预测评问题列表、系统等级保护测评报告。
参与人员	甲方：王法嘿、汤飞
	乙方：闫伟、李伟、刘少波、王静、杨彩月、史清真、钟智勇、俞婷、乔中辉

项目任务表说明：本项目任务表为中国人民银行征信中心与中科信息安全共性技术国家工程研究中心有限公司签署的第三方网络安全服务项目合同附件，用作明确任务及付款时间依据。

甲方部门负责人签字：

甲方盖章：

日期：2024 年 7 月 31 日

乙方部门负责人签字：

乙方盖章：

日期：2024 年 7 月 31 日

注：本项目任务表一式四份，双方各持两份。

（本页为《中国人民银行征信中心2023年第三方网络安全服务采购项目合同》签署页，无正文）

甲方：中国人民银行征信中心

单位盖章：

代表签字：

日期：2023.11.16

乙方：中科信息安全共性技术国家工程研究中心有限公司

单位盖章：

代表签字：

日期：2023.11.16

2.4.2. 诚通财务等保测评服务项目

合同登记编号：

技 术 服 务 合 同

项目名称：诚通财务 2024 年度信息系统等级保护测评服务项目

委 托 人：

（甲 方） 诚通财务有限责任公司

受 托 人：

（乙 方）中科信息安全共性技术国家工程研究中心有限公司

签订地点： 北京 市 海淀 区

签订日期： 2024 年 11 月 5 日

合同有效期： 2024 年 11 月 5 日至 2025 年 11 月 4 日

技术服务合同

甲　　方：诚通财务有限责任公司

地　　址：北京市海淀区中关村南大街丙 12 号院 2 号楼 6 层

邮政编码：100081

联系电话：010-83278134

传真号码：010-83278122

乙　　方：中科信息安全共性技术国家工程研究中心有限公司

地　　址：北京市海淀区中关村大街 19 号新中关大厦 B 座北翼 16 层

邮政编码：100080

联系电话：010-82486161

传真号码：010-82486355

依据《中华人民共和国民法典》的规定，合同双方就 诚通财务 2024 年度信息系统等级保护测评服务项目 相关事宜，经协商一致，签订本合同。

一、服务对象、服务内容和要求

1、甲方委托乙方对 诚通财务有限责任公司 的 以下 信息系统开展等级保护测评 服务：

系统级别	系统数量	系统名称	备注
三级	1	资金管理新系统	1、系统名称以备案证明上的系统名称为准； 2、司库信息系统备案单位为中国诚通控股集团有限公司。
三级	1	财企通服务平台	
三级	1	司库信息系统	

2、乙方派遣技术服务团队，对甲乙双方确定的服务内容，提供相关的技术

服务，具体服务内容及要求见附件一；

3. 乙方接受甲方委托所完成的工作成果遵循客观、科学、公平、公正原则，符合本合同相关约定及国家或行业相关标准。

二、项目实施计划

乙方于 T+60 个工作日内完成本合同委托的信息系统等级保护测评服务交付物提交工作（不含甲方整改时间）。

说明：T 为甲方提供被测信息系统备案证明（电子版）后与乙方协商一致确定的现场测评开始时间。

三、甲乙双方权利、义务

（一）甲方的权利和义务

1. 接受乙方提交的符合本合同约定条件的服务及服务成果或相关文件，并按约定完成审核、确认；

2. 若乙方针对本合同项目向甲方提交相关工作方案和配套计划或其他相关文件，甲方应自接收之日起五日内组织人员并完成审定、确认，因甲方迟延审定、确认，项目工作期限相应顺延；

3. 检查监督乙方完成委托项目工作的进度，但不得妨碍乙方正常工作；

4. 对乙方提交的委托项目工作成果的质量按照本合同约定及时进行评审和验收；

5. 为保证乙方工作顺利进行，甲方须及时按照乙方要求向乙方提供完成委托事项所必须的项目背景相关资料、相关技术资料和工作条件，并积极协调各方面关系，配合乙方工作；

6. 甲方安排专人负责委托项目所涉及的、与甲方有关的外部联系和协调工作。负责人：王志刚，电话/手机：010-83278134，电子邮箱：wangzhigang@cctfn.cn。负责人职责范围包括但不仅限于：1）协调双方人员正常开展本合同项目；2）作为双方代表交接双方因项目产生的各种文件；3）协调各自资源和力量有效配合项目进展；4）为乙方提供相应工作条件与便利；5）其他需要协调、安排的事项；

甲方变更项目负责人的，应当提前五日书面通知乙方，否则，甲方应当承担

因此产生的相关责任；

7. 按照本合同约定支付乙方费用；

8. 根据本合同委托项目实施或约定其他需要甲方履行的义务。

（二）乙方的权利和义务

1. 乙方为甲方提供双方约定范围内的技术服务；

2. 甲方应根据本合同项目提供正确、完整的技术资料、数据；乙方发现甲方提供的技术资料、数据有明显错误和缺陷或不足以使乙方完成委托项目的，有权通知甲方在合理期限内进行补充、修改；甲方逾期未按照乙方要求补充、修改的，乙方有权中止委托项目，待甲方补充、修改后继续进行，项目实施期限相应顺延；

3. 乙方依本合同的约定在本合同期限内向甲方提供专业的咨询服务，并在规定的委托项目工作期限内完成委托项目的工作；但因甲方责任导致乙方完成委托项目延误的，乙方对此不承担责任，项目实施期限相应顺延；

4. 乙方应遵守国家法律、法规和行业行为准则为甲方完成委托项目的工作；乙方提交的工作成果必须达到合同约定的要求，并对其完成的委托项目工作成果的真实性和准确性全面负责；

5. 乙方应认真按照合同要求完成委托项目工作，随时接受甲方的检查监督，并为检查监督提供便利条件；

6. 乙方在履行合同期间使用的由甲方提供或支付费用的设备设施，属于甲方的财产，乙方在完成委托项目并向甲方提交工作成果时，应将设备设施归还给甲方；

7. 乙方安排专人负责委托项目所涉及的、与乙方有关的外部联系和协调工作。负责人：常广祥，电话/手机：010-82486161，电子邮箱：changgx@nercis.ac.cn。负责人职责范围包括但不仅限于：1）协调双方项目组人员正常开展本合同项目；2）作为双方代表交接双方因项目产生的各种文件；3）协调各自资源和力量有效配合项目进展；4）其他需要协调、安排的事项。

乙方变更项目负责人的，应当提前五日书面通知甲方，否则，乙方应当承担因此产生的相关责任；

8. 乙方有权按约定要求甲方支付项目费用。

四、履行期限、地点和方式

履行期限：与条款二项目实施计划中实施周期一致。

履行地点：甲方指定地点。

履行方式：乙方根据本合同要求进行实施，在合同期内安排专人负责项目的实施与运作协调、管理。

五、验收标准和方式

（一）乙方向甲方提交委托项目工作成果后，甲方指定地点对乙方提交的工作成果进行评价和验收，甲方指定的验收地点为：甲方指定地点 。

（二）乙方按照本合同相关之约定向甲方交付委托项目工作成果后，甲方应当自乙方交付工作成果之日起 5 日内对工作成果根据本合同相关约定进行验收，并签署书面验收报告；甲方逾期未签署书面验收报告也未提出书面异议的，视乙方交付的工作成果验收合格且符合本合同约定及甲方的要求，甲方应当按照本合同约定支付委托报酬。

（三）乙方项目负责人有权对工作情况做出必要说明，甲方应当就验收结果向乙方出具书面报告并说明理由；乙方有权在甲方验收过程中对验收结果申述意见，甲方应根据乙方申述意见作出验收结论或在申述合理的情况下修改结论。

（四）如乙方提交的工作成果未通过甲方的验收，乙方应在甲方规定的合理期限内根据甲方在本合同约定范围内提出的合理意见进行修改并承担修改费用，并按照本合同约定重新申请进行验收。

（五）乙方提交的委托项目工作成果通过验收后，甲方向乙方出具的书面验收报告作为委托项目工作成果验收合格的依据，甲方逾期未出具验收报告的除外。

六、费用支付方式

（一）本合同项目总委托报酬：￥ 243,000.00 元，人民币(大写)： 贰拾肆万叁仟元整。甲方变更服务内容、事项或因甲方其他原因导致乙方服务内容、工作总量的增加，甲乙双方另行协商签订补充协议约定服务报酬。

（二）支付方式：

1. 甲方自本合同签署之日起 10 日内，向乙方支付本合同委托报酬 50%的首付款（即人民币 121,500.00 元，大写：壹拾贰万壹仟伍佰元整）；乙方在完成本次等级保护测评工作后，向甲方提交《等级保护测评报告》，经甲方验收合格后 10 日内向乙方支付委托报酬 50%的尾款（即人民币 121,500.00 元，大写：壹拾贰万壹仟伍佰元整）。

甲方可以支票或汇票或双方认可的其他形式向乙方支付委托服务报酬。若甲方要求乙方进场实施的时间早于本合同约定的付款时间，则甲方付款时间为甲方要求乙方进场前的最后一个工作日。甲方未支付委托报酬或者未提供被测信息系统备案证明（电子版）的，乙方有权拒绝进场实施，且工期顺延。

2. 乙方应在每次收到甲方的委托服务报酬款项后向甲方开具增值税发票。

七、名词和术语约束

（一）“技术资料”指与本项目有关的任何信息、数据、磁盘、软件、光盘、电子邮件、传真、信函、文件、图纸、表格、影像资料及其他形式的资料。

（二）“保密信息”指双方签订的本合同及所有附件和补充协议，所有软件、软件目录、文件、信息、数据、图纸、基准测试、技术规格、商业秘密，所有财务数据、资产状况，以及其他由甲、乙各自专有的、且提供给对方并明确标有“保密信息”字样的信息，包括由甲、乙方于本合同之前或之后签订的其他合同中规定为“保密信息”的所有项目。

八、保密义务

（一）乙方对其在履行合同过程中所知悉的甲方项目技术秘密和商业秘密承担保密义务。

（二）甲乙双方及其工作人员在履行本合同过程中，对因合同签署及履行接触对方并了解到的对方的无法自公开渠道获得的经营信息、技术信息、财务信息、公司计划及其他商业秘密或依法认定为秘密的内容负有保密的责任和义务。未经一方书面同意，另一方不得向第三方泄露上述秘密的全部或部分内容，但法律法规另有规定或双方另有约定的除外。

（三）当事人双方就其他保密条款未进行约定或约定不明确的，按相关法律规定执行，合同双方当事人亦应履行法定的保密义务，否则，将承担法律责任。

无论合同是否被撤销、变更、解除或终止，无论合同是否有效，合同之保密条款在保密期限内不受其限制而继续有效。本合同项下约定的保密期限为合同签订之日起至关于该项目的技术秘密和商业秘密公开时止。

九、知识产权

（一）在本合同有效期内，乙方向甲方交付的工作成果等知识产权及相关文档、资料，归__甲__方所有；未经甲方书面许可，乙方不得以任何方式向第三方披露、转让和许可或用于其它商业活动。在本合同签订前已经存在的成果，包括但不限于设计方案图纸、各种说明书、计算机软件、技术诀窍以及其他技术文档，知识产权归属原权利人所有。

（二）乙方保证委托项目成果不会受到任何第三方基于侵犯其专利权、商标权、著作权、商业秘密等的指控和诉讼。如果甲方收到上述指控和诉讼，乙方应当配合甲方积极应诉，并承担因此给甲方造成的损失。

（三）在不违反保密义务的情况下，乙方可以将本项目的工作成果列入个人或公司案例进行宣传，乙方无需事先经甲方同意。

（四）甲方未将委托报酬全部支付给乙方之前，不享有对本合同约定工作成果的任何知识产权。

十、违约责任

（一）甲方有下列情形之一的，应承担违约责任

1. 因甲方责任造成委托项目工作需要进行重大修改，双方根据重大修改的工作量另行协商确定服务报酬，若需要返工重做的，甲方应当按照双方协商确定的收费标准另行支付服务报酬。

2. 如甲方违反合同约定，延期支付委托报酬的，每延期一日，甲方应当每日按照应付报酬总额的_0.05_%向乙方支付违约金，并且乙方有权中止本合同委托项目或拒绝提交工作成果直至甲方支付应付款及违约金，因此产生的责任及期限延误由甲方承担；逾期超过_30__日仍未支付委托报酬的，乙方有权单方面解除合同并要求甲方承担不低于合同总额30%的违约金，本条约定的违约金不足以弥补乙方损失的，甲方还应补足相应的差额。

3. 如因甲方原因造成乙方完成本合同委托项目日期延误的，每延期一日，甲

方应当向乙方支付本合同约定的全部委托报酬的 0.05 %的违约金；造成乙方或第三人其他损失的，应承担赔偿责任。因甲方无法及时配合乙方工作导致乙方中止履行项目工作累积达到 30 日的，乙方有权解除本合同，甲方已经支付的费用不予退还，未支付的，乙方有权要求甲方按照乙方已经完成的实际工作量支付，同时，乙方有权要求甲方支付本合同总金额 30%的违约金。

（二）乙方有下列情形之一的，应承担违约责任：

1. 乙方因自身责任未按合同规定的日期提交委托项目工作成果的，每延期一日，乙方应每日按照本合同约定的全部委托报酬的 0.05 %向甲方支付违约金。

（三）因甲方过错或违约造成乙方发起解除合同的，甲方应向乙方支付全部合同报酬；因乙方过错或违约造成甲方发起解除合同的，乙方应返还甲方已支付的报酬。

十一、争议解决方法

在合同履行过程中发生争议，双方可协商解决。当事人不愿协商或协商不成的，选择按下列第 2 种方式解决：

1. 提交北京仲裁委员会仲裁解决，仲裁裁决为终局裁决；
2. 依法向被告方住所地人民法院起诉解决。

十二、不可抗力

（一）签约双方中的任何一方由于不可抗力如：地震、水灾、台风、战争和其它双方都认为的不可抗力原因而无法按期履行合同，则合同执行时间由于上述事件的发生作相应延期。在不可抗力事件发生 14 天内，受阻方应尽快用传真或电传通知对方，同时受阻方应尽快用传真和挂号信将有关当局出具的证明文件提交另一方确认。关于不可抗力形势的解除，受阻方应用传真和挂号信通知对方并加以确认。

（二）如果不可抗力阻碍合同的履行超过 180 天，双方就合同的进一步履行问题进行讨论并达成一致意见。

十三、通知、送达

依据本合同所产生的所有通知、声明或其他文件（包括电子邮件、电报、电传、传真、信件、电话）以到达接收方之正常营业日起生效。除非另有书面说明，上述文件应送达至本合同写明的甲乙双方或负责人联系地址或其他接收地址，方为有效。当一方的有关基本信息发生变化（如地址、帐号、法定代表人等），可能对双方的合作或送达产生影响时，应将变化信息立即书面通知另一方，未及时通知的，未通知方承担因此引起的相关责任，本合同写明的联系地址或接收地址或负责人仍有效。

十四、其它

（一）本合同未尽事宜，经双方协商一致，可签订书面补充协议，补充协议与本合同具有同等法律效力。对本合同的任何修改、变更仅得以经双方有权代表签字并加盖公章生效后的书面补充协议进行，否则此合同不得修改、变更。

（二）本合同自双方法定代表人或委托代理人签字并盖章之日起生效。

（三）本合同书及附件一式__肆__份，甲、乙方各执__贰__份，具有同等法律效力。

（四）本合同书附件是本合同不可分割之组成部分，具有同等法律效力。

本合同附件包括：

附件一：__服务内容及要求__

附件一

一、服务内容及要求

等级保护测评服务：诚通财务-资金管理新系统（三级）、诚通财务-财企通服务平台（二级）、诚通集团-词库信息系统（三级）

服务名称	服务内容	内容描述	交付物（每个系统）
等级保护测评服务	差距分析	根据信息系统定级结果，依据《网络安全等级保护基本要求》GB_T 22239-2019，对信息系统的各项安全指标进行前期符合性评估，标识信息系统不符合项，明确信息系统与对应等级保护基本要求之间的差距。	《信息系统差距分析报告》纸质版一式 3 份
	整改加固建议	根据信息系统的差距分析报告结果或信息系统存在的风险点，提出整改加固建议。	《信息系统整改方案》纸质版一式 3 份
	等级测评	依据《网络安全等级保护基本要求》GB_T 22239-2019，对信息系统从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全人员管理、安全建设管理、安全运维管理等 10 个层面对信息系统进行最终等级测评，从单项测评、单元测评、整体测评进行安全问题风险分析，形成最终测评结论，完成测评报告。	《信息系统等级保护测评报告》纸质版一式 3 份

（本页以下为签章页，无正文）

委托人（甲方）	名称(或姓名)	诚通财务有限责任公司 （签 章）			单位公章
	联系(经办)人	（签 章）			
	住 所 (通讯地址)	北京市海淀区中关村南大街丙12号院2号楼6层	邮政编码	100081	
	电话	010-83278134	传真	010-83278122	2022年11月5日
	开户银行	中国农业银行股份有限公司北京西城支行营业部			
	帐号	11021401046668880			
受托人（乙方）	名称(或姓名)	中科信息安全共性技术国家工程研究中心有限公司 （签 章）			单位公章
	联系(经办)人	常广祥 （签 章）			
	住 所 (通讯地址)	北京市海淀区中关村大街19号新中关大厦B座北翼16层	邮政编码	100080	
	电话	010-82486161	传真	010-82486355	2022年11月5日
	开户银行	平安银行北京知春路支行			
	帐号	11006992932301			

2.4.3. 中银三星人寿保险有限公司2024年等级保护测评服务项目

XS-2024-00313

2024年等级保护测评服务项目合同

项目名称：2024 年等级保护测评服务项目

委托方（以下简称甲方）：中银三星人寿保险有限公司

项目联系人：刘佳锐

联系方式：13321189972

受托方（以下简称乙方）：中科信息安全共性技术国家工程研究中心有限公司

项目联系人：李志敏

联系方式：13522418013

签订日期：2024年7月17日

合同有效期：2024年7月17日 - 2025年7月16日

委托协议书

委托单位：中银三星人寿保险有限公司（以下简称甲方）

承接单位：中科信息安全共性技术国家工程研究中心有限公司（以下简称乙方）

根据《中国人民共和国民法典》及有关规定，经双方协商，甲方委托乙方开展网络安全等级保护测评服务工作，签订本合同，共同履行。

一、甲方委托的项目

1、项目名称： 2024 年等级保护测评服务项目

2、项目内容：甲方委托乙方针对中银三星人寿保险有限公司 3 个等保三级系统进行复测，对 1 个未定级系统（银保通）进行等级保护专家评审定级、公安备案及等保测评工作。

系统级别	系统数量	系统名称	备注
三级	3	核心系统	系统名称以备案证明上的系统名称为准
		私有云平台	
		业务销售系统	
二级	1	银保通	

3、项目完成期限：

1）本协议项下乙方应当在甲方提供被测信息系统备案证明（电子版）且与乙方协商一致，确定现场测评开始时间后的 60 个工作日内完成全部测评工作（不含甲方整改时间）。

2）在本合同履行过程中发生的争议以及其他与本合同有关的一切争议，双方应当友好协商解决。

二、项目内容确定及成果的提交

2、由甲乙双方共同协商，确定本项目实施进度。

3、乙方应当在人员入场后 60 个工作日内完成全部测评工作（不含甲方整改时间），并向甲方提交经甲方认可的《网络安全等级保护测评报告》。

三、数据及相关资料的保密

本合同所确定的服务内容或测评报告仅限甲方及甲方的关联方使用。未经甲方书面许可，乙方不得将测评报告向任何第三方提供，不得上网对外发布。

四、项目费用及支付方法

1、合同金额：本合同费用含税价共计人民币：¥316039.00 元（大写：人民币叁拾壹万陆仟零叁拾玖元整）。增值税税率 6%，增值税税款金额人民币：¥18962.34 元。

2、付款措施：

全部测评工作完成后，乙方向甲方提交本合同附件一中的等级保护测评服务内约定的各项报告并经甲方确认后，且双方均在中银三星人寿项目验收报告（附件三）签字盖章后，甲方在收到乙方提供的合规等额增值税专用发票后 20 个工作日内，向乙方一次性支付 100%的合同费用。

3、乙方在甲方支付款项前应当先向甲方提供合同各个阶段对应金额的正规增值税专用发票，发票内容是：技术服务费。

4、甲乙双方账户信息如下：

甲方账户信息： 开户名称：中银三星人寿保险有限公司 开户银行：中国银行股份有限公司北京中银大厦支行 开户账号：346759372671 纳税人识别号：911100006349328035 地址及电话：北京市朝阳区霄云路 40 号院 1 号楼国航世纪大厦 20 层 07、08、09 单元，22 层、23 层 010-83262688	乙方账户信息： 开户名称：中科信息安全共性技术国家工程研究中心有限公司 开户银行：平安银行北京知春路支行 开户账号：11006992932301 纳税人识别号：91110108791603851A 地址及电话：北京市海淀区中关村大街 19 号 16 层 010-82486161

五、双方责任

甲方责任：

1、甲方负责确定评测目标系统及提供评测所需资料及技术评测环境。

2、按约定时间和金额，支付给乙方费用。

3、甲方应按合同约定支付乙方价款，如因甲方自身原因，未能按时支付，则每逾期1日，甲方将按照应付未付金额的万分之五向乙方支付违约金。超过30日的，乙方有权利解除合同，甲方逾期付款期间，乙方有权暂停提供服务且不构成违约。

4、甲方应在乙方提交本合同约定的工作成果后5日内组织验收并向乙方出具书面的验收报告，否则视为乙方提交的工作成果验收合格。甲方指定的工作成果接收和验收人信息如下：姓名【刘 佳 锐】、联系电话【010-83260757】、电子邮箱【zysxrsliujr_hq@bank-of-china.com】。

乙方责任：

1、乙方保证其具有履行本合同约定项目的相关资质。

2、乙方所提供的服务人员都必须为乙方正式雇员且乙方的劳动合同期限必须长于服务时间。

3、乙方在服务过程中需使用合法软、硬件产品。

4、乙方应确保加强所提供驻场人员管理，确保所有人员符合甲方已事先书面或者邮件告知的人员及网络信息安全的相关制度要求。

5、如期向甲方交付本合同规定的成果文件，并保证文件质量符合验收要求，如不符合验收要求，未通过甲方的验收，乙方应在甲方规定的合理期限内根据甲方在本合同约定范围内提出的合理意见进行修改并承担修改费用，并按照本合同约定重新申请进行验收。如修改的成果文件仍未通过甲方的验收，乙方应退还不符合要求的部分对应的服务费用，甲方有权拒付尾款，并解除合同。乙方因此给甲方造成经济损失的，应付赔偿责任。

6、乙方应按合同约定期限完成合同项目，实现项目目标，如因乙方自身原因，未能按时交付，则每逾期1日，乙方应按照合同金额的万分之五向甲方支付违约金。超过 30 日的，甲方有权解除合同，同时要求赔偿因此造成的实际损失。（本条约定的违约金总额不超过合同总金额的10%。）

7、按项目说明内容完成所定项目。

六、合同生效与终止

1、本合同经甲乙双方盖章后生效。

2、甲乙双方因故需变更或终止本合同时应提前通知对方，对本合同中的遗留问题取得一致意见，在补充条款中进行说明或签订补充协议。未达成协议前，本合同继续有效。

3、乙方向甲方提供本合同中规定的项目成果文件（附件 1），且甲方按合同规定付清乙方全部费用后，本合同关系终止。本合同另有条款约定的除外。

七、其他条款

1、本合同未尽事宜由甲乙双方协商确定并形成书面协议作为本合同附件执行。

本合同附件包括：

附件一：　服务内容及要求

附件二：　保密协议

附件三：　中银三星人寿 XXXXX 服务采购项目验收报告

2、本合同履行过程中如果发生纠纷，双方应通过协商解决，若协商不成，可向甲方所在地人民法院诉讼解决。

3、测评分为初测和复测，在复测完成后，如被测系统存在高风险问题或评分未达到 70 分的，乙方有权出具结论为“不符合”的测评报告。

4、本合同一式四份，甲方持二份，乙方持二份，具有同等法律效力。

5、本合同所有内容包括名称、合同金额、全部成果以及在合同履行过程中甲方提供给乙方的所有资料和文件，都作为甲方的商业秘密，乙方应承担保密义务。关于乙方保密义务的约定不因本合同终止而失效。（具体约定见附件二《保密协议》）

（以下无正文）

甲方（盖章）：

2024年07月16日

乙方（盖章）：

2024 年 7 月 16 日

附件一：

服务内容及要求

序号	服务名称	服务内容	内容描述	交付物
1	等级保护测评服务	系统定级	对信息系统基本情况进行调研，根据调研结果，确定信息系统等级，编制定级报告，协助客户组织专家对定级结果进行评审。	《信息系统定级报告》 《专家评审意见》 纸质版一式__份
		协助备案	协助用户准备备案材料，协助提交备案材料。	《信息系统备案表》 电子版一式__份
		差距分析	根据信息系统定级结果，依据《网络安全等级保护基本要求》GB_T 22239-2019，对信息系统的各项安全指标进行前期符合性评估，标识信息系统不符合项，明确信息系统与对应等级保护基本要求之间的差距。	《信息系统差距分析列表》 电子版一式__份
		整改加固建议	根据信息系统的差距分析报告结果或信息系统存在的风险点，提出整改加固建议。	《信息系统整改意见》 电子版一式__份
		等级测评	依据《网络安全等级保护基本要求》GB_T 22239-2019，对信息系统从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全人员管理、安全建设管理、安全运维管理等 10 个层面对信息系统进行最终等级测评，从单项测评、单元测评、整体测评进行安全问题风险分析，形成最终测评结论，完成测评报告。	《信息系统等级保护测评报告》 纸质版一式三份
		渗透测试	针对三级系统，在获取用户授权后通过真实模拟黑客使用的工具、分析方法来对网站等信息系统进行模拟攻击，验证当前的安全防护措施，编制渗透测试报告。	
		漏洞扫描	针对二级和三级系统，通过漏洞扫描工具对目标系统进行扫描，扫描结束后形成《漏洞扫描报告》提出安全整改建议。	

2	安全管理制度优化	安全管理制度优化	基于信息系统安全等级，根据信息安全等级保护管理要求，从信息安全管理制度、安全管理机构、安全人员管理、安全建设管理和安全运维管理五个方面对现有信息安全管理制度进行优化和修订，达到国家信息安全等级保护 2.0 管理要求。	《安全管理制度集》一套
3	信息安全意识培训服务	信息安全意识培训服务	面向普通员工和技术人员开展一次网络安全意识和安全形势的安全培训；面向网络安全管理人员及技术人员提供国家《网络安全法》的立法背景、基本框架和重点内容解读，提供《网络安全等级保护条例》主要内容介绍和解读，介绍网络安全现场执法检查重点及违反网络安全法相关处罚案例等。	培训课件及相关材料

附件二：

保密协议

甲方：中银三星人寿保险有限公司

乙方：中科信息安全共性技术国家工程研究中心有限公司

根据中华人民共和国有关法律法规的规定，为了明确甲乙双方的保密义务，经双方协商一致，就甲方委托乙方开展 2024 年等级保护测评服务项目有关工作事宜订立本保密协议。具体内容如下：

第一条 保密内容和范围

1、文档信息

文档包括但不限于甲方提供给乙方或因乙方参与服务而采集和接触到的任何甲方、甲方关联方及其用户的各种文档、信息、资料等；乙方完成项目服务时向甲方提供的各种文档、信息、资料等。

2、技术信息

包括系统相关网络拓扑结构、运维管理策略、访问控制策略、系统漏洞、使用的网络安全技术等。

3、其他信息

双方的机构情况、人员情况、项目情况等；因项目需要告知对方，并要求对方承担保密义务的信息等；依照法律规定和有关承诺的约定要求对方承担保密义务的其他事项。

第二条 乙方保密义务

1、项目负责人按照工作需要建立保守秘密的规章制度，并对项目组成员的岗位职责进行明确分工，对项目组成员开展保密教育培训；

2、项目负责人负责在项目现场工作完成后，将甲方提供的技术资料归还甲方，不私自留存或擅自处理。项目中需要留存的甲方资料，应严格按照有关保

密规定进行管理并妥善保存；

3、项目组成员对接触到的甲方文档资料、信息数据及分析结果，不得擅自以任何形式公开发表、交流或转让；需指定专人进行登记并保管，严格控制知情范围。项目实施过程中的各个阶段,要监督有关人员对涉及项目的资料、文件及复制的电子文档(如 WORD 文档、 EXECL 表格)等进行销毁和删除；

4、项目负责人负责对项目现场的工作情况进行记录并存档备查。进入甲方现场从事项目工作，严格遵守甲方现场工作制度和流程，并在其监督下进行；

5、乙方仅在工作需要时，向有关参与项目的人员提供必要的信息，并采取使知情人员保守秘密的措施，如签订保密承诺书等；乙方未经甲方书面同意，不得向任何单位、任何他人披露甲方秘密。

第三条 甲方保密义务

1、甲方使用乙方的资料仅用于本次项目；

2、甲方保证，对于乙方提供的资料妥善管理且仅在直接相关人员中传阅；

3、对乙方需要保密的信息及资料不得擅自以任何形式公开发表、交流或转让；甲方未经乙方书面同意，不得向任何单位、任何他人披露乙方秘密。

第四条 保密期限

甲、乙双方确认，双方的保密义务自本协议签订时开始，到关于该项目的技术秘密和商业秘密公开时止。

第五条 违约责任

任何一方未履行本协议第二、三条所规定的保密义务或因实施及管理上的疏忽而造成泄密情况给另外一方造成损害的，被损害方有权要求违约方承担全部赔偿责任，并保留追究相应法律责任的权利。

第六条 其他

本协议自双方盖章起生效。本协议的任何修改必须经过双方的书面同意。

本协议未尽事宜由双方协商解决，协商不成，可向甲方所在地人民法院诉讼解决。

（以下无正文）

甲方（盖章）：中银三星人寿保险有限公司

日期：2024.07.16

乙方（盖章）：中科信息安全共性技术国家工程研究中心有限公司

日期：2024.7.16

2.4.4. 金谷信托网络安全等级保护定级备案、测评服务项目

合同登记编号：

技 术 服 务 合 同

项目名称：金谷信托网络安全等级保护定级备案、测评服务项目

委 托 人：

（甲 方）中国金谷国际信托有限责任公司

受 托 人：

（乙 方）中科信息安全共性技术国家工程研究中心有限公司

签订地点： 北京市西城区

签订日期： 2024 年 9 月 20 日

技术服务合同

甲　　方：中国金谷国际信托有限责任公司

地　　址：北京市西城区金融大街 33 号通泰大厦 C 座 10 层

邮　　箱：/

邮政编码：100033

联系电话：010-88086686

传真号码：010-88088276

开 户 行：建行北京金融街支行

银行帐号：11001070800059000416

乙　　方：中科信息安全共性技术国家工程研究中心有限公司

地　　址：北京市海淀区中关村大街 19 号新中关大厦 B 座北翼 16 层

邮　　箱：gaopp@nercis.ac.cn

邮政编码：100080

联系电话：010-82486161

传真号码：010-82486355

开 户 行：平安银行北京知春路支行

银行帐号：　11006992932301

依据《中华人民共和国民法典》的规定，合同双方就 金谷信托网络安全等级保护定级备案、测评服务项目 相关事宜，经协商一致，签订本合同。

一、服务内容及服务实施依据

1、乙方派遣技术服务团队，对甲乙双方确定的服务内容，提供相关的技术服务，详细服务内容及交付物见附件一。

2、乙方接受甲方委托所完成的工作成果遵循客观、科学、公平、公正原则，符合本合同相关约定，并依据以下国家或行业相关标准开展服务：

等级保护测评服务实施依据

GB 17859-1999　计算机信息系统安全等级保护划分准则

GB/T 22240-2020　信息安全技术 网络安全等级保护定级指南

GB/T 22239-2019　信息安全技术 网络安全等级保护基本要求

GB/T 28448-2019　信息安全技术 网络安全等级保护测评要求

GB/T 28449-2018　信息安全技术 网络安全等级保护测评过程指南

GB/T 25070-2019　信息安全技术 网络安全等级保护安全设计技术要求

网络安全等级保护测评高风险判定指引

二、项目实施计划

T+60　工作日内完成本合同委托的服务工作。（不含方案编制、系统建设、定级备案、整改、招投标、设备采购及甲方确认实施方案的时间）。

说明：T 为双方协商确定的入场实施时间。

三、甲乙双方权利、义务

(一) 甲方的权利和义务

1. 接受乙方提交的符合本合同约定条件的服务及服务成果或相关文件，并按约定完成审核、确认；

2. 若乙方针对本合同项目向甲方提交相关工作方案和配套计划或其他相关文件，甲方应自接收之日起五日内组织人员并完成审定、确认，因甲方迟延审定、确认，项目工作期限相应顺延；

3. 检查监督乙方完成委托项目工作的进度，但不得妨碍乙方正常工作；

4. 对乙方提交的委托项目工作成果的质量按照本合同约定及时进行评审和验收；

5. 为保证乙方工作顺利进行，甲方须及时按照乙方要求向乙方提供完成委托事项所必须的项目背景相关资料、相关技术资料和工作条件，并积极协调各方面关系，配合乙方工作；

6. 甲方安排专人负责委托项目所涉及的、与甲方有关的外部联系和协调工

作为负责人：董鑫，电话/手机：010-88088399，电子邮箱：dongxin@jingutrust.com。负责人职责范围包括但不仅限于：1）协调双方人员正常开展本合同项目；2）作为双方代表交接双方因项目产生的各种文件；3）协调各自资源和力量有效配合项目进展；4）为乙方提供相应工作条件与便利；5）其他需要协调、安排的事项；

甲方变更项目负责人的，应当提前五日书面通知乙方，否则，甲方应当承担因此产生的相关责任；

7. 按照本合同约定支付乙方费用；

8. 根据本合同委托项目实施或约定其他需要甲方履行的义务。

（二）乙方的权利和义务

1. 乙方为甲方提供双方约定范围内的技术服务；

2. 甲方应根据本合同项目提供正确、完整的技术资料、数据；乙方发现甲方提供的技术资料、数据有明显错误和缺陷或不足以使乙方完成委托项目的，有权通知甲方在合理期限内进行补充、修改；甲方逾期未按照乙方要求补充、修改的，乙方有权中止委托项目，待甲方补充、修改后继续进行，项目实施期限相应顺延；

3. 乙方在规定的委托项目工作期限内完成委托项目的工作；但因甲方责任导致乙方完成委托项目延误的，乙方对此不承担责任，项目实施期限相应顺延；

4. 乙方应遵守国家法律、法规和行业行为准则为甲方完成委托项目的工作；乙方提交的工作成果必须达到合同约定的要求，并对其完成的委托项目工作成果的真实性和准确性全面负责；

5. 乙方应认真按照合同要求完成委托项目工作，随时接受甲方的检查监督，并为检查监督提供便利条件；

6. 乙方在履行合同期间使用的由甲方提供或支付费用的设备设施，属于甲方的财产，乙方在完成委托项目并向甲方提交工作成果时，应将设备设施归还给甲方；

7. 乙方安排专人负责委托项目所涉及的、与乙方有关的外部联系和协调工作。负责人：鹿伟，电话/手机：18801016670，电子邮箱：luwei@nercis.ac.cn。负责人职责范围包括但不仅限于：1）协调双方项目组人员正常开展本合同项目；

见，甲方应根据乙方申述意见作出验收结论或在申述合理的情况下修改结论。

（四）如乙方提交的工作成果未通过甲方的验收，乙方应在甲方规定的合理期限内根据用方在本合同约定范围内提出的合理意见进行修改，由乙方承担修改费用，并按照本合同约定重新申请进行验收。

（五）乙方提交的委托项目工作成果通过验收后，甲方向乙方出具的书面验收报告作为委托项目工作成果验收合格的依据，甲方逾期未出具验收报告的除外。

六、费用支付方式

（一）本合同项目总委托报酬：￥ 319000 元，人民币(大写)：叁拾壹万玖仟 圆整。本合同费用金额仅限于提供本合同中列明的服务内容，甲方变更服务内容、事项或因甲方其他原因导致乙方服务内容、工作总量的增加，甲乙双方另行协商签订补充协议约定增加服务报酬。

（二）甲方按照以下方式支付本合同服务报酬：

1、第一次付款：自本合同签署之日起 30 日内，甲方向乙方支付第一笔款，即服务费用合同总额的 50%，即人民币 159500 元整（人民币大写：壹拾伍万玖仟伍佰元整）。 在满足先决条件：签订合同、甲方在收到乙方开具的发票后的 30 日内完成此次付款；乙方需要开具对应金额委托服务费的增值税发票，税率 6%。

2、第二次付款：甲方向乙方支付第二笔款，即合同总额的 50%，即人民币 159500 元整（人民币大写：壹拾伍万玖仟伍佰元整）。在满足先决条件：乙方在完成本次的服务工作后，向甲方提交最终交付物并验收合格、甲方在收到乙方开具的发票后的 30 日内完成此次付款；乙方需要开具对应金额委托服务费的增值税发票，税率 6%

七、名词和术语约束

（一）“技术资料”指与本项目有关的任何信息、数据、磁盘、软件、光盘、电子邮件、传真、信函、文件、图纸、表格、影像资料及其他形式的资料。

（二）“保密信息”指双方签订的本合同及所有附件和补充协议，所有软件、软件目录、文件、信息、数据、图纸、基准测试、技术规格、商业秘密，所有财务数据、资产状况，以及其他由甲、乙各自专有的、且提供给对方并明确标有“保

委托人（甲方）	名称（或姓名）	中国金谷国际信托有限责任公司（签 章）			2024 年 9 月 20 日
	法定代表人	（签 章）			
	住 所 （通讯地址）	北京市西城区金融大街 33 号通泰大厦 C 座 10 层	邮政编码	100033	
	电话	010-88086816	传真	010-88088276	
	开户银行	建行北京金融街支行			
	帐号	11001070800059000416			
受托人（乙方）	名称（或姓名）	中科信息安全共性技术国家工程研究中心有限公司（签 章）			2024 年 9 月 20 日
	法定代表人	（签 章）			
	住 所 （通讯地址）	北京市海淀区中关村大街 19 号新中关大厦 B 座北翼 16 层	邮政编码	100080	
	电话	010-82486161	传真	010-82486355	
	开户银行	平安银行北京知春路支行			
	帐号	11006992932301			

2.4.5. 北京住房公积金管理中心综合信息系统安全等级保护测评合同

北京住房公积金管理中心
Beijing Housing Fund Management Center

北京住房公积金管理中心

综合信息系统安全等级保护测评 合同

项目名称：2024年北京住房公积金管理中心综合信息系统安全等级保护测评服务

合同编号：H2024-68

甲　　方：北京住房公积金管理中心

乙　　方：中科信息安全共性技术国家工程研究中心有限公司

2024 年 7 月

本合同甲方委托乙方就北京住房公积金管理中心 综合信息系统 进行网络安全等级保护测评、商用密码应用安全性评估，并支付相应的技术服务报酬。双方经过平等协商，在真实、充分地表达各自意愿的基础上，根据《中华人民共和国民法典》的规定，达成如下协议，并由双方共同恪守。

一、服务内容及目的

依据有关信息安全管理的政策法规，按照《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）、《信息安全技术网络安全等级保护测评要求》（GB/T28448-2019）、《信息安全技术信息系统密码应用基本要求》（GB/T 39786-2021）等标准的相关条款，乙方对综合信息系统进行网络安全等级保护测评和商用密码应用安全性评估。通过测评，乙方在坚持科学、客观、公正原则的基础上，全面、完整地了解信息安全等级保护要求的基本安全控制在被测信息系统中的实施配置情况以及系统的整体安全性，出具安全等级测评的结论，出具商用密码应用合规性、有效性和正确性的结论；指出该系统存在的安全问题并提出相应的整改建议，并出具测评报告。

二、甲方义务

1．甲方应及时向乙方提供测评范围内所需的资料，包括相关文档、配置及其他资料文件，并保证这些资料的可靠性和真实性。

2．甲方为乙方服务人员协调相关方，并提供测评服务场所。

3．甲方负责对乙方提供的测评记录、服务报告进行确认。

4．甲方应按合同要求的时间和方式支付费用。

三、乙方义务

1．乙方未按双方约定提交符合甲方要求的工作成果，应承担违约责任。

2．因乙方故意或过失导致综合信息系统被破坏、数据丢失，乙方应及时采取补救措施进行系统和数据的恢复，并根据影响程度承担相应的赔偿责任。

（本页为签署页）

甲方	名称	北京住房公积金管理中心		
	法定代表人			
	委托代理人	（签字）		
	联系（经办）人			
	住所（通讯地址）	北京市东城区西革新里 108 号	邮政编码	100077
	电话			
	开户银行			
	账号			
乙方	名称	中科信息安全共性技术国家工程研究中心有限公司		
	法定代表人			
	委托代理人	（签字）		
	联系（经办）人			
	住所（通讯地址）	北京市海淀区中关村大街 19 号 16 层	邮政编码	100080
	电话	010-82486161		
	开户名	中科信息安全共性技术国家工程研究中心有限公司		
	开户银行	平安银行北京知春路支行		
	账号	1100 6992 9323 01		

合同专用章
或
单位公章

2024年7月12日

合同专用章
或
单位公章

2024年7月12日

2.4.6. 中邮人寿保险股份有限公司网络安全等级保护测评服务合同

中邮人寿保险股份有限公司
网络安全等级保护测评服务合同

合同编号：

甲方：中邮人寿保险股份有限公司

乙方：中科信息安全共性技术国家工程研究中心有限公司

甲方：中邮人寿保险股份有限公司

乙方：中国信息安全测评技术国家工程研究中心有限公司

在自愿、平等、互利、诚实信用的基础上，经过合同双方协商，乙方向甲方提供系统测评服务。为明确双方的权利、义务、责任，特此订立本合同，以兹共同遵守。

1. 服务名称、服务内容、项目验收及服务期限

1.1 服务名称

中邮人寿保险股份有限公司 2023 年网络安全等级保护测评。

1.2 服务内容

中邮人寿保险信息系统网络安全等级保护测评服务。

1.2.1 乙方根据甲方的要求，按照信息系统安全等级保护标准和测试规范，完成甲方委托的系统等级保护测评服务。

1.2.2 根据《信息安全技术 信息系统安全等级保护测评要求》，测评内容主要分为安全技术测评和管理要求测评两大部分。其中，安全技术测评包括：物理安全、网络安全、主机系统安全、应用安全和数据安全；管理要求测评包括:安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理。具体测评内容详见附件2。

(1)乙方应在合同生效并接到甲方通知后 15 日历天内完成被测系统的前期调研和测评方案制定。

(2)乙方应在完成前期调研和测评方案制定后并接到甲方通知60日历天内通过访谈、调阅材料（制度、系统设计材料等）、对系统开展现场测评（功能测试、性能测试、渗透测试等）等方式完成等级保护系统现场测评，并出具纸质和电子版《差距分析报告》，提出整改方案。

(3)乙方在甲方完成测评整改工作后25个日历天内开展验收测评。甲方系统通过验收测评后，乙方应在15个日历天出具《信息系统安全等级测评报告》，并配合甲方向公安机关提交《信息系统安全等级测评报告》备案备查。

1.3 项目验收

1.3.1 乙方完成差距分析，向甲方提交《差距分析报告》正本壹份，甲方确认合格后，签字完成验收。

1.3.2 乙方完成验收测评，向甲方提交《信息系统安全等级测评报告》正本一份，并完成向公安机关《信息系统安全等级测评报告》备案后，甲方签字确认完成验收。

1.3.3 《差距分析报告》包括但不限于测评工作概述、测评结果、现有系统存在的问题及整改建议；《等级测评报告》包括但不限于测评工作概述、测评结果等。

1.4 服务期限

本服务期限为 自合同生效之日起至2023年 12 月 31 日止。如在2023年 12 月 31 日存在正在进行且尚未完成的服务任务，服务期限自动延续至乙方完成该任务并经甲方验收合格之日。

2. 合同价款、支付结算及履约保证金

2.1 合同价款

本合同项目总价款：[redacted]整（不含税金额：[redacted]）价款为服务期内被测系统测评费用的总和，税率[redacted]测评费根据测评最终评定的级别和测评系统设备数量确定，测评价格详见附件3报价清单。合同纳税义务发生时若国家增值税税率发生调整，不含税价款不变，增值税和合同含税价款根据国家税率变动相应调整。

2.2 支付结算

2.2.1 支付方式

乙方完成中邮人寿保险股份有限公司受测系统的网络安全等级保护测评， 提交信息系统《**信息系统差距分析报告》、《**信息系统整改意见清单》、《**信息系统网络安全等级测评报告》， 甲方验收签字确认后15工作日内，依据网络安全等级保护测评机构组织的专家评审会最终评定的级别和相应报价（详见报价清单）逐个系统进行结算。

2.2.2 每次付款条件成立后，乙方须按甲方要求向甲方开据以甲方为抬头的符合国家规定和甲方要求的增值税专用发票及相应的付款申请，甲方在收到发票后 30 日内将款项支付到乙方指定账户。

2.2.3 乙方的账户信息：

账户名称：中科信息安全共性技术国家工程研究中心有限公司

开户行：平安银行北京知春路支行

账　号：11006992932301

开户行联行号：307100003109（全国）；944（同城）

纳税人识别号：91110108791603851A

2.2.4 因本合同所产生的所有税费由乙方承担，甲方除本合同所规定的款项外不再支付任何其他费用。

（本页为合同签署页，无正文）

甲方（盖章）：中邮人寿保险股份有限公司

法定代表人（负责人）

或委托代理人：

2023年 7月 31日

乙方（盖章）：中科信息安全共性技术国家工程研究中心有限公司

法定代表人（负责人）

或委托代理人：

2023 年 7 月 31 日

2.5. 其他商务文件

2.5.1. 测评资质

2.5.1.1. 网络安全等级测评与检测评估机构服务认证证书

DJCP

网络安全服务认证证书
等级保护测评服务认证

证书编号: SC202127130010031

兹 证 明:中科信息安全共性技术国家工程研究中心有限公司

统一单位信用代码:91110108791603851A

符合TRIMPS-SC13-001:2021《网络安全等级测评与检测评估机构 服务认证实施规则》的要求。

注册地址: 北京市海淀区中关村大街19号16层B1601、B1602、B1603、B1605

办公地址: 北京市海淀区中关村大街19号新中关大厦B座北翼16层

首次颁证日期: 2021 年 11 月 18 日
发 证 日 期: 2024 年 06 月 11 日
有 效 期 至: 2027 年 11 月 17 日

在一个监督周期内,本证书必须与本机构监督评价合格后签发的证书保持通知书合并使用方可有效。

公安部第三研究所认证 The Third Research Institute Of Ministry Of Public Security Certification

签发人

公安部第三研究所

地址:上海市徐汇区岳阳路76号 电话:021-64318599 证书有效性查询:http://www.trimps.net.cn S2024000030

2.5.1.2. 国家密码管理局颁发得商用密码检测机构资质证书

商用密码检测机构资质证书

机构名称：中科信息安全共性技术国家工程研究中心有限公司

统一社会信用代码：91110108791603851A

注册地址：北京市海淀区中关村大街19号16层B1601、B1602、B1603、B1605

证书编号：GM-P-000024

有效期至：2029年11月10日

业务范围：

商用密码应用安全性评估

国家密码管理局

2024年11月11日

2.5.1.3. CNAS 检验机构认可证书

中国合格评定国家认可委员会

检验机构认可证书

（注册号：CNAS IB0300）

兹证明：

中科信息安全共性技术国家工程研究中心有限公司

（法人：中科信息安全共性技术国家工程研究中心有限公司）

北京市海淀区中关村大街 19 号新中关大厦 B 座北翼 16 层，

100080

符合 ISO/IEC 17020:2012《各类检验机构运行的基本准则》（CNAS-CI01《检验机构能力认可准则》）C 类的要求，具备承担本证书附件所列检验服务的能力，予以认可。

获认可的能力范围见标有相同认可注册号的证书附件，证书附件是本证书组成部分。

生效日期：2024-05-05

截止日期：2030-05-04

中国合格评定国家认可委员会授权人 张朝华

中国合格评定国家认可委员会（CNAS）经国家认证认可监督管理委员会（CNCA）授权，负责实施合格评定国家认可制度。
CNAS是国际实验室认可合作组织（ILAC）和亚太认可合作组织（APAC）的互认协议成员。
本证书的有效性可登录www.cnas.org.cn获认可的机构名录查询。

2.5.1.4. CNAS 实验室认可证书

中国合格评定国家认可委员会

实验室认可证书

（注册号：CNAS L7966）

兹证明：

中科信息安全共性技术国家工程研究中心有限公司

（法人：中科信息安全共性技术国家工程研究中心有限公司）

北京市海淀区中关村大街 19 号新中关大厦 B 座北翼 16 层，

100080

符合 ISO/IEC 17025：2017《检测和校准实验室能力的通用要求》（CNAS-CL01《检测和校准实验室能力认可准则》）的要求，具备承担本证书附件所列服务能力，予以认可。

获认可的能力范围见标有相同认可注册号的证书附件，证书附件是本证书组成部分。

生效日期：2025-01-18

截止日期：2031-01-17

中国合格评定国家认可委员会授权人 张朝华

中国合格评定国家认可委员会（CNAS）经国家认证认可监督管理委员会（CNCA）授权，负责实施合格评定国家认可制度。
CNAS是国际实验室认可合作组织（ILAC）和亚太认可合作组织（APAC）的互认协议成员。
本证书的有效性可登陆www.cnas.org.cn获认可的机构名录查询。

2.5.1.5. 国家信息安全漏洞库（CNNVD）技术支撑单位三级

国家信息安全漏洞库（CNNVD）

技术支撑单位等级证书

（三级）

证 书 号：CNNVD-TechSup-2025-3-880

中科信息安全共性技术国家工程研究中心有限公司

注 册 地 址：北京市海淀区中关村大街19号16层B1601、B1602、B1603、B1605

统一社会信用代码：91110108791603851A

符合CNNVD三级技术支撑单位要求

特发此证

签发日期：2025年07月19日

有效期至：2026年07月18日

批准人：

中国信息安全测评中心

2025年07月19日

2.5.2. 管理体系资质

2.5.2.1. 质量管理体系认证证书（ISO9001）

注册号：016ZB24Q32378R5M

质量管理体系认证证书

初次发证日期：2009年10月27日/ 再认证日期：2024年10月21日/ 证书有效期至：2027年10月20日

(本次再认证审核日期:2024年10月19日到2024年10月20日，上一认证周期截止日期:2024年10月20日)

CERTIFICATE

兹 证 明

中科信息安全共性技术国家工程研究中心有限公司

质量管理体系符合GB/T19001-2016/ISO9001:2015 标准,适用于
网络安全服务、信息系统咨询规划服务、网络系统检测评估服务、商用密码应用安全性评估服务、网络安全等级测评与检测评估服务、网络安全审计服务、信息系统风险评估服务、代码安全审计服务

新世纪检验认证有限责任公司
总经理：

统一社会信用代码：91110108791603851A
注册地址：北京市海淀区中关村大街19号16层B1601、B1602、B1603、B1605
经营地址：北京市海淀区中关村大街19号新中关大厦B座北翼16层

中国认可
国际互认
管理体系
MANAGEMENT SYSTEM
CNAS C016-M

BCC 地址：北京市东城区广渠门内大街45号5层45-（05）-02室
本证书在国家规定的各行政许可、资质许可有效期内使用有效
获证组织必须定期接受监督审核并经审核合格，此证书方继续有效
证书有效性可通过网站：www.bcc.com.cn查询，也可二维码查询
本证书信息可在国家认监委网站www.cnca.gov.cn 查询

2.5.2.2. 信息安全管理体系认证证书（ISO27001）

注册号：0162E2480439R2M

信息安全管理体系认证证书

初次发证日期：2018年10月26日/ 再认证日期：2024年10月22日

证书有效期至：2027年10月25日

CERTIFICATE

兹 证 明

中科信息安全共性技术国家工程研究中心有限公司

信息安全管理体系符合ISO/IEC 27001:2022,适用于
与网络安全服务、信息系统咨询规划服务、网络系统检测评估服务、商用密码应用安全性评估服务、网络安全等级测评与检测评估服务、网络安全审计服务、信息系统风险评估服务、代码安全审计服务相关的信息安全管理；适用性声明：NERCIS-01-01 版本：B

新世纪检验认证有限责任公司
总经理：

统一社会信用代码：91110108791603851A
注册地址：北京市海淀区中关村大街19号16层B1601、B1602、B1603、B1605
经营地址：北京市海淀区中关村大街19号新中关大厦B座北翼16层

中国认可
国际互认
管理体系
MANAGEMENT SYSTEM
CNAS C016-M

BCC 地址：北京市东城区广渠门内大街45号5层45-（05）-02室
本证书在国家规定的各行政许可、资质许可有效期内使用有效
获证组织必须定期接受监督审核并经审核合格，此证书方继续有效
证书有效性可通过网站：www.bcc.com.cn查询，也可二维码查询
本证书信息可在国家认监委网站www.cnca.gov.cn 查询

2.5.2.3. 业务连续性管理体系认证证书

注册号：0162E2ABCM0053R1M

CERTIFICATE

业务连续性管理体系认证证书

初次发证日期：2022年01月11日/ 再认证日期：2024年11月28日

证书有效期至：2028年01月10日

兹 证 明

中科信息安全共性技术国家工程研究中心有限公司

业务连续性管理体系符合GB/T 30146-2023/ISO 22301:2019 标准,适用于与网络安全服务、信息系统咨询规划服务、网络系统检测评估服务、商用密码应用安全性评估服务、网络安全等级测评与检测评估服务、网络安全审计服务、信息系统风险评估服务、代码安全审计服务相关的业务连续性管理

新世纪检验认证有限责任公司

总经理：

统一社会信用代码：91110108791603851A

注册地址：北京市海淀区中关村大街19号16层B1601、B1602、B1603、B1605

经营地址：北京市海淀区中关村大街19号新中关大厦B座北翼16层

CNAS 中国认可 管理体系 MANAGEMENT SYSTEM CNAS C016-M

BCC 地址：北京市东城区广渠门内大街45号5层45-（05）-02室
本证书在国家规定的各行政许可、资质许可有效期内使用有效
获证组织必须定期接受监督审核并经审核合格，此证书方继续有效
证书有效性可通过网站：www.bcc.com.cn查询，也可二维码查询
本证书信息可在国家认监委网站www.cnca.gov.cn 查询

2.5.2.4. ISO/IEC20000-1:2011 信息技术服务管理体系认证证书

注册号：01620241ISM0324R1AGH

BCC

基于ISO/IEC 20000-1的服务管理体系认证证书

初次发证日期：2022年01月11日/ 再认证日期：2024年10月22日

证书有效期至：2028年01月10日

CERTIFICATE

兹 证 明

中科信息安全共性技术国家工程研究中心有限公司

基于ISO/IEC 20000-1的服务管理体系符合ISO/IEC 20000-1:2018标准,适用于向外部客户提供信息系统咨询规划服务、网络及网络系统检测评估服务、商用密码应用检测评估服务、信息系统测试与评估服务、信息系统审计服务

新世纪检验认证有限责任公司

总经理：

统一社会信用代码：91110108791603851A

注册地址：北京市海淀区中关村大街19号16层B1601、B1602、B1603、B1605

经营地址：北京市海淀区中关村大街19号新中关大厦B座北翼16层

CNAS 中国认可 管理体系 MANAGEMENT SYSTEM CNAS C016-M

BCC 地址：北京市东城区广渠门内大街45号5层45-（05）-02室

本证书在国家规定的各行政许可、资质许可有效期内使用有效

获证组织必须定期接受监督审核并经审核合格，此证书方继续有效

证书有效性可通过网站：www.bcc.com.cn查询，也可二维码查询

本证书信息可在国家认监委网站www.cnca.gov.cn 查询

2.5.3. 信息安全国家标准制定项目经验

2.5.3.1. GBT 29240-2024 网络安全技术 终端计算机通用安全技术规范

本文件由全国网络安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件起草单位：公安部第三研究所、联想（北京）有限公司、郑州信大捷安信息技术股份有限公司、深信服科技股份有限公司、北京天融信网络安全技术有限公司、奇安信网神信息技术（北京）股份有限公司、启明星辰信息技术集团股份有限公司、西安交大捷普网络科技有限公司、深圳融安网络科技有限公司、蓝象标准（北京）科技有限公司、长扬科技（北京）股份有限公司、杭州安恒信息技术股份有限公司、安天科技集团股份有限公司、亚信科技（成都）有限公司、中国惠普有限公司、浪潮电子信息产业股份有限公司、三六零科技集团有限公司、中孚信息股份有限公司、中科信息安全共性技术国家工程研究中心有限公司、中国电子科技集团公司第十五研究所、腾讯云计算（北京）有限责任公司、北京数安行科技有

限公司、中电科网络安全科技股份有限公司、蓝盾信息安全技术股份有限公司、飞腾信息技术有限公司、北京珞安科技有限责任公司、国网区块链科技（北京）有限公司、华为技术有限公司、大唐高鸿信安（浙江）信息科技有限公司、北京升鑫网络科技有限公司、博智安全科技股份有限公司、广东省信息安全测评中心、东软集团股份有限公司、北京百度网讯科技有限公司、泰康保险集团股份有限公司、北京北信源软件股份有限公司。

本文件主要起草人：李毅、邱梓华、宋好好、胡维娜、王志佳、李谦、李汝鑫、华昌、赵华、梁连燚、韩秀德、何建锋、刘晨、董晶晶、汪敦全、黄超、张运涛、苏振宇、胡建勋、奚乾悦、刘强、王奠、肖会波、张志磊、廖双晓、杨绍波、杨沅伊、刘俊、张亚京、文槿奕、王志宾、宋晓鹏、刘玉红、万森、肖智中、潘飚、冯彦朝、石竹玉、乔华阳、李实、叶劲宏、刘祥力、郑驰、傅涛、卞建超、谭琳、崔进、郭建领、黄斌杰、杨华。

本文件及其所代替文件的历次版本发布情况为：

——2012年首次发布为GB/T 29240—2012；

——本次为第一次修订。

2.5.3.2. GBT 30278-2024 网络安全技术 政务计算机终端核心配置规范

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替GB/T 30278—2013《信息安全技术　政务计算机终端核心配置规范》和GB/T 35283—2017《信息安全技术　计算机终端核心配置基线结构规范》。本文件以GB/T 30278—2013为基础，纳入GB/T 35283—2017的相关内容。与GB/T 30278—2013、GB/T 35283—2017相比，除结构调整和编辑性改动外，主要技术变化如下：

——增加了即时通信软件，5个安全控制点（见5.1、5.2）；

——增加了身份鉴别、访问控制、可信验证、数据保密性的配置要求（见6.1）；

——增加了可信验证、数据保密性、数据备份回复、个人信息保护、应用管控、数据发送控制的配置要求（见6.2）；

——增加了访问控制、入侵防范、个人信息保护、剩余信息保护、数据发送控制的配置要求（见6.4）；

——增加了即时通信软件配置要求（见6.7）；

——增加了配置要求证实方法和自动化部署及监测要求证实方法（见9章、10章）；

——增加了规范性引用文件ISO/IEC 18180:2013替代自定义基线配置自动化文件格式（见附录A）。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国网络安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件起草单位：神州网信技术有限公司、国家信息中心、麒麟软件有限公司、华为技术有限公司、北京天融信网络安全技术有限公司、长扬科技（北京）股份有限公司、统信软件技术有限公司、电子政务云技术应用国家工程实验室、中国电子技术标准化研究院、联想（北京）有限公司、北京升鑫网络科技有限公司、中科信息安全共性技术国家工程研究中心有限公司、阿里云计算有限公司、郑州信大捷安信息技术股份有限公司、北京奇虎科技有限公司、三六零科技集团有限公司、西安邮电大学、昆仑太科（北京）技术股份有限公司、北京神州绿盟科技有限公司、奇安信科技集团股份有限公司、西安交大捷普网络科技有限公司、北京中科微澜科技有限公司、浪潮（山东）计算机科技有限公司、吉林信息安全测评中心、北京北信源软件股份有限公司、北京山石网科信息技术有限公司、深圳市能信安科技股份有限公司、启明星辰信息技术集团股份有限公司、国家保密科技测评中心、国网新疆电力有限公司电力科学研究院、大唐高鸿信安（浙江）信息科技有限公司、工业和信息化部电子第五研究所、安天科技集团股份有限公司、中国软件评测中心（工业和信息化部软件与集成电路促进中心）、北京邮电大学、联通（四川）产业互联网有限公司。

本文件主要起草人：张建军、刘蓓、杨尚欣、孟亚平、陈韵然、王强、战茅、董军平、王震、桂耀、张宇、安高峰、赵华、何雪林、许涛、闫桂勋、李占伟、朱华、李汝鑫、刘俊、孙亮、何建锋、卞建超、程度、胡建勋、龙勤、刘为华、姚一楠、张志磊、李富钦、廖百成、张勇、李德全、华昌、安锦程、郭维、白欣璐、李岩、刘占丰、杨泳、赵勇、梁桂铅、李德庆、马进、贾楠、刘博、马玮、刘海洁、柴思跃、张生华、张雷、周润松、郭盈、马向亮、李诗婧、张涛。

本文件及其所代替文件的历次版本发布情况为：

——GB/T 30278—2013；

——GB/T 35283—2017；

——本次为第一次修订。

2.5.3.3. GBT 43694-2024 网络安全技术 证书应用综合服务接口规范

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：北京数字认证股份有限公司、博雅中科(北京)信息技术有限公司、北京奇虎科技有限公司、山东得安信息技术有限公司、中国电力科学研究院、北京信安世纪科技股份有限公司、无锡江南信息安全工程技术中心、中国电子技术标准化研究院、格尔软件股份有限公司、中电科网络安全科技股份有限公司、深圳市不动产登记中心、郑州信大捷安信息技术股份有限公司、阿里云计算有限公司、浙江九州量子信息技术股份有限公司、航天信息股份有限公司、数安时代科技股份有限公司、智巡密码(上海)检测技术有限公司、中科信息安全共性技术国家工程研究中心有限公司、中国汽车工程研究院股份有限公司。

本文件主要起草人：刘伟、赵永省、夏鲁宁、李述胜、刘中、程科伟、浦雨三、张屹、张志磊、马洪富、袁中林、李智虎、焦靖伟、刘平、黄晶晶、谭武征、寇建波、颜海龙、刘献伦、刘为华、肖淑婷、张文科、杨倩媚、董亮亮、周蔚林、韩玮、高振鹏、胡建勋、刘冲、牟洁。

2.5.3.4. GBT 43779-2024 网络安全技术 基于密码令牌的主叫用户可信身份鉴别技术规范

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：中国科学院大学、中国电信集团有限公司、中国电子技术标准化研究院、中国移动通信集团有限公司、中国信息通信研究院、北京数字认证股份有限公司、华为技术有限公司、北京小米移动软件有限公司、OPPO广东移动通信有限公司、中兴通讯股份有限公司、北京三星通信技术研究有限公司、微位(深圳)网络科技有限公司、广东省电子商务认证有限公司、深圳市电子商务安全证书管理有限公司、中科信息安全共性技术国家工程研究中心有限公司、联通智慧安全科技有限公司、北京信安世纪科技股份有限公司、联通(广东)产业互联网有限公司、国民认证科技(北京)有限公司、郑州信大捷安信息技术股份有限公司、数安时代科技股份有限公司、工业信息安全(四川)创新中心有限公司、成都亚信网络安全产业技术研究院有限公司、武汉大学。

本文件主要起草人：荆继武、王跃武、刘紫千、上官晓丽、刘丽敏、魏亮、詹榜华、寇春静、任兰芳、郑学欣、王平建、颜雪薇、常新苗、雷灵光、黄钱红、李根、王榕、王鹏、华孝泉、吴越、鲍博武、陈木来、梁宁宁、吴昊、李彦峰、王志辉、胡建勋、金刚、张宇、吕召彪、李俊、刘为华、廖正贤、周蔚林、罗影、张文科、吴强、陈晶、赵文博。

3. 技术部分

3.1. 采购需求偏离表

序号	招标文件条目号	招标文件要求	投标文件响应	说明
1	第五章 5.1 项目采购需求：差距分析	通过访谈、资料调阅、走查、漏洞扫描及配置核查等方式开展差距分析（预测评）工作，分析已定级的信息系统所采取的安全保护措施与等保 2.0 标准要求之间的差距。	我公司将根据定级报告中被评估信息系统的安全等级，从等级保护基本要求的指标中选择和组合评估用的安全指标，形成一套信息系统的评估指标，作为差距分析评估的依据；	无偏离
2	第五章 5.1 项目采购需求：协助整改	根据测评中发现的技术问题，提出整改意见与建议，并指导采购方进行整改； 指导采购方完善网络安全管理制度体系建设，按照相关制度规范，指导相关管理制度编写、修改与发布。	等级保护体系设计的工作目的是根据前期系统定级、差距分析和等级保护整改结果、结合被测评单位实际网络情况和系统情况及业务现状，参考国内外成熟的信息安全管理理论和实践，以国家信息安全等级保护政策法规和标准规范为指导。从安全技术、安全管理二个维度，设	无偏离

			计合理的信息安全策略，以及安全技术措施、安全管理组织、安全管理制度等，建立结构化的信息安全管理体系，整体提高被测评单位的信息安全防护能力，满足国家等级保护要求，切实保障信息系统安全稳定运行，建立信息安全长效机制。	
3	第五章 5.3 项目采购需求：开展网络安全等级保护测评	测评机构依据《网络安全等级保护测评指南》，通过访谈、资料调阅、走查、渗透测试、漏洞扫描及配置核查等方式开展网络安全等级保护测评工作，并出具等级保护测评报告。	依据网络安全等级保护相关标准，在对被测系统充分了解、准确掌握被测系统相关安全情况的基础上，通过安全整改后开展网络安全等级保护测评工作并出具《等级保护测评报告》。	无偏离
4	第五章 5.4 项目采购需求：交付物要求	测评交付物应包括不限于《漏洞扫描报告》、《渗透测试报告》（三级信息系统）、《网络安全等级保护差距分析清单》、《网络安全等级	测评交付物包括《项目计划书》、《系统测评实施方案》、《系统测评工作计划》、《漏洞扫描报告》、《渗透测试报告》（三级信息系统）、《网络安全等级保护差距	无偏离

		保护测评报告》	分析清单》、《网络安全等级保护测评报告》等	
5	第五章 5.2 详细技术要求（一）：商用密码总体要求测评：密码算法合规性测评	密码算法合规性测评：信息系统中使用的密码算法是否符合法律法规的规定和密码相关国家标准、行业标准的有关要求。	了解信息系统中使用的密码算法的名称、用途、何处使用、执行设备及其实现方式（软件、硬件或固件），核查信息系统中使用的密码算法是否符合法律法规的规定和密码相关国家标准、行业标准的有关要求。	无偏离
6	第五章 5.2 详细技术要求（一）：商用密码总体要求测评：密码技术合规性测评	密码技术合规性测评：信息系统中使用的密码技术是否遵循密码相关国家标准和行业标准。	了解信息系统中使用的密码技术的名称、用途、何处使用、执行设备及其实现方式（软件、硬件或固件），核查信息系统中使用的密码技术是否符合法律法规的规定和密码相关国家标准、行业标准的有关要求。	无偏离
7	第五章 5.2 详细技术要求（一）：商用密码总体要求测评：密码产品合	密码产品合规性测评：信息系统中使用的密码产品与密码模块是否通过国家密码管理部门核准。	了解信息系统中使用的密码产品的型号和版本等配置信息，核查密码产品是否经商用密码认证机构认证合	无偏离

	规性测评		格，并核查密码产品的使用是否满足其安全运行的条件，例如其安全策略或使用手册说明的部署条件。遵循了密码模块相关标准的密码产品，还要核查其是否满足密码模块相应安全等级及以上安全要求。	
8	第五章 5.2 详细技术要求（一）：商用密码总体要求测评：密码服务合规性测评	密码服务合规性测评：信息系统中使用的密码服务是否通过国家密码管理部门许可。	核查信息系统中使用的密码服务是否符合法律法规的相关要求。	无偏离
9	第五章 5.2 详细技术要求（二）：密码技术应用测评	从物理和环境、网络和通信、设备和计算、应用和数据 4 个层面对信息系统中应用的密码技术进行分析与评估。	涵盖物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、安全制度、人员管理、建设运行、应急管理	无偏离
10	第五章 5.2 详细技术要求（三）：密钥管理测评	对影响商用密码防护效能的密钥生命周期相关环节，以及相关环节管理和策略制定的全过程进	核查密钥管理使用的密码产品、密码服务是否满足密码产品和密码服务的要求： 核查信息系统密钥管理实现是否安全、正	无偏离

		行分析与评估。密钥生命周期相关环节包括但不限于下列典型环节：密钥生成，密钥存储，密钥分发，密钥导入，密钥导出，密钥使用，密钥备份，密钥恢复，密钥归档，密钥销毁。	确、有效。例如:非公开密钥是否能被非授权访问、使用、泄露、修改和替换,公开密钥是否能被非授权修改和替换。	
11	第五章 5.2 详细技术要求（三）：安全管理测评	对影响商用密码防护效能的管理制度与措施进行分析与评估。管理制度与措施包括但不限于下列典型维度:安全管理制度，人员管控，信息系统实施,应急预案。	核查各项安全管理制度、安全操作规范和配套的操作规程是否覆盖包括密码建设、运维、人员、设备、密钥等密码管理相关内容；核查在规划阶段，是否依据密码相关标准和密码应用需求，制定密码应用方案；检查应急预案及相关管理制度文档，是否根据安全事件等级制定了相应的应急预案及管理制度，明确了应急事件处理流程及其他管理措施，并遵照执行。如有安全	无偏离

			事件发生，检查是否有相应的处置记录。	

注：1．本表所列内容应符合招标文件第二章“投标人须知”第 11.2 款和第 14.4.1 款规定。

2．投标人应当逐条对照招标文件第五章“采购需求”，就投标文件对技术标准及要求存在的偏差与例外逐条做出说明。

3．投标人应当对每一条款作出明确答复（如果需要，可给出详细的响应内容），否则将可能被视为放弃应答。诸如“已知”、“理解”、“明白”或“同意”等这样非确切的答复是不可接受的。

4．如招标文件中所列指标有具体要求、参数或指标要求的，投标文件中除回答“满足”、“部分满足”或“不满足”外，还应当列出具体要求、参数或指标。

5．以上表格仅供参考，投标人可以根据情况自行编制偏离文件。

3.2. 技术方案建议书

3.2.1. 项目概述

3.2.1.1. 项目目标

中科信息安全共性技术国家工程研究中心有限公司按照《信息安全技术网络安全等级保护基本要求》GB/T22239-2019 文件的要求需要进一步落实安全防护建设工作。推动信息系统安全整改工作不仅是维护社会稳定，保持社会和谐的大事，也是确保北京市文化和旅游局宣传中心（北京市旅游运行监测中心）信息化工作安全、快速发展的需要。通过开展等级保护、商用密码评估，推动北京市文化和旅游局宣传中心（北京市旅游运行监测中心）信息系统等级保护工作的进一步落实，提升信息系统整体安全性和稳定性，促进安全管理水平的提高，增强信息系统安全风险管理意识。同时，发现与《信息系统安全等级保护基本要求》的差距，并根据测评结果，完成信息安全等级保护后期整改工作，落实等级保护的各项要求，提高信息安全水平和安全防范能力。

3.2.1.2. 服务内容

根据国家信息安全相关政策和要求，由具备网络安全等级测评与检测评估机构服务认证证书、商用密码检测机构资质证书的机构进行等级保护测评及商用密码测评，全面评估信息系统现有安全防护水平和相应等级安全要求之间的差距，测评内容包括技术安全测评、管理安全测评和综合测评，并出具测评报告。等级保护测评系统包括：北京智慧文旅平台-文旅数据中心系统、北京智慧文旅平台-政府监管平台系统、北京市旅游团队电子行程单(二期)和电子合同项目、北京市文化和旅游局财务内控综合管理信息平台、北京市文化和旅游局办公系统。商用密码评估系统包括：北京智慧文旅平台-文旅数据中心系统、北京智慧文旅平台-政府监管平台系统。

3.2.1.3. 项目原则

为保障项目的顺利实施，在项目实施过程须遵循以下原则：

（1）客观性和公正性原则

测评人员不会有偏见，在最小主观判断情形下，按照评估双方相互认可的评估方案，基于明确定义的测评方式和解释，实施评估活动。

（2）规范性原则

项目实施由专业的测评服务人员依照规范的操作流程进行，对操作过程和结果要有相应的记录，并提供完整的服务报告。

（3）标准化原则

测评过程会严格遵守国家的相关法律、法规、规范、标准等相关要求。

（4）完整性原则

在测评过程中，确保测评数据、过程记录的完整性。评测内容会综合考虑所有评测对象的技术措施，并建立完整有效的评测流程，保证不存在影响评测结果的疏忽或遗漏。

（5）连续性原则

确保在高速变化的信息安全环境中，在有效的服务期间内，保证采购方风险评估结论的准确性和及时性，对于新增设的信息资产和服务，或新建立的信息化项目，进行局部系统的重新评估。从经济上，降低客户的成本，从信息安全性上，保证信息安全测评的动态稳定性。

（6）扩展性原则

在评估过程结束后，信息安全测评过程会保持扩展性，从扩展的属性上进一步加强测评结束后客户的安全管理有效性和可用性。

（7）质量保障原则

在整个测评过程中，会特别重视项目质量管理。项目的实施将严格按照项目

实施方案和流程进行，并由项目协调小组从中监督，控制项目的进度和质量。

3.2.1.4. 项目重点、难点分析

3.2.1.4.1. 差距分析阶段重点、难点

- **重点**

首先进一步详细分析已定级系统和尚未定级系统在安全架构、技术和管理等方面的差距，给出整改建议，并帮助北京市文化和旅游局宣传中心（北京市旅游运行监测中心）制定有效的整改计划，其次针对已进入定级备案流程的系统，对其保护等级和安全要求进行细化和优化，确保系统符合最新的等级保护标准和规范，为客户提供相关培训和指导，加强其信息安全意识和安全管理能力。

识别各个信息系统的安全边界和安全要求前，需要充分了解各个信息系统的特点、功能和互联关系，确定各个信息系统的边界和测评内容。需要识别各个信息系统扩展要求和安全需求。

因此本阶段服务重点在于通过对信息系统的调查和测评，找出存在的安全风险并提供整改建议。需要充分调研各类信息系统的建设情况，从服务器资产、网络设备、安全设备、制度管理等多个维度进行细致的分析，以发现可能存在的安全隐患和技术问题。

- **难点**

本阶段要充分考虑不同信息系统之间的差异性，在比较过程中安全合规，对于差距较大的系统，需要制定详细的整改计划，跟踪整改进展情况，防止漏洞等安全问题再次出现，在整改建议和方案制定过程中，需与客户充分沟通，听取反馈和建议，做到量身定制。

因此服务难点在于进行全面和实际的测评测试，并给出与客户实际情况相适应的建议和整改方案。此外，需要充分了解并尊重客户的实际情况，提供有针对性的服务和建议，为客户着想，实现信息安全防范的效果最大化。

3.2.1.4.2. 协助建设整改重点、难点

- **重点**

- 根据差距分析的结果，制定针对性的整改方案
- 协助组织实施整改措施，提升系统的安全保护能力

- **难点**

- 协助制定既符合等级保护要求又切实可行的整改方案。
- 整改措施的有效实施和持续改进

3.2.1.4.3. 等级保护测评重点、难点

- **重点**

全面评估北京市文化和旅游局宣传中心（北京市旅游运行监测中心）的各项控制措施，并提供针对性的建议和整改方案。需要进行全面的测试和评估，从安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全人员管理、安全制度管理、安全机构管理、安全建设管理、安全运维管理（如有云计算扩展、移动互联安全扩展、工业控制扩展）层面等多个维度进行细致评估，评估被测评单位的安全状况。

- **难点**

对不同类型的信息系统所面临的风险和威胁也不相同，而且本次测评还可能涉及其他系统，需要提供有针对性的评估报告和整改措施。同时，需要在测试过程中与被测评单位进行有效沟通，便于更加准确地找出漏洞并提出建议，同时确保测试过程和测试结果的准确性和可靠性。

3.2.1.5. 网络安全等级保护实施方案

3.2.1.5.1. 差距分析服务内容

3.2.1.5.1.1. 服务内容

3.2.1.5.1.1.1. 确定差距分析评估指标

我公司将根据定级报告中被评估信息系统的安全等级，从等级保护基本要求的指标中选择和组合评估用的安全指标，形成一套信息系统的评估指标，作为差距分析评估的依据；

3.2.1.5.1.1.2. 制定差距分析评估方案

我公司将根据评估指标，结合确定的具体评估对象制定可以操作的评估方案，评估方案通常包括但不局限于以下内容：

① 管理状况评估表格；

② 网络状况评估表格；

③ 网络设备（含安全设备）评估表格；

④ 主机设备评估表格；

⑤ 主要设备安全测试方案；

⑥ 重要操作的作业指导书。

3.2.1.5.2. 等级指标对比评估

我公司根据所确定的安全评估指标和安全评估方案，通过询问、检查和测试等多种手段，将系统现状与安全评估指标进行逐一对比，记录当前的现状情况，找到与评估指标之间的差距。

我公司提供的等级保护差距分析评估服务，主要是针对《网络安全等级保护基本要求及扩展要求》中的相关内容和要求进行差距评估。评估主要包括技术和

管理两个方面的内容。

① 安全技术评估：主要通过从物理安全、网络安全、主机系统安全、应用安全和数据安全与备份恢复等五个层面上评估信息安全等级保护要求的基本安全控制在信息系统中的实施配置情况。

② 安全管理评估：通过查阅文档、抽样调查等方法，针对被测单位在信息安全方面制定规章制度的合理性、适用性等进行评估，主要包括安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等内容。

3.2.1.5.3. 综合评估分析

我公司将根据等级指标对比评估结果记录，结合被评估单位提供的各种资料，评进行全面的综合分析，编制评估报告。差距分析评估报告包括安全现状和安全建议两个方面的内容。安全现状主要描述通过评估所了解到的系统的各个层面的基本安全状况，以及与等级要求的符合情况。安全建议主要描述针对系统存在的安全隐患和缺陷以及如何进行改造，以符合相应等级的安全需求。由于被评估信息系统可能包括多个安全等级不同的子系统，原则上需要分别对它们进行评估和拟定报告。

3.2.1.5.4. 控制建议

采取可行的安全保障措施，可以将已找出的威胁和弱点的可能性及其影响减至可接受的水平。

我公司评估小组根据不可接受风险级别的定义，鉴别组织存在的不可接受风险，分析控制不可接受风险的相应安全措施，最终组织参与人员根据评估小组所提的建议，结合组织的实际情况，确定适用于组织的安全措施，制定保护策略，最终形成控制建议。形成控制建议的目的是为组织制定保护策略，降低关键资产风险的方案，以及制定短期内的措施清单。

我公司评估小组对组织目前的技术安全状况进行分析，并通过与组织相关IT人员的沟通，优先确认需要立即采取措施以修复的技术弱点，制定所存在的

技术弱点及相应的安全建议。

从体系化的角度采取控制措施，例如依据风险评估结果建立纵深防御体系。常见的控制措施类型包括：

安全加固建议：这是一种有针对性地资产点对点风险减免。主要是通过各种技术手段来补救单个资产的弱点。

安全体系结构建议：这是从系统的角度来重要设计更安全的系统。主要通过更合理的网络结构与系统逻辑关系设计来补救整个系统的弱点。

安全管理建议：这是从管理的角度来保护资产不受威胁。主要通过把具有弱点而且难以补救的资产保护起来，不受威胁的影响，也就起到了降低风险的作用。

3.2.1.6. 服务方式

① 调查问卷：根据信息系统业务情况和现状，制定详细的调查表，并由被测评单位相关人员进行填写，以获得业务系统信息安全及管理情况，具体内容包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理机构、安全管理制度、安全管理人员、安全建设管理和安全运维管理等。

② 人员访谈：针对组织内的安全管理人员、安全员、安全主管、工作人员、关键活动批准人、管理人员、机房值守人员、人事负责人、人事工作人员、审计员、网络管理员、文档管理员、物理安全负责人、系统管理员、系统建设负责人、系统运维负责人、资产管理员等不同类型岗位的人员访谈。

③ 文档检查：查看安全管理机构、安全管理制度、人员安全管理、系统建设管理、系统运维管理等方面的文档。

④ 人工配置检查：查看安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心等方面的技术配置信息。

⑤ 漏洞扫描：对网络设备、服务器、终端、操作系统（win/linux/Solaris/AIX/）数据库（Oracle/SQL）、中间件、安全设备进行漏洞扫描。

⑥ 会议：召集被测信息系统相关的技术人员、管理人员、使用人员以及应用系统的开发厂商、运维服务商等对系统基本情况进行识别和分析，并就安全风险测试项目进行讨论。

3.2.1.7. 成果文档

本阶段的交付物主要有《差距分析报告》。

3.2.2. 协助安全整改

3.2.2.1. 服务内容

等级保护体系设计的工作目的是根据前期系统定级、差距分析和等级保护整改结果、结合被测评单位实际网络情况和系统情况及业务现状，参考国内外成熟的信息安全管理理论和实践，以国家信息安全等级保护政策法规和标准规范为指导。从安全技术、安全管理二个维度，设计合理的信息安全策略，以及安全技术措施、安全管理组织、安全管理制度等，建立结构化的信息安全管理体系，整体提高被测评单位的信息安全防护能力，满足国家等级保护要求，切实保障信息系统安全稳定运行，建立信息安全长效机制。

方案设计的工作内容包括方案设计项目小组根据前期现状调研和差距分析结果、用户需求等进行整改方案设计。

3.2.2.1.1. 技术整改方案设计

根据前阶段的安全基础调研、差距分析工作中技术方面单元测评的结果分析以及整体测评的结论，了解到当前安全技术措施建设的不足方面，确定针对信息系统的安全需求。根据安全需求分析，形成纲领性的安全文件，包括安全工作的总体原则、安全策略等，用于指导信息系统安全技术体系和安全管理体系的构建。设计技术方案时，应以《基本要求》为基本目标，可以针对安全现状分析发现的问题进行加固改造，查漏补缺；也可以进行总体的安全技术设计，将不同区域、不同层面的安全保护措施形成有机的安全保护体系，建立总体技术框架结构，从

物理环境，通信网络、计算环境、区域边界、安全管理中心等方面设计落实基本技术要求的物理、网络、系统、应用和数据的安全要求的技术路线。

我公司为被测评单位目标信息系统的建设整改技术部分的方案将包含：

① 安全物理环境设计

从安全技术设施和安全技术措施两方面来对涉及的主机房、辅助机房和办公环境等进行物理安全设计，设计内容包括《基本要求》内物理层面的各个控制点，将主要根据差距内容来描述将要补充的技术设施和措施。

② 安全通信网络设计

对信息系统所涉及的通信网络，包括骨干网络和其他通信网络进行安全设计，设计内容包括通信过程的数据完整性、包括链路与网络设备的荣冗余；网络的安全配置和加固等

③ 安全区域边界设计

对信息系统所涉及的区域网络边界进行安全设计，内容包括对边界保护、安全区域划分、身份认证、访问控制、安全审计、入侵防范、恶意代码检测和网络设备自身防护等

④ 安全计算环境设计

对信息系统涉及的服务器和工作站进行主机系统安全设计，内容包括操作系统或数据库管理系统的选择、安装和安全配置，主机入侵防范、恶意代码检测、资源使用等情况。对信息系统涉及的应用系统软件进行安全设计，设计内容包括身份鉴别、访问控制、安全标记、可信路径、安全审计、剩余信息保护、通信完整性、通信保密性、容错性、抗抵赖性、资源控制等。关注应用系统的安全框架、安全机制选择与实现方式、编码安全规范与代码审核。

⑤ 安全管理中心设计

对系统管理员、审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。

3.2.2.1.2. 管理整改方案设计

首先，我公司需要通过差距测评的单元测评结果和整体测评的结论提取当前安全状态下的安全管理建设需求，找到信息系统安全管理建设整改需要解决的问题，明确信息系统安全管理建设的需求。

安全管理体系的设计内容包括：

① 人员安全管理

人员安全管理主要包括人员录用、离岗、考核、教育培训等内容。针对人员安全管理方面的差距描述整改建议和措施。

② 环境和资产管理

明确环境（机房、办公环境）安全管理的责任部门或责任人，加强对人员录入、来访人员的控制，对有关物理访问、物品进出和环境安全等方面作出规定。针对环境和资产管理方面的差距描述整改建议和措施。

③ 设备和介质安全管理

明确配套设施、软硬件设备管理、维护的责任部门或责任人，对信息系统的各种软硬件设备采购发放、领用、维护和维修等过程的控制和管理，针对设备和介质安全管理方面的差距描述整改建议和措施。

④ 日常运维管理

明确网络、系统日常运行维护的责任部门或责任人，对运维管理中的日常操作、账号管理、安全配置、日志管理、补丁升级、口令更新等过程进行控制和管理，针对日常运维管理方面的差距描述整改建议和措施。

⑤ 集中安全管理

信息系统应按照统一的安全策略、安全管理要求、统一管理信息系统的安全运行，进行安全机制的配置与管理，进行安全机制的配置与管理，对设备安全配置、恶意代码、补丁升级、安全审计等进行管理。将针对集中安全管理方面的差距描述整改建议和措施。

⑥ 事件处置与应急响应

按照国家有关标准规定，确定信息安全事件等级，制定安全事件分级应急处置预案，明确应急处理策略，落实应急部门和人员，建立协调响应机制等，将针对事件处置与应急响应管理方面的差距描述整改建议和措施。

⑦ 灾难备份

要对信息系统采取灾难备份措施，定期备份重要业务信息、系统数据及软件系统等，制定备份策略和恢复策略等。将针对灾难备份安全管理方面的差距描述整改建议和措施。

⑧ 实时监测

需要开展信息系统实时安全监测，实现对物理环境、通信线路、主机、网络设备、用户行为、特殊事件等的监测和报警，及时发现设备故障、病毒入侵、黑客攻击等安全事件。可建立安全运行中心机制。针对实时监测管理方面的差距描述整改建议和措施。

⑨ 其他安全管理方面

对运维过程中的其他管理活动，如系统变更、密码使用等进行管制和管理。或其他的安全管理内容描述整改建议和措施。

3.2.2.2. 成果文档

本阶段的交付物主要有《信息系统等级保护整改方案》等。

3.2.3. 等级保护测评服务内容

依据网络安全等级保护相关标准，在对被测系统充分了解、准确掌握被测系统相关安全情况的基础上，通过安全整改后开展网络安全等级保护测评工作并出具《等级保护测评报告》。

3.2.3.1. 测评流程

本次等级测评分为以下几个步骤：测评准备、方案编制、现场测评、分析与报告编制活动。

3.2.3.1.1. 测评准备阶段

① 测评项目组组建

明确项目经理、测评人员及职责分工。

② 项目计划书编制

项目组制定《系统测评实施方案》和《系统测评工作计划》，并报项目主管审定。项目计划书包含项目概述、工作依据、技术思路、工作内容和项目组织等。测评方案包括测评对象、测评指标的选取、测评内容及测评实施等。

③ 召开项目协调会

与北京市文化和旅游局宣传中心（北京市旅游运行监测中心）进行一次协调会，内容：介绍参与该项目测评的工作人员、信息系统测评工作计划与实施方案、对方介绍网络系统情况、确定北京市文化和旅游局宣传中心（北京市旅游运行监测中心）配合的人员、确定现场核查测试的具体日期，以及需要与北京市文化和旅游局宣传中心（北京市旅游运行监测中心）沟通的其他问题，如北京市文化和旅游局宣传中心（北京市旅游运行监测中心）同意测评计划和实施方案，需进行签字确认。

④ 信息系统调研

通过查阅被测系统已有资料或使用调查表格的方式，了解整个系统的构成和保护情况，明确被测系统的范围（特别是信息系统的边界），了解被测系统的详细构成，包括网络拓扑、业务应用、业务流程、设备信息（服务器、数据库、网络设备、安全设备、数据库等）、管理制度等。

⑤ 工具和表单准备

根据被测系统的实际情况，准备测评工具和各类测评表单。

3.2.3.1.2. 方案编制阶段

① 测评对象确定

根据已经了解到的被测系统信息，分析整个被测系统及其涉及的业务应用系统，确定出本次测评的测评对象。

② 测评指标确定

根据已经了解到的被测系统定级结果，确定出本次测评的测评指标。

③ 测评工具接入点确定

确定需要进行工具测试的测评对象，选择测试路径，根据测试路径确定测试工具的接入点。

④ 测评内容确定

确定现场测评的具体实施内容，即单元测评内容。

⑤ 测评实施手册开发

编制测评实施手册，详细描述现场测评的工具、方法和操作步骤等，具体指导测评人员如何进行测评活动。

3.2.3.1.3. 现场测评阶段

现场测评实际上就是单项测评，分别从技术上的物理环境、通信网络、区域边界、计算环境、安全管理中心五个层面和管理上的管理机构、管理制度、人员管理、系统建设管理和系统运维管理五个方面分别进行。

① 现场核查测试

测评分为核查组和技术测试组，核查组负责安全管理类的文档资料查验、现场访谈、检查工作，并详细填写安全管理核查记录表单；技术测试组负责信息系统技术文档的核查和具体测试工作，测试前，必须在北京市文化和旅游局宣传中

心（北京市旅游运行监测中心）配合人员的监督下，现场对测评工具进行杀毒检测，填写《测评工具杀毒检测记录表》，由北京市文化和旅游局宣传中心（北京市旅游运行监测中心）配合人员签字确认后再进行测试。技术测试在北京市文化和旅游局宣传中心（北京市旅游运行监测中心）人员的配合下，进行访谈、查阅技术文档，技术测试，并详细填写安全技术测试检查表单。质量监督人员监督核查测试过程，填写《系统测评监督记录表》。

② 现场核查测试结束

由北京市文化和旅游局宣传中心(北京市旅游运行监测中心)配合人员检查、验证被测信息系统运行情况，确认无误后，在《系统运行情况验证记录》表上签字确认。内部对测试工具进行杀毒检测，并填写《测评工具使用情况记录》，质量监督员进行签字确认。

项目组按照测评分工，整理核查测试数据，分别完成现场核查报告和技术测试分析报告。最终形成《系统核查测试报告》。质量监督人员填写《系统测评监督记录表》。

《系统核查测试报告》由主管审核签字。

归还所有纸质文档，并填写确认单。

3.2.3.1.4. 报告服务内容

① 单项测评结果分析

针对测评指标中的单个测评项，结合具体测评对象，客观、准确地分析测评证据。

② 单元测评结果判定

将单项测评结果进行汇总，分别统计不同测评对象的单项测评结果，从而判定单元测评结果，并以表格的形式逐一列出。

③ 整体测评

针对单项测评结果的不符合项，采取逐条判定的方法，从安全控制间、层面

间和区域间出发考虑，给出整体测评的具体结果，并对系统结构进行整体安全测评。

④ 风险分析

据等级保护的相关规范和标准，采用风险分析的方法分析等级测评结果中存在的安全问题可能对被测系统安全造成的影响。

⑤ 等级测评结论形成

在测评结果汇总的基础上，找出系统保护现状与等级保护基本要求之间的差距，并形成等级测评结论。

⑥ 测评报告编制

根据等级测评结论，编制测评报告，包括概述、被测系统描述、测评对象说明、测评指标说明、测评内容和方法说明、单元测评、整体测评、测评结果汇总、风险分析和评价、等级测评结论、整改建议等。

3.2.3.2. 测评方式

依据《网络安全等级保护测评要求》三级安全保护能力基本要求，从安全技术和安全管理两方面对被测系统进行信息安全等级保护测评工作，并出具《网络安全等级保护测评报告》。

本次信息系统等级保护测评主要分为现场实施阶段和后期数据分析阶段两部分。

等级测评现场实施期间，项目组成员分别采用人员访谈、文档检查、技术核查、工具扫描等方法对被测评系统进行测评，测评内容覆盖《网络安全等级保护基本要求》、《网络安全等级保护测评要求》三级安全保护能力基本要求各个层面的要素。现场实施过程中采用的各类测评方法均以《网络安全等级保护基本要求》中相关等级的安全评价要素为基准，由测评工作人员制定相应的现场检查表，记录现场核查的相关数据、记录，作为后期对比标准中的基准要点的评判依据。

在等级保护测评过程目中，将采用以下测评方法：

① 访谈

访谈是指测评人员与被测评组织内的有关人员就测评所关注的问题进行有针对性的询问和交流的过程，该过程可以帮助评估者了解现状、澄清疑问或获得证据。

访谈深度（即访谈内容的详细程度）以及访谈的广度（即对被测评组织中员工角色类型以及每种类型中人数的覆盖程度）由测评人员依据不同的测评需要进行选择和判断。

简要描述	与被测系统有关人员（个人/群体）进行交流、讨论等活动，获取相关证据，了解有关信息。在访谈范围上，不同等级信息系统在测评时有不同的要求，一般应基本覆盖所有的安全相关人员类型，在数量上可以抽样。
达成目标	发掘技术和管理方面存在的安全问题
工作条件	提供适于单独交流的工作环境（会议室、会客室），甲方人员配合
工作结果	人员访谈记录

② 核查

检查是指对测评对象（如规范、机制或行为）进行观察、调查、评审、分析或核查的过程。与访谈类似，该过程可以帮助评估者了解现状、澄清疑问或获得证据。

比较典型的检查行为包括：对安全配置的核查、文档审查等。

文档审查	**简要描述**	检查制度、策略、操作规程、制度执行情况记录等文档（包括安全方针文件、安全管理制度、安全管理的执行过程文档、系统设计方案、网络设备的技术资料、系统和产品的实际配置说明、系统的各种运行记录文

		档、机房建设相关资料、机房出入记录等过程记录文档）的完整性，以及这些文件之间的内部一致性。
	达成目标	发掘技术和管理方面存在的安全问题
	工作条件	提供安静的工作环境，甲方人员、各类文档资料配合
	工作结果	文档审查结果记录
配置核查	**简要描述**	利用上机验证的方式检查主机、服务器、数据库、网络设备、安全设备、应用系统的配置是否正确，是否与文档、相关设备和部件保持一致，对文档审核的内容进行核实（包括日志审计等），测评其实施的正确性和有效性，检查配置的完整性，测试网络连接规则的一致性，从而测试系统是否达到可用性和可靠性的要求。
	达成目标	发现配置的安全隐患
	工作条件	可以访问网络、主机的工作环境，甲方人员、网络、系统配合
	工作结果	配置检查结果记录

③ 实地查看

通过实地的观察人员行为、技术设施和物理环境状况判断人员的安全意识、业务操作、管理程序和系统物理环境等方面的安全情况，测评其是否达到了相应等级的安全要求。

简要描述	通过现场察看人员行为、技术设施和物理环境状况，检查人

	员的安全意识、业务操作、管理程序和系统物理环境等方面的安全情况。
达成目标	发掘技术和管理方面存在的安全问题
工作条件	不限制，甲方人员配合
工作结果	实地查看结果记录

④ 工具测试

利用技术工具（漏洞扫描工具、渗透测试工具、压力测试工具等）对系统进行测试，包括基于网络探测和基于主机审计的漏洞扫描、渗透测试等。

简要描述	利用技术工具，从网络的不同接入点对网络内的主机、服务器、数据库、网络设备、安全设备等进行脆弱性检查和分析
达成目标	发掘系统的安全漏洞
工作条件	相对独立的工作环境，电源和网络接入环境，甲方人员、网络、系统配合
工作结果	工具测试结果记录

我们在等级保护测评过程中使用的测评工具严格遵循可控性原则，即所有使用的测评工具将事先提交给甲方检查确认，确保在双方认可的范围之内，而且测评过程中采用的技术手段确保已经过可靠的实际应用。

在本项目中，将采用以下测评工具：

序号	工具名称	工具用途分类
1	绿盟远程评估系统	系统层、应用层漏洞检测

2	渗透测试工具集	应用渗透测试
3	等保测评工具箱	承载等保测评工具
4	等保测评工具	辅助测评人员开展等保测评工作
5	AppScan9.0.3.6	发现相关的安全漏洞，如 SQL 注入，跨站点脚本攻击，敏感信息泄漏等

3.2.3.3. 测评风险管理

3.2.3.3.1. 测评风险

带宽占用，测试以网络为基础进行，扫描控制台通过网络对被测评对象进行安全测评，因此这种测试方式主要消耗一定的网络带宽资源，并对被测评的对象消耗很小一部分的网络连接的资源，对于其他的资源没有特殊的要求。实际的使用情况表明，网络测试对网络资源和被测评系统的资源占用在 3%-5%之间，并且可以通过修改、配置一定的扫描策略来使这些资源消耗降低至最小。

3.2.3.3.2. 风险规避

① 测试手段的选择

时间选择，为减轻扫描测试对网络和应用系统的影响，对于重要业务的漏洞扫描时间可尽量安排在业务量不大的时段或晚上；

② 测试过程中合理沟通的保证

在测试实施过程中，确定不同阶段的测试人员以及客户方的配合人员，建立直接沟通的渠道，并在测试出现难题的过程中保持合理沟通与配合。

3.2.3.4. 测评内容

3.2.3.4.1. 安全物理环境

安全物理环境测评实施过程涉及物理位置选择、物理访问控制、防盗链和防破坏、防雷击等 10 个方面的安全保护能力，具体测评指标如下表所示：

序号	控制点	条款要求
1	物理位置选择	a)机房场地应选择在具有防震、防风和防雨等能力的建筑内；
		b)机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。
2	物理访问控制	机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。
3	防盗链和防破坏	a)应将设备或主要部件进行固定，并设置明显的不易除去的标识；
		b)应将通信线缆铺设在隐蔽安全处；
		c)应设置机房防盗报警系统或设置有专人值守的视频监控系统。
4	防雷击	a)应将各类机柜、设施和设备等通过接地系统安全接地；
		b)应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。

5	防火	a) 机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；
		b) 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；
		c) 应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。
6	防水和防潮	a) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；
		b) 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透；
		c) 应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。
7	防静电	a) 应采用防静电地板或地面并采用必要的接地防静电措施；
		b) 应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。
8	温湿度控制	应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。
9	电力供应	a) 应在机房供电线路上配置稳压器和过电压防护设备；
		b) 应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求；

		c) 应设置冗余或并行的电力电缆线路为计算机系统供电。
10	电磁防护	a) 电源线和通信线缆应隔离铺设，避免互相干扰；
		b) 应对关键设备实施电磁屏蔽。

3.2.3.4.2. 安全通信网络

安全通信网络测评实施过程涉及网络架构、通信传输及可信验证等 3 个方面的安全保护能力，具体测评指标如下表所示：

序号	控制点	条款要求
1	网络架构	a) 应保证网络设备的业务处理能力满足业务高峰期需要；
		b) 应保证网络各个部分的带宽满足业务高峰期需要；
		c) 应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；
		d) 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段；
		e) 应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。
2	通信传输	a) 应采用校验技术或密码技术保证通信过程中数据的完整性；

		b)应采用密码技术保证通信过程中数据的保密性。
3	可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

3.2.3.4.3. 安全区域边界

安全区域边界测评主要涉及边界防护、访问控制、入侵防范等 6 个方面的安全保护能力，具体测评指标如下表所示：

序号	控制点	条款要求
1	边界防护	a)应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信；
		b)应能够对非授权设备私自联到内部网络的行为进行检查或限制；
		c)应能够对内部用户非授权联到外部网络的行为进行检查或限制；
		d)应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。
2	访问控制	a)应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有

		通信； 
		b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；
		c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；
		d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力；
		e) 应对进出网络的数据流实现基于应用协议和应用内容的访问控制。
3	入侵防范	a) 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；
		b) 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为；
		c) 应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；
		d) 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。

4	恶意代码和垃圾邮件防范	a) 应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新； b) 应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。
5	安全审计	a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等； d) 应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。
6	可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

3.2.3.4.4. 安全计算环境

安全计算环境测评主要涉及身份鉴别、访问控制、安全审计、入侵防范、恶

意码防范等 10 个方面的安全保护能力，具体测评指标如下表所示：

序号	控制点	条款要求
1	身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；
		b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；
		c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；
		d) 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。
2	访问控制	a) 应对登录的用户分配账户和权限；
		b) 应重命名或删除默认账户，修改默认账户的默认口令；
		c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；
		d) 应授予管理用户所需的最小权限，实现管理用户的权限分离；

		e) 应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；
		f) 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；
		g) 应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。
4	安全审计	a） 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
		b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
		c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
		d) 应对审计进程进行保护，防止未经授权的中断
5	入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；
		b) 应关闭不需要的系统服务、默认共享和高危端口；
		c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；
		d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要

		求；  e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞； f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。
6	恶意代码防范	应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。
7	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
8	数据完整性	应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

8	数据保密性	a) 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；
		b) 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。
9	数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；
		b) 应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；
		c) 应提供重要数据处理系统的热冗余，保证系统的高可用性。
10	剩余信息保护	a) 应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；
		b) 应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。
11	个人信息保护	a) 应仅采集和保存业务必需的用户个人信息；
		b) 应禁止未授权访问和非法使用用户个人信息。

3.2.3.4.5. 安全管理中心

安全管理中心测评主要涉及系统管理、审计管理、安全管理及集中管控4个方面的安全保护能力，具体测评指标描述如下表所示：

序号	控制点	条款要求
1	系统管理	a)应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；
		b)应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。
2	审计管理	a)应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；
		b)应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。
3	安全管理	a)应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计；
		b)应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。
4	集中管控	a)应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；

		b)应能够建立一条安全的信息传输路径,对网络中的安全设备或安全组件进行管理;
		c)应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测;
		d)应对分散在各个设备上的审计数据进行收集汇总和集中分析,并保证审计记录的留存时间符合法律法规要求;
		e)应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理;
		f)应能对网络中发生的各类安全事件进行识别、报警和分析。

3.2.3.4.6. 安全管理制度

安全管理制度测评主要涉及安全策略、管理制度、制定和发布、评审和修订4个方面的安全保护能力，具体测评指标如下表所示：

序号	控制点	条款要求

1	安全策略	应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。
2	管理制度	a）应对安全管理活动中的各类管理内容建立安全管理制度；
		b）应对管理人员或操作人员执行的日常管理操作建立操作规程；
		c）应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。
3	制定和发布	a）应指定或授权专门的部门或人员负责安全管理制度的制定；
		b）安全管理制度应通过正式、有效的方式发布，并进行版本控制。
4	评审和修订	应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。

3.2.3.4.7. 安全管理机构

安全管理制度测评主要涉及岗位设置、人员配备、授权和审批、沟通和合作、

审核和检查 5 个方面的安全保护能力，具体测评指标如下表所示：

序号	控制点	条款要求
1	岗位设置	a) 应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权；
		b) 应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；
		c) 应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。
2	人员配备	a) 应配备一定数量的系统管理员、审计管理员和安全管理员等；
		b) 应配备专职安全管理员，不可兼任。
3	授权和审批	a) 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；
		b) 应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；
		c) 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。

4	沟通和合作	a) 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题；
		b) 应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；
		c) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。
5	审核和检查	a) 应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；
		b) 应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；
		c) 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。

3.2.3.4.8. 安全管理人员

安全管理人员测评主要涉及人员录用、人员离岗、安全意识教育和培训、外部人员访问管理 4 个方面的安全保护能力，具体测评指标如下表所示：

序号	控制点	条款要求

1	人员录用	a)应指定或授权专门的部门或人员负责人员录用；
		b)应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核；
		c)应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。
2	人员离岗	a)应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；
		b)应办理严格的调离手续，并承诺调离后的保密义务后方可离开。
3	安全意识教育和培训	a)应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；
		b)应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训；
		c)应定期对不同岗位的人员进行技能考核。
4	外部人员访问管理	a)应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；
		b)应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；
		c)外部人员离场后应及时清除其所有的访问权限；

		d) 获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。

3.2.3.4.9. 安全建设管理

安全建设管理测评主要涉及定级和备案、安全方案设计、产品采购和使用、自行软件开发、外包软件开发等 10 个方面的安全保护能力，具体测评指标如下表所示：

序号	控制点	条款要求
1	定级备案	a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；
		b) 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；
		c) 应保证定级结果经过相关部门的批准；
		d) 应将备案材料报主管部门和相应公安机关备案。
2	安全方案设计	a) 应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；
		b) 应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内

		容应包含密码技术相关内容，并形成配套文件； 
		c）应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。
3	产品采购和使用	a）应确保网络安全产品采购和使用符合国家的有关规定；
		b）应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求；
		c）应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。
4	自行软件开发	a）应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；
		b）应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；
		c）应制定代码编写安全规范，要求开发人员参照规范编写代码；
		d）应具备软件设计的相关文档和使用指南，并对文档使用进行控制；
		e）应保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测；

		f) 应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制；
		g) 应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。
5	外包软件开发	a) 应在软件交付前检测其中可能存在的恶意代码；
		b) 应保证开发单位提供软件设计文档和使用指南；
		c) 应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。
6	工程实施	a) 应指定或授权专门的部门或人员负责工程实施过程的管理；
		b) 应制定安全工程实施方案控制工程实施过程；
		c) 应通过第三方工程监理控制项目的实施过程。
7	测试验收	a) 应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；
		b) 应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。
8	系统交付	a) 应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；
		b) 应对负责运行维护的技术人员进行相应的技能培训；

		c) 应提供建设过程文档和运行维护文档。
9	等级测评	a) 应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；
		b) 应在发生重大变更或级别发生变化时进行等级测评；
		c) 应确保测评机构的选择符合国家有关规定。
10	服务供应商选择	a) 应确保服务供应商的选择符合国家的有关规定；
		b) 应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务；
		c) 应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。

3.2.3.4.10. 安全运维管理

安全管理人员测评主要涉及环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理等 14 个方面的安全保护能力，具体测评指标如下表所示：

序号	控制点	条款要求
1	环境管理	a) 应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；

		b)应建立机房安全管理制度,对有关物理访问、物品带进出和环境安全等方面的管理作出规定;
		c)应不在重要区域接待来访人员,不随意放置含有敏感信息的纸档文件和移动介质等。
2	资产管理	a)应编制并保存与保护对象相关的资产清单,包括资产责任部门、重要程度和所处位置等内容;
		b)应根据资产的重要程度对资产进行标识管理,根据资产的价值选择相应的管理措施;
		c)应对信息分类与标识方法作出规定,并对信息的使用、传输和存储等进行规范化管理。
3	介质管理	a)应将介质存放在安全的环境中,对各类介质进行控制和保护,实行存储环境专人管理,并根据存档介质的目录清单定期盘点;
		b)应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制,并对介质的归档和查询等进行登记记录。
4	设备维护管理	a)应对各种设备(包括备份和冗余设备)、线路等指定专门的部门或人员定期进行维护管理;
		b)应建立配套设施、软硬件维护方面的管理制度,对其维护进行有效的管理,包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等;

		c)信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据应加密；
		d)含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。
5	漏洞风险管理	a)应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补；
		b)应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。
6	网络和系统安全管理	a)应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；
		b)应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；
		c)应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；
		d)应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；

		e)应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容；
		f)应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为；
		g)应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库；
		h)应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据；
		i)应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道；
		j)应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。
7	恶意代码防范管理	a)应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；
		b)应定期验证防范恶意代码攻击的技术措施的有效性。
8	配置管理	a)应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等；

		b)应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。
9	密码管理	a)应遵循密码相关国家标准和行业标准；
		b)应使用国家密码管理主管部门认证核准的密码技术和产品。
10	变更管理	a)应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施；
		b)应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程；
		c)应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。
11	备份与恢复管理	a)应识别需要定期备份的重要业务信息、系统数据及软件系统等；
		b)应规定备份信息的备份方式、备份频度、存储介质、保存期等；
		c)应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。
12	安全事件处置	a)应及时向安全管理部门报告所发现的安全弱点和可疑事件；

		b) 应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；
		c) 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训；
		d) 对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。
13	应急预案管理	a) 应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容；
		b) 应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；
		c) 应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练；
		d) 应定期对原有的应急预案重新评估，修订完善。
14	外包运维管理	a) 应确保外包运维服务商的选择符合国家的有关规定；
		b) 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容；

		c) 应保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确；
		d) 应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等。

3.2.3.5. 成果文档

本阶段的交付物主要有《等级保护测评报告》。

3.2.3.6. 商用密码评估方案

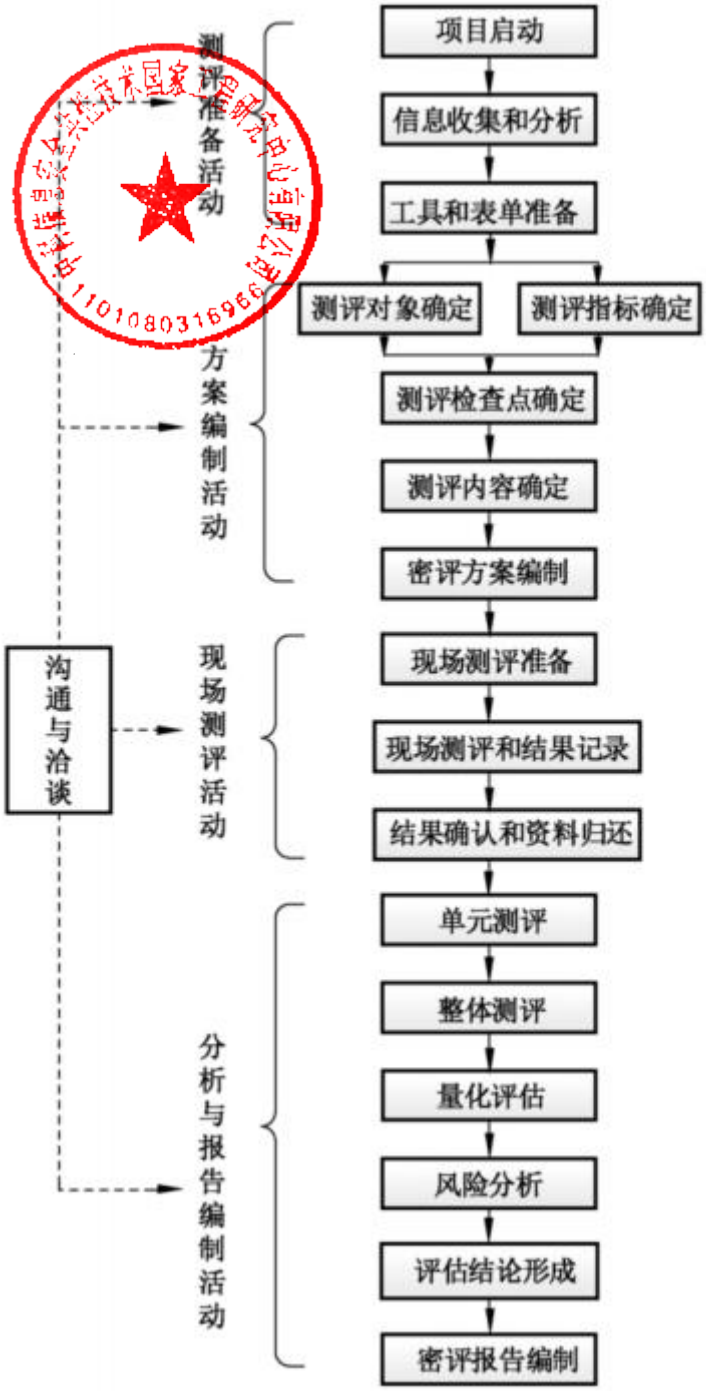
3.2.4. 商用密码测评流程

3.2.4.1. 密评流程

密评工作由四个核心阶段构成，各阶段环环相扣，阶段实施过程中我公司将与北京市文化和旅游局宣传中心（北京市旅游运行监测中心）保持紧密的沟通洽谈：

- 测评准备阶段：奠定基础，完成前期筹备
- 方案编制阶段：明确标准，制定实施蓝图
- 现场测评阶段：实地核查，收集客观证据
- 分析与报告编制阶段：综合研判，形成最终结论

实施流程图如下：


项目启动
信息收集和分析
工具和表单准备
测评对象确定
测评指标确定
测评检查点确定
测评内容确定
密评方案编制
现场测评准备
现场测评和结果记录
结果确认和资料归还
单元测评
整体测评
量化评估
风险分析
评估结论形成
密评报告编制
测评准备活动
方案编制活动
现场测评活动
分析与报告编制活动
沟通与洽谈

3.2.4.2. 各阶段工作内容及交付物

3.2.4.3. 测评准备阶段

阶段目标：顺利启动项目，收集系统信息，准备测评工具与表单，为方案编制提供支撑。

核心任务及交付物

任务名称	输入材料	实施内容	输出成果
项目启动	委托测评协议书、保密协议	1. 组建测评项目组，编制含项目概述、工作依据、技术思路等内容的项目计划书； 2. 与北京市文化和旅游局宣传中心（北京市旅游运行监测中心）确认本次评估信息系统的基本情况	项目计划书
信息收集与分析	调查表格	1. 收集系统总体描述、密码应用方案、定级报告等技术资料； 2. 发放并回收调查表格，分析系统基本信息、行业特征、密码部署等内容； 3. 核实信息准确性，必	完成的调查表格、系统相关技术资料

		要时开展现场调查	
工具和表单准备	调查表格、系统技术资料	1. 校准符合国家密码标准的测评工具； 2. 按需搭建模拟测评环境； 3. 准备现场测评授权书、风险告知书等表单	测评工具清单、各类打印表单

3.2.4.4. 方案编制阶段

阶段目标：基于准备阶段信息，确定测评对象、指标及检查点，形成可指导现场测评的密评方案。

核心任务及交付物

任务名称	输入材料	实施内容	输出成果
测评对象确定	调查表格、系统技术资料	1. 识别系统物理环境、网络拓扑、密码产品等核心组件及密码应用情况； 2. . 协助北京市文化和旅游局宣传中心（北京市旅游运行监测中心）明确核心资产、威胁模型及安全策略； 3. 评估资产价值与	密评方案的测评对象部分

		威胁频率，确定测评对象范围	
测评指标确定	调查表格、GM/T0115、密码应用方案	1. 依据系统定级结果匹配 GM/43206 对应等级指标； 2. 核查密码算法、密钥管理、密码服务等指标适用性	密评方案的测评指标部分
测评检查点确定	系统网络结构、密码产品信息、GM/T0115	1. 明确关键设备配置核查、抓包测试等检查内容； 2. 确定工具接入点与测试路径，规避业务影响	密评方案的测评检查点部分
测评内容确定	调查表格、密评方案相关部分、GM/T0115	1. 结合测评指标与对象，划分可实施的测评单元； 2. 单元测评实施表格	密评方案的单元测评实施部分
密评方案编制	委托协议、项目计划书、上述各部分成果	1. 汇总项目信息、标准依据、工作量估算等内容； 2. 编制含时间安排（避开业务高峰	经评审确认的密评方案文本

		期）、人员分工的实施计划； 3. 内部评审后提交北京市文化和旅游局宣传中心（北京市旅游运行监测中心）确认	

3.2.4.5. 现场测评阶段

阶段目标：依据密评方案开展现场核查，获取真实有效的测评证据，确认测评结果。

核心任务及交付物

任务名称	输入材料	实施内容	输出成果
现场测评准备	现场测评授权书、密评方案、风险告知书	1. 召开首次会，明确测评计划、风险及资源需求； 2. 确认系统数据已备份，北京市文化和旅游局宣传中心（北京市旅游运行监测中心）签署授权书与风险告知书； 3. 更新测评表单与程序	会议记录、更新后的密评方案、签署版授权书/风险告知书
现场测评与结果记录	密评方案、测评记录表格、系统技术资料	1. 通过访谈、文档审查、配置检查、工具测试等方式实施测评； 2. 对已认证密码产品进行符合性核验，必要时联系厂	各类测评结果记录

		商核实； 3. 采集通信/存储数据，分析密码合规性、防攻击能力等 4. 填写测评结果记录表格	
结果确认和资料归还	测评结果记录、工具测试电子记录	1. 汇总记录，补充遗漏或需验证的内容 2. 召开结束会，与北京市文化和旅游局宣传中心（北京市旅游运行监测中心）确认测评结果； 3. 归还借阅资料，恢复现场环境	经北京市文化和旅游局宣传中心（北京市旅游运行监测中心）确认的各类测评结果记录

3.2.4.6. 分析与报告编制阶段

阶段目标：基于现场测评证据，通过多维度分析形成评估结论，编制规范密评报告。

核心任务及交付物

任务名称	输入材料	实施内容	输出成果
单元测评	确认后的测评记	1. 对照标准判定	密评报告的单元

	录、GM/T0115 	各测评对象结果（符合/不符合/部分符合/不适用） 2. 汇总单元测评结果符合、基本符合、不符合	测评部分
整体测评	单元测评部分成果	1. 分析“部分符合/不符合”项与其他单元/层面的关联影响； 2. 修正各测评对象结果，统计整体符合情况	密评报告的单元测评结果修正部分
量化评估	单元测评与整体测评成果	1. 计算测评对象、单元、安全层面及整体得分 2. 评价有效保护措施与安全问题	密评报告的量化评估及总体评价部分
风险分析	调查表格、量化评估成果、风险评估标准	1. 分析安全问题被威胁利用的可能性（高/中/低）； 2. 评估对业务信息安全的影响程度综合判定系统整体风险等级	密评报告的风险分析部分

评估结论形成	综合得分、风险分析成果	1. 符合：无安全问题，综合得分 100 分； 2. 基本符合：有安全问题但无高风险，不低于 60 阈值； 3. 不符合：存在高风险或得分低于 60	密评报告的评估结论部分
密评报告编制	调查表格、密评方案、上述各部分成果	1. 按标准模板编制报告（含概述、测评过程、结论、改进建议等）； 2. 列出测评文档清单与结果判定情况； 3. 内部评审后签发提交北京市文化和旅游局宣传中心（北京市旅游运行监测中心）	经评审确认的密评报告

3.2.5. 商用密码测评内容与方式

3.2.5.1. 测试内容

3.2.5.1.1. 通用测试内容

3.2.5.1.1.1. 密码算法评估

测评指标	信息系统中使用的密码算法符合法律、法规的规定和密码相关国家标准、行业标准的有关要求(适用于第一级到第四级)。
测评对象	信息系统中使用的密码算法。
测评实施	了解信息系统中使用的密码算法的名称、用途、何处使用、执行设备及其实现方式(软件、硬件或固件),核查信息系统中使用的密码算法是否符合法律法规的规定和密码相关国家标准、行业标准的有关要求。

3.2.5.1.1.2. 密码技术评估

测评指标	信息系统中使用的密码技术应遵循密码相关国家标准和行业标准(适用于第一级到第四级)
测评对象	信息系统中使用的密码技术
测评实施	了解信息系统中使用的密码技术的名称、用途、何处使用、执行设备及其实现方式(软件、硬件或固件),核查信息系统中使用的密码技术是否符合法律法规的规定和密码相关国家标准、行业标准的有关要求。

3.2.5.1.1.3. 密码产品评估

测评指标	信息系统中使用的密码产品符合法律法规和密码相关国家标准、行业标准的相关要求(适用于第级到第四级)。 ✓ 信息系统中使用的密码产品如遵循密码模块相关标准,则应: ✓ 达到密码模块安全等级一级及以上安全要求(适用于第二级); ✓ 达到密码模块安全等级二级及以上安全要求(适用于第三级): ✓ 达到密码模块安全等级三级及以上安全要求(适用干第四级)
测评对象	信息系统中使用的密码产品。
测评实施	了解信息系统中使用的密码产品的型号和版本等配置信息,核查密码产品是否经商用密码认证机构认证合格,并核查密码产品的使用是否满足其安全运行的条件,例如其安全策略或使用手册说明的部署条件。遵循了密码模块相关标准的密码产品,还要核查其是否满足密码模块相应安全等级及以上安全要求。

3.2.5.1.1.4. 密码服务

测评指标	信息系统中使用的密码服务符合法律法规的相关要求(适用于第一级到第四级),
测评对象	信息系统中使用的密码服务。
测评实施	核查信息系统中使用的密码服务是否符合法律法规的相关要求。

3.2.5.1.1.5. 密钥管理评估

测评指标	本单元测评指标如下: 信息系统密钥管理使用的密码产品、密码服务符合法律法规和密码相关国家标准、行业标准的要求(适用于第一级到第四级); 信息系统密钥管理应符合密码相关国家标准和行业标准的要求(适用于第一级到第四级)。
测评对象	信息系统密钥管理使用的密码产品、密码服务以及密钥管理实现
测评实施	本单元测评实施如下: 核查密钥管理使用的密码产品、密码服务是否满足密码产品和密码服务的要求:

	核查信息系统密钥管理实现是否安全、正确、有效。例如:非公开密钥是否能被非授权访问、使用、泄露、修改和替换,公开密钥是否能被非授权修改和替换。

3.2.5.1.2. 物理和环境安全

3.2.5.1.2.1. 测评内容

序号	测评指标	测评对象	测评方式	测评实施工作单元描述
1	宜采用密码技术进行物理访问身份鉴别,保证重要区域进入人员身份的真实性。	电子门禁系统	访谈和文档审查、实地查看或配置检查、工具测试	访谈物理安全负责人,并查阅相关技术文档,了解电子门禁系统的身份鉴别措施;核查电子门禁系统是否具有商密型号证书;查验受测电子门禁系统是否采用密码技术来确保进入重要区域人员身份鉴别信息的真实性,并截取相关关键数据,作为证据材料。
2	宜采用密码技术保证电子门禁系统进出记录数据的存储完整性。	电子门禁系统	访谈和文档审查、实地查看或配置检查、工具测试	访谈物理安全负责人,并查阅相关技术文档,了解电子门禁系统进出记录完整性保护措施;核查电子门禁系统是否具有商密型号证书;查验受测电子门禁系统是否采用密

序号	测评指标	测评对象	测评方式	测评实施工作单元描述
				码技术的完整性服务来确保电子门禁系统进出记录的完整性，并截取相关关键数据，作为证据材料。
3	宜采用密码技术保证视频监控音像记录数据的存储完整性。	视频监控系统	访谈和文档审查、配置检查或工具测试	访谈系统管理员，并查看技术文档中关于视频监控系统视频监控音像记录数据的完整性保护技术及实现机制；查验受测视频监控系统中密码应用的正确性和有效性、是否使用国家密码管理局认可的密码算法、身份鉴别协议；并截取相关关键数据，作为证据材料。

3.2.5.1.2.2. 配合需求

序号	配合项目	需求说明
1	提供详细技术证明文件	提供商密产品型号证书和/或商用密码测评机构出具的合格检测报告、国家密码管理部门颁发的密码服务许可证等合规性证明材料。
2	访谈和技术文档审查	提供门禁及视频监控系统产品技术文

		档；产品供应商介绍产品相关实现技术、完整性保护实现技术。
3	门禁卡测试	提供门禁卡用于测试。

3.2.5.1.3. 网络和通信安全

3.2.5.1.3.1. 测评内容

序号	测评指标	测评对象	测评方式	测评实施工作单元描述
1	应采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性。	终端与 SSLVPN 之间的通信	访谈和文档审查、实体查看或配置检查	查看设计文档中身份鉴别采用的密码技术及实现机制；查验通信主体身份鉴别功能的正确性和有效性；并截取相关关键数据，作为证据材料；查看身份鉴别机制密码算法、密码协议是否符合有关密码国家标准和行业标准；查看密码设备是否获得国家密码管理部分颁发的密码产品型号证书。并截取相关关键数据，作为正确材料。
2	宜采用密码技术保证通信过程中数据的完整性。	终端与 SSLVPN 之间的通信	访谈和文档审查、实体查看、配置检查或工具测试	查看技术文档中关于通信过程中数据采用的完整性保护技术及实现机制；查

序号	测评指标	测评对象	测评方式	测评实施工作单元描述
				验通信过程中数据完整性保护的正确性和有效性、使用的密码算法身份鉴别协议是否得到国家密码管理局认可，相关网络安全设备是否经过了国家密码管理部门核准；并截取相关关键数据，作为证据材料。
3	应采用密码技术保证通信过程中重要数据的机密性。	终端与 SSLVPN 之间的通信	访谈和文档审查、实体查看、配置检查或工具测试	查看技术文档中网络通信中敏感数据采用的机密性保护技术及实现机制；查验受测通信过程中数据机密性保护的正确性和有效性，是否使用国家密码管理局认可的密码算法、身份鉴别协议，相关网络安全设备是否经过了国家密码管理部门核准；并截取相关关键数据，

序号	测评指标	测评对象	测评方式	测评实施工作单元描述
				作为证据材料。
4	宜采用密码技术保证网络边界访问控制信息的完整性。	终端与 SSLVPN 之间的通信	访谈和文档审查、实体查看、配置检查或工具测试	查看系统是否使用国家密码管理局认可的密码算法对网络边界和系统资源访问控制信息进行完整性保护；并截取相关关键数据，作为证据材料；密码设备是否获得国家密码管理部门颁发的密码产品型号证书。
5	可采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入的设备身份真实性。	终端与 SSLVPN 之间的通信	访谈和文档审查、实体查看、配置检查或工具测试	查看技术文档，系统是否对外部连接到内部网络的设备进行了接入认证，接入认证的具体实现方式。

3.2.5.1.3.2. 配合需求

序号	配合项目	需求说明
1	提供详细技术证明文件	提供商密产品型号证书和/或商用密码测评机构出具的合格检测

		报告、国家密码管理部门颁发的密码服务许可证等合规性证明材料。
2	访谈和技术文档审查	1、配合访谈进行运维网络中身份鉴别、通信数据传输等采用的密码技术及实现机制情况的了解； 2、提供运维网络中实现身份鉴别、通信数据传输等采用的密码技术及实现机制相关的技术文档。
3	网络通信审查	1、提供网络交换机、终端PC、运维网络的接入端口，用于接入工具审查通信流量； 2、协助查验运维网络访问控制信息的完整性保护措施及所用密码算法合规性正确性情况。

3.2.5.1.4. 设备和计算安全

3.2.5.1.4.1. 测评内容

序号	测评指标	测评对象	测评方式	测评实施工作单元描述
1	应采用密码技术对登录设备的用户进行身份鉴别，	堡垒机、网御星云SSLVPN、CFCA签名验签服务	访谈和文档审查、配置检查或工具测试	结合设计文档，访谈系统管理员和数据库管理员，了解用户

序号	测评指标	测评对象	测评方式	测评实施工作单元描述
	保证用户身份的真实性。	器、应用服务器、启明天旬终端、Oracle 数据库		在本地登录核心数据库或核心服务器时，系统对用户实施身份鉴别的过程中是否采用密码技术对主机标识信息进行密码保护，并明确其所采用的密码技术；查验主机身份鉴别机制中所采用的加密算法是否符合法规和密码相关标准的要求；查验相关密码功能是否止确有效；并截取相关关键数据，作为证据材料。
2	远程管理设备时，应采用密码技术建立安全的信息传输通道。	堡垒机、网御星云 SSLVPN、CFCA 签名验签服务器、应用服务器、启明天旬终端、Oracle 数据库	访谈和文档审查、配置检查或工具测试	访谈系统管理员，并查阅相关技术文档，了解远程管理时，所使用密码技术；查验远程管理所采用的密码机制是否正确有效；并截取相关关键数据，作为证据材

序号	测评指标	测评对象	测评方式	测评实施工作单元描述
				料。
3	宜采用密码技术保证系统资源访问控制信息的完整性。	堡垒机、网御星云 SSLVPN、CFCA 签名验签服务器、应用服务器、启明天旬终端、Oracle 数据库	访谈和文档审查、配置检查或工具测试	查看设计文档中访问控制信息完整性保护密码技术及实现机制；查验系统是否使用以及使用何种密码技术对系统资源访问控制信息进行完整性保护：查看是否使用国家密码管理局认可的密码算法；密码设备是否获得国家密码管理部门颁发的密码产品型号证书；并截取相关关键数据，作为证据材料。
4	宜采用密码技术保证设备中的重要信息资源安全标记的完整性。	堡垒机、网御星云 SSLVPN、CFCA 签名验签服务器、应用服务器、启明天旬终端、Oracle 数据	访谈和文档审查、配置检查或工具测试	访谈系统负责人是否设置了敏感标记，若系统设置了敏感标记，查看设计文档中敏感标记完整性保护密码技术及实

序号	测评指标	测评对象	测评方式	测评实施工作单元描述
		库		现机制；查验系统是否使用以及使用何种密码技术对重要信息命案标记进行完整性保护：查看是否使用国家密码管理局认可的密码算法；密码设备是否获得国家密码管理部门颁发的密码产品型号证书；并截取相关关键数据，作为证据材料。
5	宜采用密码技术保证日志记录的完整性。	堡垒机、网御星云 SSLVPN、CFCA 签名验签服务器、应用服务器、启明天旬终端、Oracle 数据库	访谈和文档审查、配置检查或工具测试	查看设计文档中日志信息完整性保护密码技术及实现机制；查验完整性保护功能的正确性和有效性；并截取相关关键数据，作为证据材料。
6	宜采用密码技术对重要可执行程序进行完整性保	堡垒机、网御星云 SSLVPN、CFCA 签名验签服务	访谈和文档审查、配置检查或工具测试	查看设计文档中重要可执行程序完整性保护密码技术及

序号	测评指标	测评对象	测评方式	测评实施工作单元描述
	护，并对其来源进行真实性验证。	器、应用服务器、启明天旬终端、Oracle 数据库		实现机制；查验系统是否使用以及使用何种密码技术对重要可执行程序进行完整性保护：查看是否使用国家密码管理局认可的密码算法；密码设备是否获得国家密码管理部门颁发的密码产品型号证书；并截取相关关键数据，作为证据材料。

3.2.5.1.4.2. 配合需求

序号	配合项目	需求说明
1	访谈和技术文档审查	提供技术文档，配合访谈进行业务系统登录核心数据库或应用服务器身份鉴别、访问控制信息完整性、日志完整性、敏感标识完整性等采用的密码技术及实现机制情况的了解。
2	远程管理审查	提供网络交换机、远程管理的接入端口，用于接入工具审查

		远程管理所采用密码机制的完整性和有效性。

3.2.5.1.5. 应用和数据安全

3.2.5.1.5.1. 测评内容

序号	测评指标	测评方式	测评实施工作单元描述
1	应采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性.	访谈和文档审查、配置检查或工具测试	结合设计文档访谈应用系统管理员，了解受检应用系统在对用户实施身份鉴别的过程中是否使用了密码技术来实现对假冒的应用程序身份标识信息进行有效鉴别，并明确其所采用的密码技术和安全设备；查验应用系统用户身份鉴别过程是否使用国家密码管理局认可的密码算法；专用安全设备是否经过了国家密码管理部门核准；查验相关密码功能是否正确、有效；并截取相关关键数据，作为证据

序号	测评指标	测评方式	测评实施工作单元描述
			材料。
2	宜采用密码技术保证信息系统应用的访问控制信息的完整性。	访谈和文档审查、配置检查或工具测试	审阅技术文档，访谈系统管理员，了解系统如何对业务应用系统访问控制策略、数据库表访问控制信息和重要信息资源敏感标记等重要信息进行完整性保护；了解是否使用密码技术对重要信息进行完整性保护；查验系统是否使用国家密码管理局认可的密码算法，密码协议；设备是否经过了国家密码管理部门核准；相关密码功能是否正确有效；并截取相关关键数据，作为证据材料。

序号	测评指标	测评方式	测评实施工作单元描述
3	宜采用密码技术保证信息系统应用的重要信息资源安全标记的完整性。	访谈和文档审查、配置检查或工具测试	访谈系统管理员，信息系统是否设置重要信息资源安全标记，了解系统如何对重要信息资源安全标记进行完整性保护；了解是否使用密码技术对重要信息进行完整性保护；查验系统是否使用国家密码管理局认可的密码算法，密码协议；设备是否经过了国家密码管理部门核准；相关密码功能是否正确有效；并截取相关关键数据，作为证据材料。
4	应采用密码技术保证信息系统应用的重要数据在传输过程中的机密性。	访谈和文档审查、配置检查或工具测试	查看相关技术文档，了解业务系统中重要数据在传输过程中的机密性保护技术及实现机

序号	测评指标	测评方式	测评实施工作单元描述
			制；查验业务系统中重要数据在传输过程中机密性保护的正确性和有效性，是否使用国家密码管理局认可的密码算法、身份鉴别协议；并截取相关关键数据，作为证据材料。
5	应采用密码技术保证信息系统应用的重要数据在存储过程中的机密性。	访谈和文档审查、配置检查或工具测试	查看相关技术文档，了解业务系统中重要数据在存储过程中的机密性保护技术及实现机制；查验业务系统中重要数据在存储过程中机密性保护的正确性和有效性，是否所使用国家密码管理局认可的密码算法、身份鉴别协议是否符合有关密码国家标准和行业标准；并截

序号	测评指标	测评方式	测评实施工作单元描述
			取相关关键数据，作为证据材料。
6	宜采用密码技术保证信息系统应用的重要数据在传输过程中的完整性。	访谈和文档审查、配置检查或工具测试	查看相关技术文档，了解业务系统中重要数据在传输过程中的完整性保护技术及实现机制；查验业务系统中重要数据在传输过程中完整性保护的正确性和有效性，是否使用国家密码管理局认可的密码算法、身份鉴别协议；并截取相关关键数据，作为证据材料。
7	宜采用密码技术保证信息系统应用的重要数据在存储过程中的完整性。	访谈和文档审查、配置检查或工具测试	查看相关技术文档，了解业务系统中重要数据在存储过程中的完整性保护技术及实现机制；查验业务系统

序号	测评指标	测评方式	测评实施工作单元描述
			中重要数据在存储过程中完整性保护的正确性和有效性，是否使用国家密码管理局认可的密码算法、身份鉴别协议；并截取相关关键数据，作为证据材料。
8	在可能涉及法律责任认定的应用中，宜采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性。	访谈和文档审查、配置检查或工具测试	审阅技术文档，访谈系统管理员信息系统的数据流转情况，确认这些数据的流转过程，了解业务系统中流转数据原发和接收的实现机制；查验业务系统中流转数据通过哪些技术保证这些数据以及数据原发行为和接收行为的不可否认性，是否使用国家密码管理局认可的密码算法、身份鉴别协议；

序号	测评指标	测评方式	测评实施工作单元描述
			并截取相关关键数据，作为证据材料。

3.2.5.1.5.2. 配合需求

序号	配合项目	需求说明
1	访谈和技术文档审查	配合访谈进行业务系统中身份鉴别、重要数据传输、数据安全存储、日志记录完整性、访问控制信息完整性等采用的密码技术及实现机制情况的了解。
2	重要数据传输审查	提供网络交换机、SSLVPN的接入端口，用于接入工具审查通信流量。

3.2.5.1.6. 安全制度

3.2.5.1.6.1. 测试内容

单元	测评指标	测评对象	测评方式	测评实施工作单元描述

单元	测评指标	测评对象	测评方式	测评实施工作单元描述
制度	应具备密码应用安全管理制度，包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度。	安全管理制度文档	访谈和文档审查	核查各项安全管理制度、安全操作规范和配套的操作规程是否覆盖包括密码建设、运维、人员、设备、密钥等密码管理相关内容。
	应根据密码应用方案建立相应密钥管理规则。	安全管理制度文档	访谈	1）访谈安全主管是否对系统使用到的产品建立对应的密钥管理规则。
			文档审查	2）核查安全管理制度中关于密钥管理规则是否完善。
	应对管理人员或操作人员执行的日常管理操作建立操作规程。	安全管理制度文档	访谈	1）访谈安全主管是否有密码产品的管理人员或操作人员的操作规程的安全管理制度。
			文档审查	2）安全管理制度中

单元	测评指标	测评对象	测评方式	测评实施工作单元描述
				内容是否包含了管理人员或操作人员执行日常管理操作的操作规程。
	应定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定，对存在不足或需要改进之处进行修订。	安全管理制度文档	访谈	1）访谈安全主管是否具有管理制度发布流程。
			文档审查	2）核查是否具有管理制度发布文件。
	应明确相关密码应用安全管理制度和操作规程的发布流程并进行版本控制。	安全管理制度文档	访谈	1）访谈安全主管是否定期对密码安全管理制度体系的合理性和适用性进行审定。
			文档审查	2）核查是否具有安全管理制度的审定或论证记录，如果对制度做过修订，核查是否有修订版本的安全管理制

单元	测评指标	测评对象	测评方式	测评实施工作单元描述
				度。
	应具有密码应用操作规程的相关执行记录并妥善保存。	安全管理制度文档	访谈	1）访谈安全主管是否有密码操作的相关记录。
			文档审查	2）核查密码应用操作规程的相关执行记录。

3.2.5.1.6.2. 配合需求

单元	配合项目	需求说明
制度	制度制定	（1）配合访谈进行安全管理制度体系情况的了解； （2）提供信息安全总体方针政策的文件、与信息安全相关的管理制度和操作规程； （3）提供安全管理制度认证和评审的记录。
	评审和修订	（1）配合访谈进行安全管理制度体系、制度制订与发布、评审和修订相关内容的了解； （2）提供安全管理制度定期评审修订的记录。
	制度发布	（1）配合访谈进行制度发布情况的了解；

		（2）提供安全管理制度收发文记录。

3.2.5.1.7. 人员管理

3.2.5.1.7.1. 测试内容

单元	测试指标	测评对象	测试方式	测试实施工作单元描述
人员	相关人员应了解并遵守密码相关法律法规、密码应用安全管理制度。	密码相关人员	访谈	1）随机抽查 1-2 位与密码相关的人员及系统负责人进行访谈，确认是否了解并遵守商用密码相关法律法规。
	应建立密码应用岗位责任制度，明确各岗位在安全系统中的职责和权限： 1）根据密码应用的实际情况，设置密钥管理员、密码安全审计员、密码操作员等关键安全岗位； 2）对关键岗位建立多人共管机制； 3）密钥管理、密码安全审计、密码操作人员职责互相制约	制度文档、记录文档	访谈	1）访谈信息安全主管是否建立的密码应用岗位责任制度，是否设置了密钥管理员、密码操作人员、关键岗位是否实行多人共管、相关设备和系统的管理和使用账号是否存在多人共用的情况。
			文档审查	2）核查安全管理制度类文档是否明确了相关人员在密码

	互相监督，其中密钥管理员岗位不可与密码审计员、密码操作员等关键安全岗位兼任； 4）相关设备与系统的管理和使用账号不得多人共用。			设备管理与密钥系统管理中的职责和权限。
				3）核查人员配备文档是否针对关键岗位配备多人。
				4）核查记录表单类文档是否明确配备了密钥管理、安全审计、密码设备操作岗位人员，是否对关键岗位建立多人共管机制，密钥管理、密码安全审计、密码操作人员等关键岗位是否互相制约互相监督，相关设备与系统的管理和使用账号是否多人共用。
	应建立上岗人员培训制度，对于涉及密码的操作和管理的人员进行专门培训，	制度文档、记录文档	访谈	1）访谈信息安全主管是否对涉及密码的操作和管理的人员进行专门培训。

	确保其具备岗位所需专业技能。		文档审查	2)核查记录表单类文档是否有对涉及密码的操作和管理的人员进行培训的培训记录。
	应定期对密码应用安全岗位人员进行考核。	制度文档、记录文档	访谈和文档审查	1)核查是否建立了人员考核制度，是否定期进行岗位人员考核。
	应建立关键人员保密制度和调离制度，签订保密合同，承担保密义务。	制度文档、记录文档	文档审查	1)核查人员关键岗位人员保密制度和调离制度等。
			文档审查	2)核查关键岗位人员是否签订了保密合同，承担保密业务。

3.2.5.1.7.2. 配合需求

单元	配合项目	需求说明
人员	了解遵守法律法规	(1)配合访谈进行商用密码相关法律法规的了解； (2) 商用密码相关法律法规的文档。
	正确使用密码产品	(1) 提供商用密码产品操作手册；

		(2)配合访谈进行商用密码产品使用方法的了解。
	关键岗位设置	(1)配合访谈提供信息安全管理岗位的划分情况； (2) 提供安全管理制度类文档； (3) 提供配备各岗位人员的记录表单。
	岗位、职责与权限	(1)配合访谈提供信息安全管理岗位责任制度、职责与权限情况； (2) 提供安全管理制度类文档。
	制约与监督	(1) 配合访谈进行密钥管理、安全审计、密码操作人员职责、互相制约机制的了解； (2) 提供相关制度，相关设备与系统的管理和使用的账号记录。
	人员考核	(1)配合访谈进行人员岗位考核情况的了解； (2) 提供定期考核记录。
	人员培训	(1)配合访谈进行涉及密码的操作和管理以及密钥管理培训情况的了解； (2)提供涉及密码的操作和管理以及密钥管理、安全教育的培训计划和记录。
	关键岗位保密制度	(1)配合访谈进行保密制度和调离制

		度的了解； (2)提供岗位人员保密制度和调离制度，保密合同。

3.2.5.1.8. 建设运行

3.2.5.1.8.1. 测试内容

单元	测试指标	测评对象	测试方式	测试实施工作单元描述
建设运行	应依据密码相关标准和密码应用需求，制定密码应用方案。	实施方案、评审文档	文档审查	核查在规划阶段，是否依据密码相关标准和密码应用需求，制定密码应用方案。
	应根据密码应用方案，确定系统涉及的密钥种类、体系及其生命周期环节，各环节安全管理要求参照《信息安全技术信息系统密码应用基本要求》附录A。	实施方案、评审文档	文档审查	查看密码应用方案中是否包含系统涉及的密钥种类、体系及生命周期等内容。
	应按照应用方案	实施方案	文档审查	检查是否按照国家相

	实施建设。			关标准，制定实施方案，方案内容应包括但不少于信息系统概述、安全需求分析、商用密码系统设计方案、商用密码产品清单（包括产品资质、功能及性能列表和产品生产单位等）、商用密码系统安全管理与维护策略、商用密码系统实施计划等。
	投入运行前应进行密码应用安全性评估，评估通过后系统方可正式运行。	资质文档	访谈和资质核查	检查信息系统投入运行前，责任单位是否进行了密码安全性评估，是否具有评估报告。
	在运行过程中，应严格执行既定的密码应用安全管理制度，应定期开展密码应用安全性评估及攻防对抗演习，并根据评估结果进行整改。	评审文档	访谈和资质核查	检查信息系统投入运行后，责任单位是否定期委托测评机构开展密码应用安全性评估，是否具有评估报告。有重大安全隐患的，是否停止系统运行，制定整改方案，整改完成并通过评估

				后方可投入运行。

3.2.5.1.8.2. 配合需求

单元	配合项目	需求说明
建设运行	项目规划立项	（1）提供安全规划设计类文档、安全建设方案评估文档、项目立项规划文档、评审报告。
	制定实施方案	（1）通过访谈了解方案内容，应包括但不少于信息系统概述、安全需求分析、商用密码系统设计方案、商用密码产品清单（包括产品资质、功能及性能列表和产品生产单位等）、商用密码系统安全管理与维护策略、商用密码系统实施计划等； （2）提供密码应用安全评估文档、项目安全建设验收文档、设备采购文件。
	应选用的密码产品、密码服务的	（1）通过访谈了解选用的经国家密码管理部门核准的密码产品、许可的密码服务； （2）提供密码应用安全评估文档、项目安全建设验收文档。
	运行前应进行安全性评估	（1）通过访谈了解信息系统投入运行前的安全性评估情况；

		（2）提供密码应用安全评估文档。
	运行后定期评估和整改	（1）通过访谈了解信息系统投入运行后的安全性评估及整改情况； （2）提供密码应用安全评估文档。

3.2.5.1.9. 应急管理

3.2.5.1.9.1. 测试内容

单元	测试指标	测评对象	测试方式	测试实施工作单元描述
应急	应制定密码应用应急策略，做好应急资源准备，当密码应用安全事件发生时，应立即启动应急处置措施，结合实际情况及时处置。	应急方案、记录文档	文档审查	检查应急预案及相关管理制度文档，是否根据安全事件等级制定了相应的应急预案及管理制度，明确了应急事件处理流程及其他管理措施，并遵照执行。如有安全事件发生，检查是否有相应的处置记录。
	事件发生后，应及时向信息系统主管部门进行报告。	记录文档	访谈和文档审查	检查安全事件发生后，是否及时向信息系统的上级主管部门进行报告。

	事件处置完成后，应及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况。	记录文档	访谈和文档审查	检查安全事件完成后，是否及时向同级的密码主管部门报告事件发生情况及处置情况。

3.2.5.1.9.2. 配合需求

单元	配合项目	需求说明
应急	制定应急预案	（1）配合访谈进行应急预案管理的情况的了解； （2）提供不同事件的应急预案；
	应急响应	（1）提供应急预案培训、演练、审查记录； （2）提供上级主管部门报告。
	完成后的处置	（1）配合访谈进行安全事件处置情况的了解； （2）提供安全事件报告和处置管理制度； （3）提供安全事件处理过程记录。

3.2.5.2. 技术测试方式

3.2.5.2.1. 物理和环境安全测评

序号	测评对象	测评方式	说明
1	机房	☑访谈 ☑文档审查 ☑实地查看 ☑配置检查 ☑工具测试	针对进出机房人员的身份鉴别、进出记录完整性、视频监控文件完整性进行测评。

3.2.5.2.2. 网络和通信安全测评

序号	测评对象	测评方式	说明
1	外部客户端与被测系统的通信信道	☑访谈 ☑文档审查 ☑实地查看 ☑配置检查 ☑工具测试	针对外部网络与被测系统通信信道的身份鉴别、访问控制信息完整性、传输过程中的机密性、完整性进行测评。
2	集中管理通道	☑访谈 ☑文档审查 ☑实地查看	针对运维方式为集中运维的情况下对网络层的数据传输安全进行测评。

		☑配置检查 ☑工具测试	

3.2.5.2.3. 设备和计算机安全测评

序号	测评对象	测评方式	说明
1	密码产品/设备	☑访谈 ☑文档审查 ☐实地查看 ☑配置检查 ☑工具测试	
2	通用服务器	☑访谈 ☑文档审查 ☑实地查看 ☑配置检查 ☑工具测试	
3	其他涉及设备	☑访谈 ☑文档审查 ☑实地查看 ☑配置检查 ☑工具测试	

4	数据库	☑访谈 ☑文档审查 ☑实地查看 ☑配置检查 ☑工具测试	

3.2.5.2.4. 应用和数据安全测评

序号	测评对象	测评方式	说明
1	应用系统	☑访谈 ☑文档审查 □实地查看 ☑配置检查 ☑工具测试	针对被测系统范围内的所有相关子系统的身份鉴别、访问控制信息完整性、重要信息资源安全标记完整性、重要数据传输机密性、重要数据存储机密性、重要数据传输完整性、重要数据存储完整性、不可否认性进行测评。

3.2.5.3. 管理测评方式

序号	测评单元	测评对象	测评方式	说明
1	管理制度	管理体系（包括安全管理制度类文档、密码应用方案、	☑访谈 ☑文档审查	包括安全管理制度类文档、密码应用方案、密钥管理制度及策略

		密钥管理制度及策略类文档、操作规程类文档、记录表单类文档、系统相关人员）		类文档、操作规程类文档、记录表单类文档、系统相关人员
2	人员管理	管理体系（包括安全管理制度类文档、记录表单类文档、系统相关人员）	☑访谈 ☑文档审查	包括安全管理制度类文档、记录表单类文档、系统相关人员
3	建设运行	密码应用方案、密钥管理制度及策略类文档、密码实施方案、密码应用安全性评估报告、密码应用安全管理制度、攻防对抗演习报告、整改文档	☑访谈 ☑文档审查	密码应用方案、密钥管理制度及策略类文档、密码实施方案、密码应用安全性评估报告、密码应用安全管理制度、攻防对抗演习报告、整改文档
4		管理体系（包括安全管理制度类文档、记录表单类文档、系统相关人员）	☑访谈 ☑文档审查	包括安全管理制度类文档、记录表单类文档、系统相关人员
5	应急处置	管理体系（包括密码应用应急处置方案、应急处置记录类文档、安全事件发生情况及处置情	☑访谈 ☑文档审查	包括密码应用应急处置方案、应急处置记录类文档、安全事件发生情况及处置情况报告、系统相关人员

		况报告、系统相关人员）		

3.2.5.4. 项目成果交付物

《商业密码应用安全性评估整改建议》、《商业密码安全性评估报告》

3.2.6. 技术测试使用到的工具说明

3.2.6.1. 物理和环境安全测评工具

测评单元	测评内容	测评工具推荐建议	工具说明
身份鉴别	采用密码技术进行物理访问身份鉴别，保证重要区域进入人员身份的真实性；	密码算法校验工具 APDU 报文分析工具 密码应用缺陷验证工具	1）密码算法校验工具可用于校验身份鉴别所使用密码算法的合规性、正确性； 2）APDU 报文分析工具可用于分析门禁卡与读卡器之间的 APDU 报文； 3）密码应用缺陷验证工具可用于识别、利用身份鉴别存在的密码应用缺陷，综合分析、确定密码应用缺陷风险等级。
电子门禁	采用密码技术保证电子门禁系统进出记录	密码算法校验工具源代码审计工具	1）密码算法校验工具可用于校验电子门禁

记录数据 存储完整性	数据的存储完整性；	接口测试工具	记录数据存储完整性保护所使用密码算法的合规性、正确性； 2）源代码审计工具可用于分析电子门禁记录数据存储完整性保护相关代码； 3）接口测试工具可用于测试密码相关接口的安全性。
视频监控 记录数据 存储完整性	采用密码技术保证视频监控音像记录数据的存储完整性。	密码算法校验工具 源代码审计工具 接口测试工具	1）密码算法校验工具可用于校验视频监控记录数据存储完整性保护所使用密码算法的合规性、正确性； 2）源代码审计工具可用于分析视频监控记录数据存储完整性保护相关代码； 3）接口测试工具可用于测试密码相关接口的安全性。

3.2.6.2. 网络和通信安全测评工具

测评单元	测评内容	测评工具推荐建议	工具说明

身份鉴别	采用密码技术对通信实体进行单向或双向身份鉴别，保证通信实体身份的真实性；	端口扫描工具 数字证书校验工具协议分析工具 密码算法校验工具密码应用缺陷验证工具	1）端口扫描工具可用于探测和识别被测信息系统中相关设备所对应的端口服务开启情况； 2）数字证书校验工具可用于校验数字证书有效性； 3）协议分析工具可用于分析协议类型、协议版本、密钥交换过程、密码算法等； 4）密码算法校验工具可用于校验身份鉴别所使用密码算法的合规性、正确性； 5）密码应用缺陷验证工具可用于识别、利用身份鉴别存在的密码应用缺陷，综合分析、确定密码应用缺陷风险等级。

通信数据完整性	采用密码技术保证通信过程中数据的完整性；	端口扫描工具 协议分析工具 密码算法校验工具密码应用缺陷验证工具	1）端口扫描工具可用于探测和识别被测信息系统中相关设备所对应的端口服务开启情况； 2）协议分析工具可用于分析协议类型、协议版本、密钥交换过程、密码算法等； 3）密码算法校验工具可用于校验通信数据完整性保护所使用密码算法的合规性、正确性； 4）密码应用缺陷验证工具可用于识别、利用通信过程中数据的完整性保护存在的密码应用缺陷，综合分析、确定密码应用缺陷风险等级。

通信过程中重要数据的机密性	采用密码技术保证通信过程中重要数据的机密性；	端口扫描工具 协议分析工具 密码算法校验工具密码应用缺陷验证工具	1）端口扫描工具可用于探测和识别被测信息系统中相关设备所对应的端口服务开启情况； 2）协议分析工具可用于分析协议类型、协议版本、密钥交换过程、密码算法等； 3）密码算法校验工具可用于校验通信过程中重要数据的机密性保护所使用密码算法的合规性、正确性； 4）密码应用缺陷验证工具可用于识别、利用通信过程中重要数据的机密性保护存在的密码应用缺陷，综合分析、确定密码应用缺陷风险等级； 5）随机数检测工具可用于检测 IPSec、TLS、TLCP 等协议中密文数据的随机性。

网络边界访问控制信息的完整性	采用密码技术保证网络边界访问控制信息的完整性。	端口扫描工具 密码算法校验工具源代码审计工具 接口测试工具	1）端口扫描工具可用于探测和识别被测信息系统中相关设备所对应的端口服务开启情况； 2）密码算法校验工具可用于校验网络边界访问控制信息的完整性保护所使用密码算法的合规性、正确性。 3）源代码审计工具可用于分析网络边界访问控制信息的完整性保护相关代码； 4）接口测试工具可用于测试密码相关接口的安全性。
安全接入认证	采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入的设备身份真实性。	端口扫描工具 数字证书校验工具协议分析工具 密码算法校验工具源代码审计工具 接口测试工具 密码应用缺陷验证工具	1）端口扫描工具可用于探测和识别被测信息系统中相关设备所对应的端口服务开启情况； 2）数字证书校验工具可用于校验数字证书有效性；

			3) 协议分析工具可用于分析设备接入通道涉及的协议类型、协议版本、密钥交换过程、密码算法等；分析安全接入认证的工作机制； 4) 密码算法校验工具可用于校验安全接入认证所使用密码算法的合规性、正确性； 5) 源代码审计工具可用于分析安全接入认证相关代码； 6) 接口测试工具可用于测试密码相关接口的安全性； 7) 密码应用缺陷验证工具可用于识别、利用安全接入认证存在的密码应用缺陷，综合分析、确定密码应用缺陷风险等级。

3.2.6.3. 设备和计算安全测评工具

测评单元	测评内容	测评工具推荐建议	工具说明
身份鉴别	采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性；	端口扫描工具 数字证书校验工具协议分析工具 密码算法校验工具源代码审计工具 接口测试工具 APDU 报文分析工具 密码应用缺陷验证工具	1) 端口扫描工具可用于探测和识别被测信息系统中相关设备所对应的端口服务开启情况； 2) 数字证书校验工具可用于校验数字证书有效性； 3) 协议分析工具可用于分析协议类型、协议版本、密钥交换过程、密码算法等；分析对登录设备的用户进行身份鉴别的工作机制； 4) 密码算法校验工具可用于校验身份鉴别所使用密码算法的合规性、正确性； 5) 源代码审计工具可用于分析身份鉴别相关代码； 6) 接口测试工具可用于测试密码相关

			接口的安全性； 7)APDU 报文分析工具可用于分析密码卡、智能密码钥匙等的 APDU 报文； 8)密码应用缺陷验证工具可用于识别、利用身份鉴别存在的密码应用缺陷，综合分析、确定密码应用缺陷风险等级。
远程管理通道安全	远程管理设备时，采用密码技术建立安全的信息传输通道；	端口扫描工具 数字证书校验工具协议分析工具 密码算法校验工具密码应用缺陷验证工具	1)端口扫描工具可用于探测和识别被测信息系统中相关设备所对应的端口服务开启情况； 2)数字证书校验工具可用于校验数字证书有效性； 3)协议分析工具可用于分析协议类型、协议版本、密钥交换过程、密码算法等； 4)密码算法校验工具可用于校验远程管理通道所使用密码算法的合规性、正

			确性； 5）密码应用缺陷验证工具可用于识别、利用远程管理通道存在的密码应用缺陷，综合分析、确定密码应用缺陷风险等级； 6）随机数检测工具可用于检测 IPSec、TLS、TLCP 等协议中密文数据的随机性。
系统资源访问控制信息完整性	采用密码技术保证系统资源访问控制信息的完整性；	密码算法校验工具源代码审计工具 接口测试工具	1）密码算法校验工具可用于校验系统资源访问控制信息完整性保护所使用密码算法的合规性、正确性； 2）源代码审计工具可用于分析系统资源访问控制信息完整性保护相关代码； 3）接口测试工具可用于测试密码相关接口的安全性。

重要信息资源安全标记完整性	采用密码技术保证设备中的重要信息资源安全标记的完整性；	密码算法校验工具源代码审计工具 接口测试工具	1）密码算法校验工具可用于校验重要信息资源安全标记完整性保护所使用密码算法的合规性、正确性； 2）源代码审计工具可用于分析重要信息资源安全标记完整性保护相关代码； 3）接口测试工具可用于测试密码相关接口的安全性。
日志记录完整性	采用密码技术保证日志记录的完整性；	密码算法校验工具源代码审计工具 接口测试工具	1）密码算法校验工具可用于校验日志记录完整性保护所使用密码算法的合规性、正确性； 2）源代码审计工具可用于分析日志记录完整性保护相关代码； 3）接口测试工具可用于测试密码相关接口的安全性。

重要可执行程序完整性、重要可执行程序来源真实性	采用密码技术对重要可执行程序进行完整性保护，并对其来源进行真实性验证。	数字证书校验工具密码算法校验工具源代码审计工具 接口测试工具逆向分析工具	1) 数字证书校验工具可用于校验数字证书有效性； 2) 密码算法校验工具可用于校验重要可执行程序完整性和来源真实性保护所使用密码算法的合规性、正确性； 3) 源代码审计工具可用于分析重要可执行程序完整性和来源真实性保护相关代码； 4) 接口测试工具可用于测试密码相关接口的安全性； 5) 逆向分析工具可用于分析重要可执行程序完整性和来源真实性保护的工作机制。

3.2.6.4. 应用和数据安全测评工具

测评单元	测评内容	测评工具推荐建议	工具说明
身份鉴别	采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性；	端口扫描工具 数字证书校验工具协议分析工具 密码算法校验工具源代码审计工具 接口测试工具 APDU 报文分析工具 密码应用缺陷验证工具	1) 端口扫描工具可用于探测和识别被测信息系统中相关设备所对应的端口服务开启情况； 2) 数字证书校验工具可用于校验数字证书有效性； 3) 协议分析工具可用于分析协议类型、协议版本、密钥交换过程、密码算法等；分析对登录用户进行身份鉴别的工作机制； 4) 密码算法校验工具可用于校验身份鉴别所使用密码算法的合规性、正确性； 5) 源代码审计工具可用于分析身份鉴别相关代码； 6) 接口测试工具可用于测试密码相关接口的安全性；

			7)APDU 报文分析工具可用于分析智能密码钥匙等的 APDU 报文。 8)密码应用缺陷验证工具可用于识别、利用身份鉴别存在的密码应用缺陷，综合分析、确定密码应用缺陷风险等级。
访问控制信息完整性	采用密码技术保证信息系统应用的访问控制信息的完整性；	密码算法校验工具源代码审计工具 接口测试工具	1)密码算法校验工具可用于校验访问控制信息完整性保护所使用密码算法的合规性、正确性； 2)源代码审计工具可用于分析访问控制信息完整性保护相关代码； 3)接口测试工具可用于测试密码相关接口的安全性。
重要信息资源安全标记完整性	采用密码技术保证信息系统应用的重要信息资源安全标记的完整性；	密码算法校验工具源代码审计工具 接口测试工具	1)密码算法校验工具可用于校验重要信息资源安全标记完整性保护所使用密码算法的合规性、正

			确性； 2）源代码审计工具可用于分析重要信息资源安全标记完整性保护相关代码； 3）接口测试工具可用于测试密码相关接口的安全性。
重要数据传输机密性	采用密码技术保证信息系统应用的重要数据在传输过程中的机密性；	端口扫描工具 协议分析工具 密码算法校验工具源代码审计工具 接口测试工具 编码转换工具 密码应用缺陷验证工具	1）端口扫描工具可用于探测和识别被测信息系统中相关设备所对应的端口服务开启情况； 2）协议分析工具可用于分析协议类型、协议版本、密钥交换过程、密码算法等；分析重要数据传输机密性保护的工作机制； 3）密码算法校验工具可用于校验重要数据传输机密性保护所使用密码算法的合规性、正确性； 4）源代码审计工具可用于分析重要数据传输机密性保护

			相关代码； 5）接口测试工具可用于测试密码相关接口的安全性； 6）编码转换工具可用于对所采集数据进行编码转换、编码解析等； 7）密码应用缺陷验证工具可用于识别、利用重要数据传输机密性保护存在的密码应用缺陷，综合分析、确定密码应用缺陷风险等级； 8）随机数检测工具可用于检测使用加密算法对数据进行机密性保护后的密文数据的随机性。
重要数据存储机密性	采用密码技术保证信息系统应用的重要数据在存储过程中的机密性；	密码算法校验工具源代码审计工具 接口测试工具 编码转换工具 密码应用缺陷验证工具	1）密码算法校验工具可用于校验重要数据存储机密性保护所使用密码算法的合规性、正确性； 2）源代码审计工具可用于分析重要数

			据存储机密性保护相关代码； 3）接口测试工具可用于测试密码相关接口的安全性； 4）编码转换工具可用于对所采集数据进行编码转换、编码解析等； 5）密码应用缺陷验证工具可用于识别、利用重要数据存储机密性保护存在的密码应用缺陷，综合分析、确定密码应用缺陷风险等级； 6）随机数检测工具可用于检测使用加密算法对数据进行机密性保护后的密文数据的随机性。
重要数据传输完整性	采用密码技术保证信息系统应用的重要数据在传输过程中的完整性；	端口扫描工具 协议分析工具 密码算法校验工具电子签章校验工具源代码审计工具	1）端口扫描工具可用于探测和识别被测信息系统中相关设备所对应的端口服务开启情况； 2）协议分析工具可用

		接口测试工具编码转换工具	于分析协议类型、协议版本、密钥交换过程、密码算法等；分析重要数据传输完整性保护的工作机制； 3）密码算法校验工具可用于校验重要数据传输完整性保护所使用密码算法的合规性、正确性； 4）电子签章校验工具可用于校验电子签章数据传输完整性保护的合规性、正确性； 5）源代码审计工具可用于分析重要数据传输完整性保护相关代码； 6）接口测试工具可用于测试密码相关接口的安全性； 7）编码转换工具可用于对所采集数据进行编码转换、编码解析等。

重要数据存储完整性	采用密码技术保证信息系统应用的重要数据在存储过程中的完整性；	密码算法校验工具电子签章校验工具源代码审计工具 接口测试工具 编码转换工具 密码应用缺陷验证工具	1）密码算法校验工具可用于校验重要数据存储完整性保护所使用密码算法的合规性、正确性； 2）电子签章校验工具可用于校验电子签章数据存储完整性保护的合规性、正确性； 3）源代码审计工具可用于分析重要数据存储完整性保护相关代码； 4）接口测试工具可用于测试密码相关接口的安全性； 5）编码转换工具可用于对所采集数据进行编码转换、编码解析等； 6）密码应用缺陷验证工具可用于识别、利用重要数据存储完整性保护存在的密码应用缺陷，综合分析、确定密码应用缺陷风

			险等级。
不可否认性	在可能涉及法律责任认定的应用中，采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性。	密码算法校验工具电子签章校验工具源代码审计工具 接口测试工具 编码转换工具 密码应用缺陷验证工具	1）密码算法校验工具可用于校验不可否认性保护所使用密码算法的合规性、正确性； 2）电子签章校验工具可用于校验在进行电子签章操作时，不可否认性保护的合规性、正确性； 3）源代码审计工具可用于分析不可否认性保护的相关代码； 4）接口测试工具可用于测试密码相关接口的安全性； 5）编码转换工具可用于对所采集数据进行编码转换、编码解析等； 6）密码应用缺陷验证工具可用于识别、利用不可否认性保护存

			在的密码应用缺陷，综合分析、确定密码应用缺陷风险等级。

3.2.7. 常见的工具测试示例表

3.2.7.1. 对称密码算法校验功能对应表

算法名称	密钥长度（比特）	依据标准
SM4	128	GB/T32907《信息安全技术 SM4 分组密码算法》
ZUC	28	GB/T33133.2《信息安全技术祖冲之序列密码算法第 2 部分：保密性算法》 GB/T33133.3《信息安全技术祖冲之序列密码算法第 3 部分：完整性算法》
AES	128、192、256	ISO/IEC18033-3《Informationtechnology-Security techniques-Encryptionalgorithms-Part3:Blockciphers》
DES	64（由于加入错误检查比特，密钥实质长度为 56）	
3DES	128（2TDEA，实质长度为 112）、192（3TDEA，实质长度为 168）	

3.2.7.2. 对称密码算法支持对应表

工作模式	涉及的参数及参数长度要求	是否需要数据填充	依据标准
ECB	无	需要	GB/T17964《信息

CBC	初始向量 IV，IV 长度为一个分组的长度	需要	安全技术分组密码算法的工作模式》
CFB	初始向量 IV，IV 长度为一个分组的长度	可能需要（具体情况可参考标准 GB/T17964《信息安全技术分组密码算法的工作模式》附录 A.3）	
OFB	初始向量 IV，IV 长度为一个分组的长度	可能需要（具体情况可参考标准 GB/T17964《信息安全技术分组密码算法的工作模式》附录 A.4）	
CTR	计时器 Counter，Counter 长度为一个分组的长度	不需要	
XTS	加密调整值 TWeak，TWeak 长度为一个分组的长度	不需要	
CCM	**参数 1**：S，S 长度为 120-8w 比特； **参数 2**：w，w 为信息长度域的长度（以字节为单位），应在集合{2,3,4,5,6,7,8}	需要	GB/T36624《信息技术安全技术可鉴别的加密机制》

	中选取； **参数 3：** tag（标志，与加密后的消息拼接，用于提供数据完整性保护），tag 的长度为 t（以比特为单位），t 应在集合 {32, 48, 64, 80, 96, 112, 128}中选取。 备注:CCM 工作模式应使用分组长度为 128 位的分组密码算法		
GCM	**参数 1：** S，S 可为任意长度； **参数 2：** A，A 可为任意长度，在工具开发时可明确定义输入长度上限； **参数 3：** tag（标志，与加密后的消息拼接，用于提供数据完整性保护），tag 的长度为 t，t 的取值应是 8 的整数倍，且满足 96≤t	不需要	

	≤128（在特定情况下 t 的值也可以为 32 或 64）。 备注：GCM 工作模式应使用分组长度为 128 位的分组密码算法		

3.2.7.3. 支持的数据填充方式表

填充方式	填充过程	示例
不填充	无	略
Zero 填充	在输入后填充 a 个字节 0x00，其中“a”表示输入最后一个分组达到分组长度所需要的字节数。如果输入为空串或其最后一个分组正好为分组长度，则不填充。	以 SM4 密码算法为例，以 Hex 格式编码：输入为 00112233445566778899，则填充后为 00112233445566778899000000000000；若输入为 00112233445566778899AABBCCDDEEFF，则填充后为 00112233445566778899AABBCCDDEEFF。
PKCS#7 填充	在输入后填充 a 个字节“a”，其中“a”表示输入最后一个分组达到分组	以 SM4 密码算法为例，以 Hex 格式编码：输入为 00112233445566778899，则填充后为 00112233445566778899060606060606；若输入为 00112233445566778899AABBCCDDEEFF，

	长度所需要的字节数。如果输入为空串或其最后一个分组正好为分组长度，则填充 b 个字节“b”，其中“b”表示一个分组所需要的字节数。	则填充后为 00112233445566778899AABBCCDDEEFF101010101010101010101010101010。
PKCS#5 填充	PKCS#5 填充是 PKCS#7 填充的子集，只是分组长度固定为 8 字节。	以 DES 密码算法为例，以 Hex 格式编码：输入为 0011223344，则填充后为 0011223344030303。
ISO10126 填充	在输入后填充 a-1 个随机字节，然后填充 1 个字节“a”，其中“a”表示输入最后一个分组达到分组长度所需要的字节数。	以 SM4 密码算法为例，以 Hex 格式编码：输入为 00112233445566778899，则填充后可能为 00112233445566778899c6fb28f2e006；若输入为 00112233445566778899AABBCCDDEEFF，则填充后可能为 00112233445566778899AABBCCDDEEFF27ac3cbde9f215f6d80e1e4b46b0fb10。
ISO/IEC7816-4 填充	在输入后填充 1 个字节 0x80，然后填充 a-1 个字节 0x00，其中“a”表示输入最后一个分组达到分组长度所需要的字节数。	以 SM4 密码算法为例，以 Hex 格式编码：输入为 00112233445566778899，则填充后为 00112233445566778899800000000000；若输入为 00112233445566778899AABBCCDDEEFF，则填充后为 00112233445566778899AABBCCDDEEFF80000000000000000000000000000。

ANSIX9.23 填充	在输入后填充 a-1 个字节 0x00，然后填充 1 个字节“a”，其中“a”表示输入分组达到分组长度所需要的字节数。	以 SM4 密码算法为例，以 Hex 格式编码：输入为 00112233445566778899，则填充后为 00112233445566778899000000000006；若输入为 00112233445566778899AABBCCDDEEFF，则填充后为 00112233445566778899AABBCCDDEEFF00000000000000000000000010。

3.2.7.4. 密码杂凑算法校验功能对应表

算法名称		输入长度要求	输出长度（比特）	依据标准
SM3		小于 2^64 比特	256	GB/T32905《信息安全技术 SM3 密码杂凑算法》
MD5		无限制	128	RFC1321:TheMD5Message-DigestAlgorithm
SHA-1		小于 2^64 比特	160	ISO/IEC10118-3《Informationtechnology-Securitytechniques-Hash-functions-Part3:Dedicatedhash-functions》
SHA-2	SHA-224	小于 2^64 比特	224	
	SHA-256		256	
	SHA-384	小于 2^128 比	384	

	SHA-512	特	512	
	SHA-512/224		224	
	SHA-512/256		256	
SHA-3	SHA3-224	无限制	224	
	SHA3-256		256	
	SHA3-384		384	
	SHA3-512		512	

3.2.7.5. 消息鉴别码（MAC）算法校验功能对应表

MAC 算法	输入参数及要求	输出及输出长度比特）	依据标准
CBC-MAC	参数 1：数据串，其比特长度 L≥0，如果选择填充模式 3，则 0≤L<2^n，其中 n 为分	MAC 算法的输出长度为 m，满足：0<m≤n，其中 n 为分组密码的分组长度。	GB/T15852.1《信息技术安全技术消息鉴别码第 1 部分：采用分组

	组密码的分组长度； **参数 2：**选择填充模式（可使用填充方法 1、2 和 3）； **参数 3：**选择分组密码算法； **参数 4：**密钥，密钥比特长度为对应分组算法密钥长度。		密码的机制》
EMAC	**参数 1：**数据串，其比特长度 L≥0，如果选择填充模式 3，则 0≤L<2^n，其中 n 为分组密码的分组长度； **参数 2：**选择填充模式（可使用填充方法 1、2 和 3）； **参数 3：**选择分组密码算法； **参数 4：**密钥 K、K，，比特长度均等于对应分组算法密钥的长度，K 和 K，可由同一个主密钥（分组密码密钥）通过密钥诱导方法生成，应满足 K 和 K，高概率不	MAC 算法的输出长度为 m，满足：0<m≤n，其中 n 为分组密码的分组长度。	GB/T15852.1《信息技术安全技术消息鉴别码第 1 部分：采用分组密码的机制》

	相同。		
ANSI retailMAC	**参数 1：**数据串，其比特长度 L≥0，如果选择填充模式 3，则 0≤L<2^n，其中 n 为分组密码的分组长度； **参数 2：**选择填充模式（可使用填充方法 1、2 和 3）； **参数 3：**选择分组密码算法； **参数 4：**密钥 K、K，，两个密钥应独立选取，比特长度均等于对应分组算法密钥的长度。	MAC 算法的输出长度为 m，满足：0<m≤n，其中 n 为分组密码的分组长度。	GB/T15852.1《信息技术安全技术消息鉴别码第 1 部分：采用分组密码的机制》
MacDES	**参数 1：**数据串，其比特长度 L≥2n，如果选择填充模式 3，则 0≤L<2^n，其中 n 为分组密码的分组长度； **参数 2：**选择填充模式（可使用填充方法 1、2	MAC 算法的输出长度为 m，满足：0<m≤n，其中 n 为分组密码的分组长度。	GB/T15852.1《信息技术安全技术消息鉴别码第 1 部分：采用分组密码的机制》

	和 3，填充的 分组数不应小于 2；参数 3：选择分组密码算法； 参数 4：密钥 K 和 K，两个密钥应独立选取，比特长度均等于对应分组算法密钥的长度。		
CMAC	参数 1：明文字符串，其长度 L≥0； 参数 2：选择填充模式（可使用填充方法 4）； 参数 3：选择分组密码算法； 参数 4：密钥 K，长度等于对应分组算法密钥的长度。	MAC 算法的输出长度为 m，满足：0<m≤n，其中 n 为分组密码的分组长度。	GB/T15852.1《信息技术安全技术消息鉴别码第 1 部分：采用分组密码的机制》
LMAC	参数 1：数据串，其比特长度 L≥0，如果选择填充模式 3，则 0≤L<2^n，其中 n 为分组密码的分组长度； 参数 2：选择填充模式（可使用填充方法 1、2 和 3）；	MAC 算法的输出长度为 m，满足：0<m≤n，其中 n 为分组密码的分组长度。	GB/T15852.1《信息技术安全技术消息鉴别码第 1 部分：采用分组密码的机制》

	参数 3：选择分组密码算法； **参数 4：**密钥 K、K,，比特长度均等于对应分组算法密钥的长度，K 和 K,可由同一个主密钥（分组密码密钥）通过密钥诱导方法生成，应满足 K 和 K,高概率不相同。		
TrCBC	**参数 1：**数据串，其比特长度 L≥0； **参数 2：**选择填充模式（可使用填充方法 4）； **参数 3：**选择分组密码算法； **参数 4：**密钥，密钥比特长度等于对应分组算法密钥长度。	MAC 算法的输出长度为 m，满足：0<m≤n，其中 n 为分组密码的分组长度。	GB/T15852.1《信息技术安全技术消息鉴别码第 1 部分：采用分组密码的机制》
GMAC	**参数 1：**输入消息，其比特长度 L ≤128*2^64； **参数 2:**分组长度为 128 比特的分组密码算法； **参数 3：**主密钥 K； **参数 4:**临时值比特串，	MAC 算法的输出长度为 m，满足：m 为 8 的整数倍，96≤m≤128 （在特定场合下，m=32 和 m=64 仍允许使用，具体参考 GB/T15852.3-2019）。	GB/T15852.3《信息技术安全技术消息鉴别码第 3 部分：采用泛杂凑函数的机制》

	其比特长度为任意长度。		
HMAC	**参数 1:**选择杂凑函数，m（m≤L2，其中 L2 为杂凑值的比特长度）。杂凑函数应从 ISO/IEC10118-3 中的专用杂凑函数 1、2、3 和 7 中选取。使用的专用杂凑函数也可以为 SM3 算法； **参数 2:** 输入消息。其比特长度 L 不大于 2^64-1； **参数 3:** 密钥。密钥比特长度 k 应该满足 L2≤k≤L1，其中 L1 为输入到轮函数的比特串的比特长度，L2 为杂凑值的比特长度。		GB/T15852.2《信息技术安全技术消息鉴别码第 2 部分:采用专用杂凑函数的机制》

3.2.7.6. 消息鉴别码（MAC）算法填充对应表

序号	填充方法分类	填充方法	示例

1	填充方法 1	在数据比特串 D 的右侧填充“0”，尽可能少填充(甚至不填充)，使填充后比特串的长度是分组长度 n 的正整数倍。	明文字符串： 546869732069732074686520746573742006D65737361676520 填充后输出： 546869732069732074686520746573742006D6573736167652000000000000000
2	填充方法 2	在数据比特串 D 的右侧填充一个比特“1”，然后在所得到的比特串右侧填充“0”，尽可能少填充(甚至不填充)，使填充后的比特串的长度是 n 的正整数倍。	明文字符串： 546869732069732074686520746573742006D65737361676520 填充后输出： 546869732069732074686520746573742006D6573736167652080000000000000
3	填充方法 3	在数据比特串 D 的右侧填充“0”，尽可能少填充(甚至不填充)，使填充后比特串的长度是 n 的正整数倍。然后在所得到的数据比特串左侧填充一个分组 L。分组 L 由尽可能少的“0”和数据比特串 D 的长度 LD 的二进制表示组成，	明文字符串： 546869732069732074686520746573742006D65737361676520 填充后输出： 00000000000000000000000000000C854686973206973207468652074657374206D6573736167652000000000000000

		其中位于 LD 二进制表示的左侧的“0”尽可能少，且使 L 的长度为 n 比特。L 最右端的比特和 LD 的二进制表示中的最低位相对应。 填充后的数据串 D 的比特长度应小于 2。	
4	填充方法 4	如果输入 MAC 算法的数据比特串 D 的比特长度是 n 的正整数倍，则不需要填充。否则，在数据比特串 D 的右侧填充一个“1”比特，然后在所得到的比特串右侧填充“0”，尽可能少填充（甚至不填充），使填充后的比特串的长度是 n 的正整数倍。	明文字符串： 54686973206973207468652074657374206D65737361676520 填充后输出： 54686973206973207468652074657374206D6573736167652080000000000000

3.2.7.7. 对称密码算法校验功能对应表

算法名称		公钥长度	私钥长度	依据标准
SM2		512 比特，包含两个坐标分量，每个坐标分量长度为 256 比特	256 比特	GB/T32918.1《信息安全技术 SM2 椭圆曲线公钥密码算法第 1 部分：总则》 GB/T32918.2《信息安全技术 SM2 椭圆曲线公钥密码算法第 2 部分：数字签名算法》 GB/T32918.3《信息安全技术 SM2 椭圆曲线公钥密码算法第 3 部分：密钥交换协议》 GB/T32918.4《信息安全技术 SM2 椭圆曲线公钥密码算法第 4 部分：公钥加密算法》 GB/T32918.5《信息安全技术 SM2 椭圆曲线公钥密码算法第 5 部分：参数定义》
SM9	签名验签	主公钥 1024 比特，包含两个坐标分量，每个坐标分量长度为 512 比特	用户签名私钥512比特，包含两个坐标分量，每个坐标分量长度为	GB/T38635.1《信息安全技术 SM9 标识密码算法第 1 部分:总则》 GB/T38635.2《信息安全

			256 比特	技术 SM9 标识密码算法第 2 部分:算法》
	加密解密	加密主公钥 512 比特，包含两个坐标分量，每个坐标分量长度为 256 比特	用户加密私钥 1024 比特，包含两个坐标分量，每个坐标分量长度为 512 比特	
	密钥交换	加密主公钥 512 比特，包含两个坐标分量，每个坐标分量长度为 256 比特	用户加密私钥 deA、deB，其中 deA 和 deB 都为 1024 比特，包含两个坐标分量，每个坐标分量长度为 512 比特	
	密钥封装	加密主公钥 512 比特，包含两个坐标分量，每个坐标分量长度为 256 比特	用户加密私钥 1024 比特，包含两个坐标分量，每个坐标分量长度为 512 比特	
RSA	RSA-1024	(n,e)，其中，n 为 1024 比特	(d,p,q),d 长度为 1024 比特	RFC8017:PKCS#1:RSA CryptographySpecifications Version2.2
	RSA-2048	(n,e)，其中，n 为 2048 比特	(d,p,q),d 长度为 2048 比特	
	RSA-3072	(n,e)，其中，n 为 3072 比特	(d,p,q),d 长度为 3072 比特	

3.2.7.8. SM2 密码算法校验功能对应表

SM2 算法功能	输入参数及输入参数长度要求（比特）	输出参数及输出参数长度要求（比特）
密钥生成	私钥 d，长度为 256 比特	公钥（x,y），其中 x 和 y 均为 256 比特
验证公钥	公钥（x,y），其中 x 和 y 均为 256 比特	公钥在曲线上/公钥不在曲线上
加密	**参数 1：** 公钥（x,y），x 和 y 均为 256 比特 **参数 2：** 明文 M，M 长度为 m_len	密文 C，长度为 768+m_len
解密	**参数 1：** 私钥 d，d 为 256 比特 **参数 2：** 密文 C，密文 C，768+m_len	明文 M，长度为 m_len
签名	**参数 1：** 私钥 d，d 为 256 比特 **参数 2：** 待签名原文 M **参数 3：** 用户 ID	签名值（r,s），其中 r 和 s 均为 256 比特
验签	**参数 1：** 公钥（x,y），x 和 y 均为 256 比特	验证通过/验证不通过

	参数 2： 待验签消息 M **参数 3：** 签名值（r,s），r 和 s 均为 256 比特 **参数 4：** 用户 ID	
密钥交换	**用户 A 参数：** 用户标识 ZA，私钥 dA，公钥 PA=（xA,yA） **用户 B 参数：** 用户标识 ZB，私钥 dB，公钥 PB=（xB,yB），其中 ZA、ZB、dA、dB、xA、yA、xB、yB 均为 256 比特	用户 A 发送至用户 B 数据：RA=（x1,y1）、SA 用户 B 发送至用户 A 数据:RB=(x2,y2)、SB，其中 x1、y1、x2、y2、SA 和 SB 均为 256 比特

3.2.7.9. SM9 密码算法校验功能对应表

SM9 算法功能	**输入参数及参数输入长度要求**	**输出参数及参数输输出长度**
系统签名主密钥和用户签名密钥产生	**参数 1：** 系统私钥 ks，ks 长度为 256 比特 **参数 2：** 用户公钥 IDA	签名主公钥 Ppub-s，签名私钥 dsA
签名	**参数 1：** 待签名原文 M **参数 2：** 主公钥 Ppub-s，Ppub-s 的两个坐标分量长度均为 512 比特 **参数 3：** 用户公钥 IDA **参数 4：** 用户签名私钥 dsA，dsA 的两个坐标分	签名（h,S），其中 h 长度为 256 比特，S 长度为 512 比特

	量长度均为 256 比特	
验签	**参数 1：** 待验签消息 M **参数 2：** 主公钥 Ppub-s，Ppub-s 的两个坐标分量长度均为 512 比特 **参数 3：** 用户公钥 IDA	验证通过/验证不通过
系统加密主密钥和用户加密密钥产生	**参数 1：** 系统私钥 ke，ke 长度为 256 比特 **参数 2：** 用户公钥 IDA，IDB	加密主公钥 Ppub-e、用户私钥 dA、dB
加密	**参数 1：** 明文 M **参数 2：** 公钥 IDB: **参数 3：** 加密主公钥 Ppub-e，Ppub-e 的两个坐标分量长度均 256 比特	密文 C
解密	**参数 1：** 密文 C **参数 2：** 用户私钥 dB，dB 的两个坐标分量均为 512 比特	明文 M
密钥封装	**参数 1：** 用户标识 IDB	封装密文 C，被封装的密钥 K

	参数 2： 加密主公钥 Ppub-e，Ppub-e 的两个坐标分量长度均为 256 比特	
密钥解封	**参数 1：** 封装密文 C **参数 2：** 用户标识 IDB **参数 3：**用户私钥 dB:dB 的两个坐标分量均为 512 比特	被封装的密钥 K

3.2.7.10. RSA 密码算法校验功能对应表

常用 RSA 算法功能		**输入参数及输入参数长度要求**	**输出参数及输出参数长度**
密钥生成	RSA-1024	**参数 1：** 公钥（n,e） **参数 2：** 私钥 p 和 q，p 和 q 的长度为 512 比特	私钥（d,p,q），d 长度为 1024 比特
	RSA-2048	**参数 1：** 公钥（n,e） **参数 2：** 私钥 p 和 q，p 和 q 的长度为 1024 比特	私钥（d,p,q），d 长度为 2048 比特
	RSA-3072	**参数 1：** 公钥（n,e） **参数 2：** 私钥 p 和 q，p 和 q 的长度为 1536 比特	私钥（d,p,q），d 长度为 3072 比特
加密	RSA-1024	**参数 1：** 明文 M，M 长度	密文 C，为 1024 比特

		为 1024 比特 **参数 2：** 公钥（n,e），n 长度为 1024 比特	
	RSA-2048	**参数 1：** 明文 M，M 长度为 2048 比特 **参数 2：** 公钥（n,e），n 长度为 2048 比特	密文 C，为 2048 比特
	RSA-3072	**参数 1：** 明文 M，M 长度为 3072 比特 **参数 2：** 公钥（n,e），n 长度为 3072 比特	密文 C，为 3072 比特
解密	RSA-1024	**参数 1：** 密文 C，C 长度为 1024 比特 **参数 2：** 私钥（d,p,q），d 长度为 1024 比特	明文 M，为 1024 比特
	RSA-2048	**参数 1：** 密文 C，C 长度为 2048 比特 **参数 2：** 私钥（d,p,q），d 长度为 2048 比特	明文 M，为 2048 比特
	RSA-3072	**参数 1：** 密文 C，C 长度为 3072 比特 **参数 2：** 私钥（d,p,q），d 长度为 3072 比特	明文 M，为 3072 比特

签名	RSA-1024	**参数 1：** 待签名原文 M **参数 2：** 私钥（d,p,q）	签名值 S
	RSA-2048	**参数 1：** 待签名原文 M **参数 2：** 私钥（d,p,q）	签名值 S
	RSA-3072	**参数 1：** 待签名原文 M **参数 2：** 私钥（d,p,q）	签名值 S
验签	RSA-1024	**参数 1：** 待验签消息 M **参数 2：** 签名值 S **参数 3：** 公钥（n,e）	验签通过/验签不通过
	RSA-2048	**参数 1：** 待验签消息 M **参数 2：** 签名值 S **参数 3：** 公钥（n,e）	验签通过/验签不通过
	RSA-3072	**参数 1：** 待验签消息 M **参数 2：** 签名值 S **参数 3：** 公钥（n,e）	验签通过/验签不通过

3.2.8. 可能遇到的风险及处理办法

具体需根据威胁类型和威胁发生频率，判断测评结果汇总中部分符合项或不符合项所产生的安全问题被威胁利用的可能性，可能性的取值范围为高、中和低。根据资产价值的高低，判断测评结果汇总中部分符合项或不符合项所产生的安全问题被威胁利用后，对被测系统的业务信息安全造成的影响程度，影响程度取值

范围为高、中和低。

综合以上的结果，我司根据自身经验和相关国家标准要求，对被测系统面临的安全风险进行赋值，风险值的取值范围为高、中和低。结合被测系统的安全保护等级对风险分析结果进行评价，即对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益造成的风险。如果存在高风险项，则认为信息系统面临高风险；同时也需要考虑多个中低风险叠加可能导致的高风险问题。

3.2.9. 商业密码安全评估服务进度计划

我公司在于北京市文化和旅游局宣传中心（北京市旅游运行监测中心）签订合同后在合同生效之日起 5 日内提交实施方案，供北京市文化和旅游局宣传中心（北京市旅游运行监测中心）审查，经北京市文化和旅游局宣传中心（北京市旅游运行监测中心）审核同意后，我公司于北京市文化和旅游局宣传中心（北京市旅游运行监测中心）通知的开工日期为起点，将 30 日内完成现场测评工作。以下为我公司制定的实施计划方案

序号	阶段	服务内容	工期	项目交付物
1	准备阶段	收集评估系统相关信息 确定评估范围和目标 准备评估所需的文档和工具	3	《评估准备材料清单》、评估范围和目标确认书
2	评估阶段	依据商用密码相关标准和规范进行安全性评估 对系统进行调研、上机核查、抓包等方式对信息系统密码应用防护进行验证	15	现场评估记录

		分析评估结果，编制评估报告		
3	整改建议	根据评估结果，提出整改建议 编制整改建议书，明确整改措施和期限	5	整改建设书
4	测评报告编制阶段	整理评估内容进行综合分析，输出评估报告	7	《商业密码安全性评估报告》

3.3. 售后服务内容

在项目实施过程中我单位承诺会进行以下售后服务，包括等保回访和追踪、等保培训服务、信息及网络安全支持服务等。

(1)、等保回访和追踪

定期回访、沟通、了解客户评价及支撑需求；合同服务期内提供 7*24 小时服务热线。

（2)、等保培训服务

提供等保测评培训服务，包括技术和管理部分的培训。

（3)、信息及网络安全支持服务

提供信息安全支持服务，在合同签署日期所在年度，可以实时响应北京市文化和旅游局宣传中心(北京市旅游运行监测中心)信息安全及网络安全咨询需求；同时协助北京市文化和旅游局宣传中心（北京市旅游运行监测中心）规划设计信息安全整改建设方案；且承诺在项目实施期间除客户要求外不更换项目经理。

3.4. 具体服务方案，质量管理和应急响应方案

3.4.1. 进度管理

3.4.1.1. 项目进度计划

序号	阶段	工作内容	工期	主要输出物
1	等级保护差距分析	现状分析	15	《差距分析报告》、《渗透测试报告》、《漏洞扫描报告》
		差距分析		
		渗透测试及漏洞扫描		
		控制建议		
2	协助安全整改	依据等级保护差距分析、渗透测试及漏扫结果最终编制等级保护整改方案，对被测系统提出整改和加固建议，并为安全整改和加固工作提供指导。	10	《等级保护整改方案》
3	信息安全等级保护测评	测评准备	30	《测试申请》、《测评方案》、《测评记录》、《网络安全等级保护测评报告》
		测评方案编制		
		现场测试实施		
		单项测评结果分析		

		单元测评结果分析		
		整体测评		
		风险分析		
		等级测评结论形成		
		测评报告编制		

3.4.1.2. 项目进度保障

■ 我公司的项目进度管理遵循以下原则：

1）依据项目合同约定的工期目标，组织项目进度管理；

2）在确保项目质量和安全的原则下，控制项目进度。

■ 我公司的项目进度管理包含以下内容：

1）我公司在了解项目特点的前提下，根据工期目标，已提交总体进度计划，以及定期提交阶段性工作计划。

2）我公司制定详细的项目建设进度计划，按照合同的进度计划制定具体的实施计划，定期跟踪检查，对可能发生的工程延误提出相应对策；

3）我公司定期或不定期地召开或参加项目例会、协调会议等，向客户通报项目进展情况，提交进度报告，及时解决相关问题。

■ 我公司已建立项目变更流程，记录项目变更。

3.4.2. 项目质量保障

3.4.2.1. 项目质量保证原则

质量保证的原则如下：

1）质量管理贯穿于整个项目实施之全过程

必须从项目立项之日开始就重视项目的质量管理工作，质量管理应贯穿于整个项目实施之全过程。

在制定详细计划时，要清楚的制定项目的检查点，除了便于检查工作进展，也是控制项目质量的需要。

2）对质量的承诺应落实到项目组的每一个人

服务项目在实施过程中，中科信息安全共性技术国家工程研究中心有限公司按照 ISO9001 及 CMM 质量管理体系进行完善的管理，并设立专门的、独立于项目的质量保障组，对项目进行全程质量管理。

参加项目的每一个人都重视本次项目的质量管理工作，要让参与项目的每个人都具有正确的质量观念和负有相应的质量保证责任。如果质量管理的贯彻只停留在服务单位或者项目经理级别，那么应用系统的质量就得不到保证。

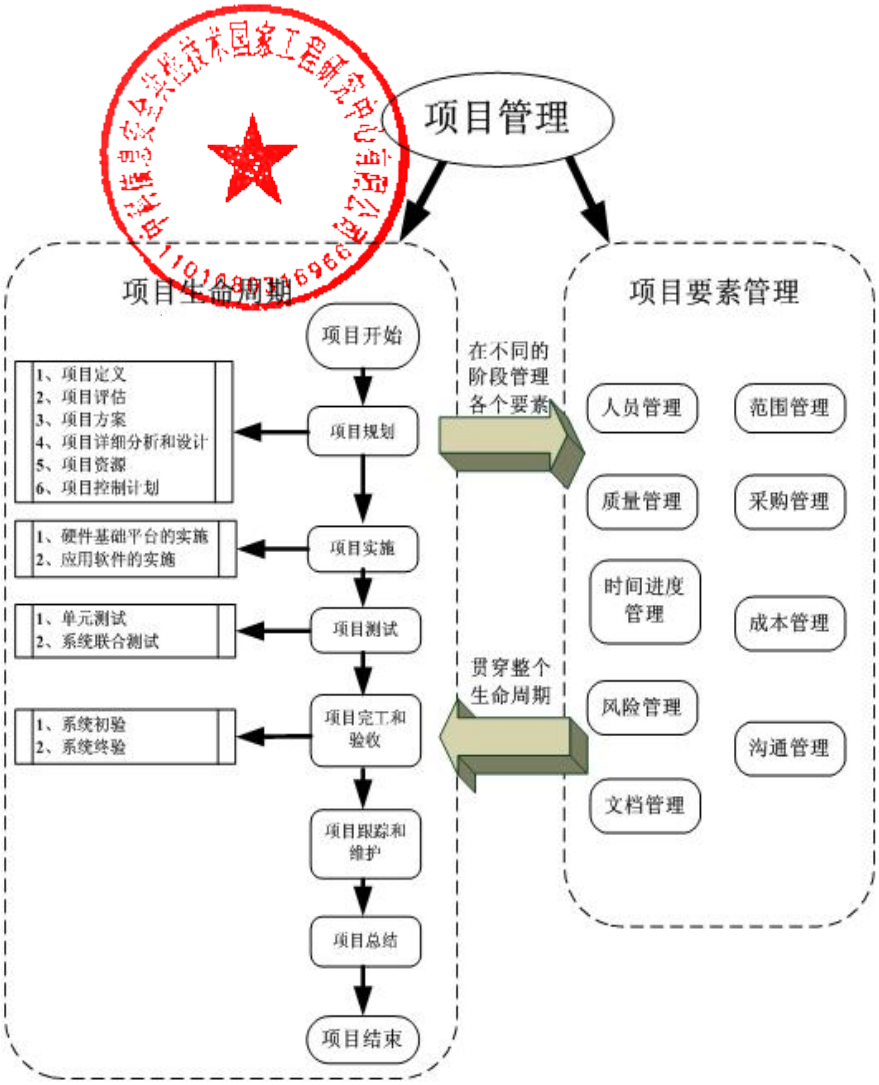
3）对项目质量保证的策划要充分考虑项目工程的实际情况

对项目质量保证的策划必须符合工程统一标准，并符合项目自身的情况，充分考虑项目的特点，以做到有的放矢。

4）重视质量体系的文档化

文档既是工程所依据的标准，又是检验工作的凭证，文档的正确和完整程度是检验项目规范化管理程度的要素之一。只有文档化的质量体系，才能保证质量是可控制的。为此，在质量管理活动的全过程中，必须做到文档的规范管理。

3.4.2.2. 项目管理流程



本次项目管理内容主要包括组织范围管理、进度管理、人员管理、风险管理、文档管理、质量管理、沟通管理等方面，这些内容贯穿于项目的整个生命周期中。

3.4.2.3. 项目管理要素

1）范围管理：需要准确定义项目的范围，以及对项目的工作范围进行有效地管理和控制。

2）进度管理：该项目既有深度又有广度，深度是指在某一节点上不同平台，广度是指不同区域的互联。因此其进度控制包括节点施工进度、不同区域的施工进度、物资供应进度、进度的协调等。由于项目时间紧，因此整个进度控制不仅需要精心设计进度计划，而且需要计划进度和实施进度之间的协调和严格控制。

3）人员管理：该项目系统结构复杂、项目量大，涉及服务商、北京市文化和旅游局宣传中心（北京市旅游运行监测中心）方各个相关部门等。为了确保项目的顺利实施，需要建立统一的项目管理组织、清晰的组织结构和合理的人员配备，同时制定该项目的各项工作制度、明确相互的关系和责任、精心组织施工队伍和项目实施、组织物资供应和后勤保障等。本部分工作包括了对组织和人员的一系列协调和管理工作。

4）风险管理：由于项目的复杂性和一些问题的不可预知性，项目的实施存在风险。风险管理主要是根据中科信息安全共性技术国家工程研究中心有限公司的项目经验，提出该项目中存在的主要风险、风险后果及风险的预防措施，尽可能地规避风险或减少风险发生的可能性，并提出应对风险的措施。

5）文档管理：文档作为管理依据、任务之间联系的凭证、质量保证、培训与参考、软件维护支持和历史档案，对项目重要性是不言而喻的。因此文档的管理是项目管理的一个重要环节，中科信息安全共性技术国家工程研究中心有限公司在项目的每个阶段都会产生相应的详尽的文档，并指定专人管理。

6）质量管理：项目质量与许多过程、许多环节和因素相关联，我单位尽可能保证项目质量。

7）沟通管理：对项目的项目会议等沟通活动进行管理，有效地协调和沟通项目组的各个组成部分。

3.4.2.4. 人员管理

我公司已向客户提供拟派参加本项目的主要人员名单以及各自职责，并向客户保证中标后工程人员的稳定性，在本项目工程结束前，参加本项目的人员变动必须取得客户同意。

我公司已按照项目的需求建立完善的项目组织机构，进行相关的项目管控和随时调整项目实施方向。

3.4.2.5. 沟通管理

现在项目的实施过程中，可能遇到争议问题，为了尽快解决这些问题，提高工作效率，中科信息安全共性技术国家工程研究中心有限公司制定了详细的问题与争议管理措施。

1) 遇到争议问题时及时召开项目会议，由相关项目组讨论、协调解决。

2) 如果项目会议无法解决问题，应及时向上级领导和相关单位汇报，协调解决，或请示解决方法和资源。

3) 视问题的严重情况，采用的报告方式可以是口头汇报或以书面形式汇报。

4) 用详细的文档记录问题的原因、解决方法、解决结果等。

5) 对项目的项目会议等沟通活动进行管理，有效地协调和沟通项目组的各个组成部分。

3.4.2.6. 文档管理

项目组讨论作出的决定能及时请示汇报相关单位并形成纪要存档。各个环节的重要决策要有书面文件汇报。

中科信息安全共性技术国家工程研究中心有限公司将建立完善的项目决策管理体系、制定详细的决策制度来保证项目实施过程中高效、正确地做出相关的决策。

针对不同影响程度的决策点可以分不同的决策等级，如重要决策，关联性决策和一般决策等。

针对不同的等级的决策需建立相应的决策制度。例如，对一般的某设备的配置实施由工程师自己决策，如何准备、配置、调试等；对于关键性的决策，需要中科信息安全共性技术国家工程研究中心有限公司、项目小组和厂家共同讨论决

策，并由上级领导批准。

关于决策需要形成文档记录，并由相关负责人签字，如项目实施方案评审记录、实施记录、会议纪要等。

决策需要及时报告给上级领导，并及时报告相关项目成员。

3.4.3. 应急管理

我公司会建立严格的应急管理体系，制定项目的应急控制方案和实施措施，一旦在测评过程中出现信息安全事件，我公司承诺 2 小时内赶到现场处理问题，同时我公司会尽力避免信息安全事件的发生，在实施过程中督促并落实各环节风险控制内容和目标；保证项目各个阶段工作满足客户对风险控制的要求。

3.4.4. 风险管理

为了顺利地完成差距分析评估工作，中科信息安全共性技术国家工程研究中心有限公司采取相应的措施来对评估工作本身可能带来的风险和问题进行规避，这主要包括签署委托协议、保密协议并规避现场评估风险、规范实施过程、加强沟通交流等方面。

3.4.4.1. 委托协议

在开始评估工作之前，评估机构和被评估单位需要以委托协议的方式明确评估工作的目标、范围、人员组成、计划安排、执行步骤和要求以及双方的责任和义务等。使得评估双方对评估过程中的基本问题达成共识，后续的工作以此为基础，避免以后的工作出现大的分歧。

3.4.4.2. 保密协议

由于评估工作需要了解被评估单位的很多敏感信息，为保障被评估单位的权益，评估双方应签署完善的、合乎法律规范的保密协议，以约束评估双方现在及将来的行为。保密协议规定了评估双方保密方面的权利与义务。

评估工作的成果属被评估单位所有，评估机构对其的引用与公开应得到被评估单位的授权，否则被评估单位将按照保密协议的要求追究评估机构的相关责任。

3.4.4.3. 现场评估工作风险规避

进行验证测试和工具测试时，评估机构需要与被评估单位充分的协调，安排好测试时间，尽量避开业务高峰期，在系统资源处于空闲状态时进行，并需要被评估单位对整个测试过程进行监督。

在进行验证测试和工具测试前，需要对关键数据做好备份工作，并对可能出现的对系统的影响制定相应的处理方案。

上机验证测试原则上由被评估单位提供相应的技术人员进行操作，评估人员根据情况提出需要操作的内容，并进行查看和验证。避免由于评估人员对某些专用设备不熟悉所带来的隐患，如：误操作。

评估机构使用的所有技术测试工具（如：扫描、渗透和性能测试工具等）在使用前都应事先告知被评估单位，征得被评估单位的同意，并应详细介绍这些工具的用途以及可能对信息系统造成的影响。必要时可以应被评估单位的要求，先进行一些实验。

3.4.4.4. 规范化实施过程

等级评估是一项复杂的工作，必须采取规范的执行过程，以保证按计划、高质量地完成评估任务。在委托协议和正式开始评估之前制定的评估方案中，需要明确双方的人员职责、评估对象、评估内容要求、评估记录要求、执行过程要求和评估报告要求等内容，明确在评估过程中每一阶段需要产生的相关文档。使评估有章可循，按照清晰的执行要求逐步完成安全评估任务，并给出相应的评估结果报告。

3.4.4.5. 沟通与交流

为避免评估工作中可能出现的歧义，在评估开始前与评估过程中，双方需要

进行积极有效的沟通和交流，及时解决评估中出现的问题，这对保证评估的过程质量和结果质量有重要的作用。

3.5. 企业资质证明文件

3.5.1. 网络安全等级测评与检测评估机构服务认证证书

DJCP

网络安全服务认证证书
等级保护测评服务认证

证书编号：SC202127130010031

兹 证 明：中科信息安全共性技术国家工程研究中心有限公司

统一单位信用代码：91110108791603851A

符合TRIMPS-SC13-001:2021《网络安全等级测评与检测评估机构 服务认证实施规则》的要求。

注册地址：北京市海淀区中关村大街19号16层B1601、B1602、B1603、B1605

办公地址：北京市海淀区中关村大街19号新中关大厦B座北翼16层

首次颁证日期：2021 年 11 月 18 日
发 证 日 期：2024 年 06 月 11 日
有 效 期 至：2027 年 11 月 17 日

在一个监督周期内，本证书必须与本机构监督评价合格后签发的证书保持通知书合并使用方可有效。

公安部第三研究所认证 The Third Research Institute Of Ministry Of Public Security Certification

签发人

公安部第三研究所

地址：上海市徐汇区岳阳路76号 电话：021-64318599 证书有效性查询：http://www.trimps.net.cn S2024000030

3.5.2. 商用密码应用安全性评估试点机构/商用密码检测机构资质认证证书

商用密码检测机构资质证书

机构名称：中科信息安全共性技术国家工程研究中心有限公司

统一社会信用代码：91110108791603851A

注册地址：北京市海淀区中关村大街19号16层B1601、B1602、B1603、B1605

证书编号：GM-P-000024

有效期至：2029年11月10日

业务范围：

商用密码应用安全性评估

国家密码管理局

2024年11月11日

国家密码管理局

WWW.SCA.GOV.CN

首页 | 机构概况 | 新闻动态 | 信息公开 | 在线服务 | 互动交流 | 专题专栏

首页 > 新闻动态 > 通知公告

国家密码管理局公告（第49号）

发布日期：2024-11-11 来源：

【字体：大 中 小】 打印

国家密码管理局公告

（第49号）

依据《中华人民共和国密码法》、《商用密码管理条例》、《商用密码检测机构管理办法》，现发布《商用密码检测机构（商用密码应用安全性评估业务）目录》。即日起，商用密码应用安全性评估试点工作正式结束，未取得商用密码检测机构（商用密码应用安全性评估业务）资质的机构不得面向社会开展商用密码应用安全性评估业务。

特此公告。

附件：商用密码检测机构（商用密码应用安全性评估业务）目录

国家密码管理局

2024年11月11日

商用密码检测机构（商用密码应用安全性评估业务）目录

中国电子科技集团公司第十五研究所

中国航天系统科学与工程研究院

中国科学院软件研究所

中国科学院数据与通信保护研究教育中心

中国软件评测中心(工业和信息化部软件与集成电路促进中心)

中国铁道科学研究院集团有限公司

中国移动通信有限公司研究院

中科信息安全共性技术国家工程研究中心有限公司

天津恒御科技有限公司

天津鲲奥世达科技有限公司

天津联信达软件技术有限公司

天津市兴先道科技有限公司

天津云安科技发展有限公司

中互金认证有限公司

3.5.3. 信息安全应急处理二级服务资质

信息安全服务资质认证证书

证书编号：CCRC-2010-ISV-ER-037

兹证明

中科信息安全共性技术国家工程研究中心有限公司

统一社会信用代码：91110108791603851A

信息安全应急处理服务资质符合
CCRC-ISV-C01:2021《信息安全服务规范》
CCRC-ISV-R01:2022《信息安全服务资质认证实施规则》
二级服务资质要求

注册地址：北京市中关村大街19号16层B1601、B1602、B1603、B1605
办公地址：北京市中关村大街19号新中关大厦B座北翼16层
发证日期：2025年5月25日　　有效期至：2028年5月24日
首次颁证日期：2010年10月24日
证书有效期内本证书的有效性依据发证机构的定期监督获得保持。

中国认可 产品 PRODUCT CNAS C066-P

Signed: Chen Jianliang

证书可通过扫描二维码或网站查询
The certificate can be verified through scanning the QR code or the website: cx.cnca.cn or www.isccc.gov.cn

中国网络安全审查认证和市场监管大数据中心
CHINA CYBERSECURITY REVIEW, CERTIFICATION AND MARKET REGULATION BIG DATA CENTER
中国·北京·朝阳区惠新里241号 100029
No.241 Huixinli Street, Chaoyang District, Beijing, 100029 China

3.5.4. 中国合格评定国家认可委员会-检验机构认可证书（CNAS）

中国合格评定国家认可委员会

检验机构认可证书

（注册号：CNAS IB0300）

兹证明：

中科信息安全共性技术国家工程研究中心有限公司

（法人：中科信息安全共性技术国家工程研究中心有限公司）

北京市海淀区中关村大街 19 号新中关大厦 B 座北翼 16 层，

100080

符合 ISO/IEC 17020:2012《各类检验机构运行的基本准则》(CNAS-CI01《检验机构能力认可准则》) C 类的要求，具备承担本证书附件所列检验服务的能力，予以认可。

获认可的能力范围见标有相同认可注册号的证书附件，证书附件是本证书组成部分。

生效日期：2024-05-05

截止日期：2030-05-04

中国合格评定国家认可委员会授权人 张朝华

中国合格评定国家认可委员会（CNAS）经国家认证认可监督管理委员会（CNCA）授权，负责实施合格评定国家认可制度。
CNAS是国际实验室认可合作组织（ILAC）和亚太认可合作组织（APAC）的互认协议成员。
本证书的有效性可登录www.cnas.org.cn获认可的机构名录查询。

3.5.5. 信息安全风险评估一级服务资质

信息安全服务资质认证证书

证书编号：CCRC-2010-ISV-RA-025

兹证明

中科信息安全共性技术国家工程研究中心有限公司

统一社会信用代码：91110108791603851A

信息安全风险评估服务资质符合

CCRC-ISV-C01:2021《信息安全服务规范》

CCRC-ISV-R01:2022《信息安全服务资质认证实施规则》

一级服务资质要求

注册地址：北京市中关村大街19号16层B1601、B1602、B1603、B1605

办公地址：北京市中关村大街19号新中关大厦B座北翼16层

发证日期：2025年5月25日　　有效期至：2028年5月24日

首次颁证日期：2010年10月24日

证书有效期内本证书的有效性依据发证机构的定期监督获得保持。

CNAS 中国认可 产品 PRODUCT CNAS C066-P

陈建良 Signed: Chen Jianliang

证书可通过扫描二维码或网站查询 The certificate can be verified through scanning the QR code or the website: CX.CNCA.CN or www.isccc.gov.cn

中国网络安全审查认证和市场监管大数据中心

CHINA CYBERSECURITY REVIEW, CERTIFICATION AND MARKET REGULATION BIG DATA CENTER

中国·北京·朝阳区惠新里241号 100029

No.241 Huixinli Street, Chaoyang District, Beijing, 100029 China

3.5.6. ISO9001 质量管理体系认证证书

注册号：01621Q4032379R5M

质量管理体系认证证书

初次发证日期：2009年10月27日/ 再认证日期：2024年10月21日/ 证书有效期至：2027年10月20日

(本次再认证审核日期:2024年10月19日到2024年10月20日，上一认证周期截止日期:2024年10月20日)

CERTIFICATE

兹 证 明

中科信息安全共性技术国家工程研究中心有限公司

质量管理体系符合GB/T19001-2016/ISO9001:2015 标准,适用于
网络安全服务、信息系统咨询规划服务、网络系统检测评估服务、商用密码应用安全性评估服务、网络安全等级测评与检测评估服务、网络安全审计服务、信息系统风险评估服务、代码安全审计服务

新世纪检验认证有限责任公司
总经理：

统一社会信用代码：91110108791603851A
注册地址：北京市海淀区中关村大街19号16层B1601、B1602、B1603、B1605
经营地址：北京市海淀区中关村大街19号新中关大厦B座北翼16层

中国认可
国际互认
管理体系
MANAGEMENT SYSTEM
CNAS C016-M

BCC 地址：北京市东城区广渠门内大街45号5层45-（05）-02室
本证书在国家规定的各行政许可、资质许可有效期内使用有效
获证组织必须定期接受监督审核并经审核合格，此证书方继续有效
证书有效性可通过网站：www.bcc.com.cn查询，也可二维码查询
本证书信息可在国家认监委网站www.cnca.gov.cn 查询

3.5.7. ISO27001 信息安全管理体系认证证书

注册号：0162B2430439R2M

信息安全管理体系认证证书

初次发证日期：2018年10月26日/ 再认证日期：2024年10月22日

证书有效期至：2027年10月25日

CERTIFICATE

兹 证 明

中科信息安全共性技术国家工程研究中心有限公司

信息安全管理体系符合ISO/IEC 27001:2022,适用于
与网络安全服务、信息系统咨询规划服务、网络系统检测评估服务、商用密码应用安全性评估服务、网络安全等级测评与检测评估服务、网络安全审计服务、信息系统风险评估服务、代码安全审计服务相关的信息安全管理；适用性声明：NERCIS-01-01 版本：B

新世纪检验认证有限责任公司

总经理：

统一社会信用代码：91110108791603851A

注册地址：北京市海淀区中关村大街19号16层B1601、B1602、B1603、B1605

经营地址：北京市海淀区中关村大街19号新中关大厦B座北翼16层

中国认可
国际互认
管理体系
MANAGEMENT SYSTEM
CNAS C016-M

BCC 地址：北京市东城区广渠门内大街45号5层45-（05）-02室
本证书在国家规定的各行政许可、资质许可有效期内使用有效
获证组织必须定期接受监督审核并经审核合格，此证书方继续有效
证书有效性可通过网站：www.bcc.com.cn查询，也可二维码查询
本证书信息可在国家认监委网站www.cnca.gov.cn 查询

3.5.8. IT服务管理体系认证证书

CERTIFICATE

注册号：01620241ISM0324R1AGH

基于ISO/IEC 20000-1的服务管理体系认证证书

初次发证日期：2022年01月11日/ 再认证日期：2024年10月22日

证书有效期至：2028年01月10日

兹 证 明

中科信息安全共性技术国家工程研究中心有限公司

基于ISO/IEC 20000-1的服务管理体系符合ISO/IEC 20000-1:2018标准,适用于向外部客户提供信息系统咨询规划服务、网络及网络系统检测评估服务、商用密码应用检测评估服务、信息系统测试与评估服务、信息系统审计服务

新世纪检验认证有限责任公司

总经理：

统一社会信用代码：91110108791603851A

注册地址：北京市海淀区中关村大街19号16层B1601、B1602、B1603、B1605

经营地址：北京市海淀区中关村大街19号新中关大厦B座北翼16层

中国认可
管理体系
MANAGEMENT SYSTEM
CNAS C016-M

BCC 地址：北京市东城区广渠门内大街45号5层45-（05）-02室
本证书在国家规定的各行政许可、资质许可有效期内使用有效
获证组织必须定期接受监督审核并经审核合格，此证书方继续有效
证书有效性可通过网站：www.bcc.com.cn查询，也可二维码查询
本证书信息可在国家认监委网站www.cnca.gov.cn 查询

3.6. 拟投入本项目的服务人员及主要人员

3.6.1.1. 拟投入本项目主要工程技术人员情况表

序号	姓名	本项目中技术职务	执业资格		职称（资格）	从业年限
			名称	编号		
1.	闫伟	项目经理	网络安全等级保护测评师	2050382112500418	高级测评师	10
2.	魏敬坡	项目成员	网络安全等级保护测评师	20489501140390116	初级测评师	25
3.	胡建勋	项目成员	网络安全等级保护测评师	20632451112190313	高级测评师	22
4.	刘元	项目成员	网络安全等级保护测评师	21321431124190316	中级测评师	25
5.	郭义丽	项目成员	网络安全等级保护测评师	19022191102260310	中级测评师	9
6.	刘晓丽	项目成员	网络安全等级保护测评师	217522553302X0115	初级测评师	5

说明：

（1）上表应填写响应人拟投入本项目主要技术人员基本情况；

（2）“技术职务”一栏应说明在本项目中的技术职务或分工；

（3）本表应加盖响应人公章，填写空间不足可根据需要可自行增加表格数量，每页均需盖章；

3.6.1.2. 主要人员简历及资质

3.6.1.2.1. 项目经理-闫伟

3.6.1.2.1.1. 简历

姓　名	闫伟	性　别	男	年　龄	34
职　务	项目经理	学　历	本科	参加工作时间	2015 年
职　称	无		专　　业	计算机科学与技术	
职称证书编号	无		从事专业年限	10 年	
参　与　项　目　情　况					
时间	项目名称		工程规模	担任的技术职务	注

2023-8	北京市行政复议与应诉平台软件 安全和密码测评	25.8 万	项目经理	无
2022-2	北京市生态环境局辐射安全管理系统项目	32 万	项目经理	无
2024-3	中国针灸学会综合会员管理与服务云平台安全测试项目	2 万	项目经理	无

响应人：中科信息安全共性技术国家工程研究中心有限公司（盖章）

3.6.1.2.1.2. 身份证

3.6.1.2.1.3. 毕业证


普通高等学校

毕业证书

学生 闫伟 性别 男 ，一九九一年 十 月 十六 日生，于 二〇一一年 九 月至二〇一五年 七 月在本校 计算机科学与技术 专业 四 年制 本 科学习，修完教学计划规定的全部课程，成绩合格，准予毕业。

校 名：内蒙古师范大学 校（院）长：

证书编号：101351201505011871

二〇一五 年 七 月 一 日

中华人民共和国教育部学历证书查询网址：http://www.chsi.com.cn

3.6.1.2.1.4. CISP


中国信息安全测评中心

China Information Technology Security Evaluation Center

注册信息安全专业人员(CISP)

Certified Information Security Professional

注册信息安全工程师

CERTIFIED INFORMATION SECURITY ENGINEER

证书编号：CNITSEC2017CISE01383

Certificate No.

兹证明

This is to certify that

闫伟

YAN WEI

证件号码：150303199110162510

ID No.

经中国信息安全测评中心的考试和审定，符合

has successfully fulfilled the requirements prescribed by CNITSEC

《注册信息安全专业人员资质评估准则》

for certification and is hereby awarded this professional designation.

的要求，获准 注册信息安全工程师(CISE) 资质。

首次注册：2017 年 6 月 24 日

Certified Since

发证日期：2023 年 5 月 20 日

Issue Date

有效期：2023 年 5 月 20 日至 2026 年 5 月 19 日

Valid thru

批准人

Signed by

中国信息安全测评中心 CNITSEC 证书专用章

3.6.1.2.1.5. PMP


Project Management Institute.
THIS IS TO CERTIFY THAT
Wei Yan
HAS BEEN FORMALLY EVALUATED FOR DEMONSTRATED EXPERIENCE, KNOWLEDGE AND PERFORMANCE IN ACHIEVING AN ORGANIZATIONAL OBJECTIVE THROUGH DEFINING AND OVERSEEING PROJECTS AND RESOURCES AND IS HEREBY BESTOWED THE GLOBAL CREDENTIAL
Project Management Professional (PMP)®
IN TESTIMONY WHEREOF, WE HAVE SUBSCRIBED OUR SIGNATURES UNDER THE SEAL OF THE INSTITUTE
LuAnn Piccard, PMP | Chair, Board of Directors
Pierre Le Manh | President & CEO
PMP® Number: 3051217
PMP® Original Grant Date: 20 June 2021
PMP® Expiration Date: 20 June 2027

3.6.1.2.1.6. CISAW-应急服务

CISAW

信息安全保障人员认证证书

Certificate of Information Security Assurance Workforce Certification

兹证明 This is to certify that

闫伟 YANWEI

考试成绩合格，并通过了认证评价，符合《信息安全保障人员认证准则》的要求，具备下述认证方向和级别所需的知识和技能，特颁此证。

has passed the examination and certification assessment, successfully fulfilled the requirements of Cisaw Criteria, and obtained the knowledge and skills required for the following field and level. This certificate is hereby issued.

认证方向 / Certification Field: 应急服务 / Emergency Service

认证级别 / Certification Level: 专业级 / Professional Level

证书编号 / Certificate No.: 2019CISAWIM0085（R3）

发证日期 / Date of Issue: 2025年08月15日 / August 15, 2025

有效期至 / Date of Expiry: 2028年09月07日 / September 7, 2028

CCRC

陈建良

Signed: Chen Jianliang

中国网络安全审查认证和市场监管大数据中心

CHINA CYBERSECURITY REVIEW,CERTIFICATION AND MARKET REGULATION BIG DATA CENTER

通过www.isccc.gov.cn或扫描二维码验证本证书的真实性、有效性。

You can verify the authenticity and validity of this certificate via www.isccc.gov.cn or scanning the QR code.

本证书仅发放电子证书

E-certificate only

3.6.1.2.1.7. 网络安全等级保护测评师-高级

网络安全等级测评师证书

姓　　名：闫伟

身份证号：150303199110162510

证书编号：20503821125100418

证书等级：高级

证书查询网址：http://www.djbh.net

发证日期：2020-09-10

持有人参加网络安全等级测评师培训及考核，成绩合格，特颁发此证书。

中关村信息安全测评联盟

批准人：鲍逸明

3.6.1.2.2. 团队成员-魏敬坡

姓　名	魏敬坡	性　别	男	年　龄	48
职　务	项目成员	学　历	专科	参加工作时间	2000 年
职　称	无	专　　业	计算机及应用		
职称证书编号	无		从事专业年限	25 年	
参　与　项　目　情　况					
时间	项目名称	工程规模	担任的技术职务	注	
2023-8	北京市行政复议与应诉平台软件、安全和密码测评	25.8 万	项目成员	无	
2022-2	北京市生态环境局辐射安全管理系统项目	32 万	项目成员	无	
2024-3	中国针灸学会综合会员管理与服务云平台安全测试项目	2 万	项目成员	无	

响应人：中科信息安全共性技术国家工程研究中心有限公司（盖章）

3.6.1.2.2.1. 身份证


姓名 魏敬坡
性别 男 民族 汉
出生 1977 年 9 月 27 日
住址 河北省石家庄市长安区谈固西街87号40栋301号
公民身份号码 131002197709274039
中华人民共和国
居民身份证
签发机关 石家庄市公安局长安分局
有效期限 2020.11.20-2040.11.20

3.6.1.2.2.2. 毕业证


普通高等学校

毕业证书

学生 魏敬坡 性别 男，

一九七七年 九 月二十七日生，于一九九七年

九 月至二〇〇〇 年 七 月在本校

计算机及应用 专业

三年制专科学习，修完教学计划规定

的全部课程，成绩合格，准予毕业。

校(院)长：

校 名：

二〇〇〇 年 七 月 十日

中华人民共和国教育部制

No. 00480871

学校编号：272232

3.6.1.2.2.3. 网络安全等级测评师（初级）


网络安全等级测评师证书

姓 名： 魏敬坡

身份证号： 131002197709274039

证书编号： 20489501140390116

证书等级： 初级

证书查询网址：http://www.djbh.net

发证日期： 2020-09-10

持有人参加网络安全等级测评师培训及考核，成绩合格，特颁发此证书。

中关村信息安全测评联盟

批准人：

3.6.1.2.2.4. CISP

中国信息安全测评中心
China Information Technology Security Evaluation Center
注册信息安全专业人员 (CISP)
Certified Information Security Professional

首次注册：2020 年 3 月 28 日
Certified Since
发证日期：2023 年 5 月 20 日
Issue Date
有效期：2023 年 5 月 20 日至 2026 年 5 月 19 日
Valid thru

注册信息安全工程师
CERTIFIED INFORMATION SECURITY ENGINEER

(证书编号：CNITSEC2020CISE01437)
Certificate No.
兹证明
This is to certify that

魏敬坡
WEI JINGPO

(证件号：131002197709274039)
ID No.

经中国信息安全测评中心的考试和审定，符合
has successfully fulfilled the requirements prescribed by CNITSEC
《注册信息安全专业人员资质评估准则》
for certification and is hereby awarded this professional designation.
的要求，获准 注册信息安全工程师(CISE) 资质。

批准人
Signed by

中国信息安全测评中心 CNITSEC 证书专用章

3.6.1.2.2.5. CIIPT-D

姓 名：魏敬坡
身份证号：131002197709274039
证书编号：012423002008604232
证书类别：CIIPT-D
有 效 期：2027 年 12 月 1 日

持有人参加国家重要信息系统保护人员培训（CIIPT）及考核，成绩合格，特颁发此证书。

Participants CIIPT and assessment are qualified. This certificate is hereby issued.

公安部网络安全等级保护评估中心

批准人：

证书查询：www.cspec.org.cn

3.6.1.2.2.6. DSA

数据安全评估师证书

Data Security Assessor Certificate

兹证明 This is to certify that 魏敬坡 WEI JINGPO

通过了数据安全评估师岗位能力评定考试，具备《信息安全技术 网络安全从业人员能力基本要求》(GB/T 42446-2023)中规定的网络数据安全保护和评估工作任务所需的知识和技能，特发此证。

passed the Data Security Assessor competency assessment, mastered the knowledge and skills for network data security protection and assessment as stipulated in the "Information security technology-Basic requirements for competence of cybersecurity workforce"(GB/T 42446-2023), this certificate is hereby issued.

证书编号 / Certificate No.: 2024DSA0089

发证日期 / Date of issue: 2024年05月07日

有效期至 / Date of expiry: 2027年05月06日

中国网络安全审查技术与认证中心

通过www.isccc.gov.cn或扫描二维码验证本证书的真实性、有效性

You can verify the authenticity and validity of this certificate via www.isccc.gov.cn or scanning the QR code

本证书仅发放电子证书

E-certificate only

3.6.1.2.2.7. CISAW-应急服务

信息安全保障人员认证证书

Information Security Assurance Worker Certification Certificate

兹证明 This is to certify that

魏敬坡 WEI JINGPO

认证考试成绩合格，并通过了认证评价，符合《信息安全保障人员认证准则》的要求，特颁此证。

has passed the examination, certification assessment, and successfully fulfilled the requirements of Certification Criteria for information Security Assurance Worker and is hereby awarded the professional-level in emergency service field.

认证方向/Certification field: 应急服务（专业级）ES/PL

证书编号/Certificate No.: 2021CISAWES0325（R）

序列号/Serial No.: 1054148

发证日期/Date of Issue: 2024年06月25日

有效期/Term of Validity: 2027年07月19日

通过www.isccc.gov.cn或扫描二维码验证本证书的真实性、有效性。

You can verify the authenticity and validity of this certificate via www.isccc.gov.cn or scanning the QR code.

本证书仅发放电子证书

E-certificate only

3.6.1.2.2.8. 商用密码应用安全性评估人员测评能力考核

商用密码应用安全性评估从业人员考核成绩

准考证号：071502026832

姓　　名：魏敬坡

身份证号：131002197709274039

报考单位：中科信息安全共性技术国家工程研究中心有限公司

持证人参加商用密码应用安全性评估从业人员考核，成绩 62.00 分。考核合格。

国家密码管理局商用密码管理办公室

2023 年 8 月 16 日

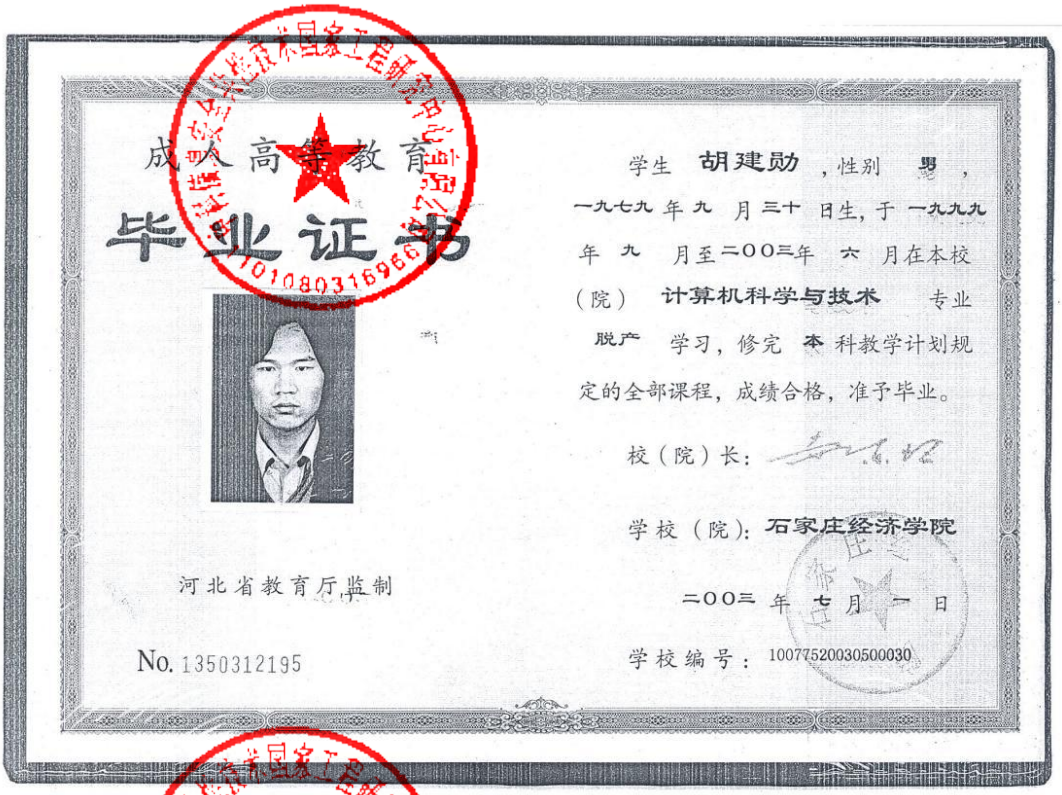
3.6.1.2.3. 团队成员-胡建勋

3.6.1.2.3.1. 简历

姓　名	胡建勋	性　别	男	年　龄	46
职　务	项目成员	学　历	本科	参加工作时间	2003 年
职　称	无		专　　业	计算机科学与技术	
职称证书编号	无		从事专业年限	22 年	
参　与　项　目　情　况					
时间	项目名称		工程规模	担任的技术职务	注
2023-8	北京市行政复议与应诉平台软件、安全和密码测评		25.8 万	项目成员	无
2022-2	北京市生态环境局辐射安全管理系统项目		32 万	项目成员	无
2024-3	中国针灸学会综合会员管理与服务云平台安全测试项目		2 万	项目成员	无

响应人：中科信息安全共性技术国家工程研究中心有限公司（盖章）

3.6.1.2.3.2. 毕业证


成人高等教育
毕业证书
学生 胡建勋 ，性别 男 ，
一九七九 年 九 月 三十 日生，于 一九九九
年 九 月至二〇〇三年 六 月在本校
（院） 计算机科学与技术 专业
脱产 学习，修完 本 科教学计划规
定的全部课程，成绩合格，准予毕业。
校（院）长：
学校（院）：石家庄经济学院
二〇〇三 年 七 月 一 日
河北省教育厅监制
No. 1350312195
学校编号：10077520030500030

3.6.1.2.3.3. 信息系统项目管理师（高级）


计算机技术与软件专业技术资格
Qualification of Computer and Software Professional
本证书由中华人民共和国人力资源和社会保障部、工业和信息化部批准颁发，表明持证人通过国家统一组织的考试，取得计算机技术与软件专业技术资格。
中华人民共和国人力资源和社会保障部
中华人民共和国工业和信息化部
姓 名：胡建勋
证件号码：142701197909301219
性 别：男
出生年月：1979年09月
级 别：高级
专 业：信息系统项目管理师
批准日期：2017年11月11日
管 理 号：17201111336

3.6.1.2.3.4. 网络安全等级测评师（高级）

3.6.1.2.3.5. 商用密码应用安全性评估人员测评能力考核证书

商用密码应用安全性评估
人员测评能力考核

编　　号：200267686

姓　　名：胡建勋

身份证号：142701197909301219

所在单位：信息安全共性技术国家工程研究中心

持证人参加2020年第1期全国商用密码应用安全性评估人员测评能力考核，成绩69分。

考核合格。

国家商用密码应用安全性评估
人员测评能力考核小组
2020年1月17日

3.6.1.2.4. 团队成员-刘元

姓　名	刘元	性　别	男	年　龄	54
职　务	项目成员	学　历	硕士	参加工作时间	2010 年
职　称	无	专　业	软件工程领域工程		
职称证书编号	无	从事专业年限	15 年		
参　与　项　目　情　况					
时间	项目名称	工程规模	担任的技术职务	注	
2023-8	北京市行政复议与应诉平台软件、安全和密码测评	25.8 万	项目成员	无	
2022-2	北京市生态环境局辐射安全管理系统项目	32 万	项目成员	无	
2024-3	中国针灸学会综合会员管理与服务云平台安全测试项目	2 万	项目成员	无	

响应人：中科信息安全共性技术国家工程研究中心有限公司（盖章）

3.6.1.2.4.1. 身份证


中华人民共和国
居民身份证
签发机关 南昌市公安局东湖分局
有效期限 2006.03.01-2026.03.01

3.6.1.2.4.2. 学位证


硕士学位证书
刘元 ，男，1971 年 1 月 5 日生，在 电子科技大学
完成了 软件工程领域工程 硕士专业学位培养计划，成绩合格。根据《中
华人民共和国学位条例》的规定，授予 工 程 硕士学位。
校 长
电 子 科 技 大 学
学位评定委员会主席
证书编号：Z1061432010000140
二〇一〇 年 六 月二十六 日
（专业学位证书）

3.6.1.2.4.3. 网络安全等级测评师-中级

网络安全等级测评师证书

姓　　名：刘元

身份证号：360102197101052419

证书编号：21321431124190316

证书等级：中级

证书查询网址：http://www.djbh.net

发证日期：2021-07-29

持有人参加网络安全等级测评师培训及考核，成绩合格，特颁发此证书。

中关村信息安全测评联盟

批准人：鲍逸明

3.6.1.2.4.4. 商用密码应用安全性评估人员测评能力考核证书

商用密码应用安全性评估
人员测评能力考核

编　　号：220367469

姓　　名：刘元

身份证号：360102197101052419

所在单位：中科信息安全共性技术国家工程研究中心有限公司

持证人参加商用密码应用安全性评估人员测评能力考核，成绩 76 分。考核 优秀 。

国家商用密码应用安全性评估
人员测评能力考核小组
2022 年 7 月 8 日

3.6.1.2.5. 团队成员-郭义丽

姓　名	郭义丽	性　别	女	年　龄	35
职　务	项目成员	学　历	本科	参加工作时间	2016 年
职　称	无		专　　业	信息安全	
职称证书编号	无		从事专业年限	9 年	
参　与　项　目　情　况					
时间	项目名称	工程规模	担任的技术职务	注	
2023-8	北京市行政复议与应诉平台软件、安全和密码测评	25.8 万	项目成员	无	
2022-2	北京市生态环境局辐射安全管理系统项目	32 万	项目成员	无	
2024-3	中国针灸学会综合会员管理与服务云平台安全测试项目	2 万	项目成员	无	

响应人：中科信息安全共性技术国家工程研究中心有限公司（盖章）

3.6.1.2.5.1. 身份证


姓名 郭义丽
性别 女 民族 汉
出生 1990 年 12 月 11 日
住址 贵州省遵义县龙坑镇谢家坝村银山组
公民身份号码 522121199012110226
中华人民共和国
居民身份证
签发机关 遵义县公安局
有效期限 2018.02.12-2038.02.12

3.6.1.2.5.2. 毕业证

普通高等学校

毕业证书

学生 郭义丽 性别 女 ,一九九〇年十二月 十一 日生，于 二〇一二年 九 月至二〇一六年 七 月在本校 信息安全 专业 四 年制 本 科学习，修完教学计划规定的全部课程，成绩合格，准予毕业。

校 名：贵州大学 校 长：郑强

证书编号：106571201605003107 二〇一六年 七 月 一 日

中华人民共和国教育部学历证书查询网址：http://www.chsi.com.cn

3.6.1.2.5.3. 网络安全等级测评师-中级

网络安全等级测评师证书

姓 名： 郭义丽

身份证号： 522121199012110226

证书编号： 19022191102260310

证书等级： 中级

证书查询网址：http://www.djbh.net

发证日期： 2019年5月24日

持有人参加网络安全等级测评师培训及考核，成绩合格，特颁发此证书。

中关村信息安全测评联盟

批准人：

3.6.1.2.5.4. CISP

中国信息安全测评中心
China Information Technology Security Evaluation Center

注册信息安全专业人员 (CISP)
Certified Information Security Professional

首次注册：2020 年 3 月 28 日
Certified Since

发证日期：2023 年 5 月 20 日
Issue Date

有效期：2023 年 5 月 20 日至 2026 年 5 月 19 日
Valid thru

注册信息安全工程师
CERTIFIED INFORMATION SECURITY ENGINEER

（证书编号：CNITSEC2020CISE01435）
Certificate No.

兹证明
This is to certify that

郭义丽
GUO YILI

（证件号：522121199012110226）
ID No.

经中国信息安全测评中心的考试和审定，符合
has successfully fulfilled the requirements prescribed by CNITSEC
《注册信息安全专业人员资质评估准则》
for certification and is hereby awarded this professional designation.
的要求，获准 注册信息安全工程师(CISE) 资质。

批准人
Signed by

3.6.1.2.5.5. CISAW

信息安全保障人员认证证书

Information Security Assurance Worker Certification Certificate

兹证明 This is to certify that 郭义丽 GUO YILI

认证考试成绩合格，并通过了认证评价，符合《信息安全保障人员认证准则》的要求，特颁此证。

has passed the examination, certification assessment, and successfully fulfilled the requirements of Certification Criteria for information Security Assurance Worker and is hereby awarded the professional-level in risk management field.

认证方向/Certification field: 风险管理（专业级）RM/PL

证书编号/Certificate No.: 2017CISAWRM1221（R2）

序列号/Serial No.: 1047734

发证日期/Date of Issue: 2023年09月05日

有效期/Term of Validity: 2026年09月26日

通过www.isccc.gov.cn或扫描二维码验证本证书的真实性、有效性。

You can verify the authenticity and validity of this certificate via www.isccc.gov.cn or scanning the QR code.

本证书仅发放电子证书

E-certificate only

3.6.1.2.5.6. 商用密码应用安全性评估人员测评能力考核证书

商用密码应用安全性评估从业人员
考核成绩

准考证号：071602021711

姓　　名：郭义丽

身份证号：522121199012110226

报考单位：中科信息安全共性技术国家工程研究中心有限公司

持证人参加商用密码应用安全性评估从业人员考核，成绩 64.50 分。考核合格。

国家密码管理局商用密码管理办公室

2023 年 8 月 16 日

3.6.1.2.6. 团队成员-刘晓丽

姓　名	刘晓丽	性　别	女	年　龄	27
职　务	项目成员	学　历	本科	参加工作时间	2020 年
职　称	无		专　　业	通信工程	
职称证书编号	无		从事专业年限	5 年	
参　与　项　目　情　况					
时间	项目名称	工程规模	担任的技术职务	注	
2023-8	北京市行政复议与应诉平台软件、安全和密码测评	25.8 万	项目成员	无	
2022-2	北京市生态环境局辐射安全管理系统项目	32 万	项目成员	无	
2024-3	中国针灸学会综合会员管理与服务云平台安全测试项目	2 万	项目成员	无	

响应人：中科信息安全共性技术国家工程研究中心有限公司（盖章）

3.6.1.2.6.1. 身份证


姓名 刘晓丽
性别 女
住址 云南省保山市隆阳区丙麻乡秀岭村委会秀岭2组016号
公民身份号码
中华人民共和国
居民身份证
签发机关 保山市公安局隆阳分局
有效期限 2014.09.07-2024.09.07

3.6.1.2.6.2. 毕业证


普通高等学校

毕业证书

学生 刘晓丽 性别 女，

一九九八年 三 月 三 日生，于二〇一六年

九 月至 二〇二〇 年 六 月在本校

通信工程 专业

四 年制 本 科学习，修完教学计划

规定的全部课程，成绩合格，准予毕业。

校(院)长：黎素梅

校 名：昆明学院

二〇二〇 年 六 月二十四日

证书编号：113931202005001333

云南省教育厅监制

查询网址：http://www.chsi.com.cn

3.6.1.2.6.3. 网络安全等级测评师-初级


DJCP

网络安全等级测评师证书

姓 名：刘晓丽

身份证号：533001199803033O2X

证书编号：217522553302X0115

证书等级：初级

证书查询网址:http//www.djbh.net

持有人参加网络安全等级测评师培训及考核，成绩合格，特颁发此证书。

中关村信息安全测评联盟

批准人：

3.6.1.2.6.4. PMP

3.6.1.2.6.5. 信息系统监理师

3.6.1.2.6.6. 商用密码应用安全性评估人员测评能力考核证书

商用密码应用安全性评估从业人员
考核成绩

准考证号： 071502034030

姓　　名： 刘晓丽

身份证号： 53300119980303302X

报考单位： 中科信息安全共性技术国家工程研究中心有限公司

持证人参加商用密码应用安全性评估从业人员考核，成绩 79.50 分。考核合格。

国家密码管理局商用密码管理办公室

2023 年 8 月 16 日