信息系统安全等级保护评测项目

需求公示

1、项目名称：信息系统安全等级保护评测项目

2、项目编号：GZBYCG2025-084

3、项目联系人：华英峰、殷婷、何琼

4、项目联系电话：18185165747

6、采购方式：公开招标

7、采购货物或服务情况：

（1）采购主要内容：为人社信息系统提供系统信息系统安全等级保护评估服务等。

（2）采购数量：1 批。

（3）采购预算：1223700.00 元。

（4）服务时间：1 年，从签订合同之日起计算。

（5）服务地点：采购人指定地点。

投标供应商资格要求

1、供应商符合《中华人民共和国政府采购法》第二十二条规定，并结合政府采购法实施条例第十七条规定提供以下材料：

（1）一般资格要求：中华人民共和国境内能够独立承担民事责任的法人或其他组织，符合中华人民共和国政府采购法第二十二条之规定：①具有独立承担民事责任的能力：提供法人或其他组织有效的营业执照等证明文件，或自然人身份证明；

②具有良好的商业信誉和健全的财务会计制度：经合法审计机构出具的2023年度或2024年度财务审计报告（含资产负债表、利润表、现金流量表和财务报表附注），审计报告应盖有会计师事务所单位章和注册会计师的执业专用章，并附会计师事务所的营业执照及执业证书复印件，或其基本开户银行出具的资信证明；（复印件加盖投标单位公章）

③具有履行合同所必需的设备和专业技术能力：提供具备履行合同所必需的设备和专业技术能力的承诺函（投标供应商自行承诺，提供承诺函并加盖公章）。

④具有依法缴纳税收和社会保障资金的良好记录：提供依法缴纳税收和社会保障资金的有效证明材料（2025年至今任意一个月）；

⑤参加政府采购活动前三年内，在经营活动中没有重大违法记录：提供参加政府采购活动前3年内在经营活动中没有重大违法记录的书面声明（自拟声明）；

⑥供应商须承诺，提供承诺书：在“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）等渠道查询中未被列入严重失信名单、司法判决名单、政府采购严重违法失信行为记录名单中，如被列严重失信名单、司法判决名单、政府采购严重违法失信行为记录名单中的供应商取消其投标资格，并承担由此造成的一切法律责任及后果；

（2）本项目不接受联合体投标，不接受分包、转包。

（3）根据《政府采购促进中小企业发展管理办法》财库〔2020〕46号规定：本项目是否专门面向中小企业采购：否。

评标办法

评标办法正文

一、投标供应商资格审查

根据《政府采购货物和服务招标投标管理办法》（财政部令第87号）规定，公开招标采购项目开标结束后，采购人或者采购代理机构应当依法对投标供应商的资格进行审查。合格投标供应商不足3家的，不得评标。

投标供应商名称 须提供的资质和相关证明材料	投标供应商1	投标供应商2	投标供应商3	……
具有独立承担民事责任的能力：提供法人或其他组织有效的营业执照等证明文件，或自然人身份证明；（扫描件加盖投标单位公章）				
具有良好的商业信誉和健全的财务会计制度：具有良好的商业信誉和健全的财务会计制度，提供2024年度经第三方审计机构出具的审计报告或2025年任意一个月的财务报表或提供基本开户银行出具的有效的资信证明；（扫描件加盖投标单位公章）				
具有履行合同所必需的设备和专业技术能力：提供具备履行合同所必需的设备和专业技术能力的承诺函（投标供应商自行承诺，提供承诺函并加盖公章）				
具有依法缴纳税收和社会保障资金的良好记录：提供依法缴纳税收和社会保障资金的有效证明材料(2025年至今任意一个月）				
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：提供参加政府采购活动前3年内在经营活动中没有重大违法记录的书面声明（自拟声明）				
供应商须承诺，提供承诺书：在“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）等渠道查询中未被列入严重失信名单、司法判决名单、政府采购严重违法失信行为记录名单中，如被列严重失信名单、司法判决名单、政府采购严重				

违法失信行为记录名单中的供应商取消其投标资格，并承担由此造成的一切法律责任及后果；				
本项目不接受联合体投标，不接受分包、转包：提供承诺函				
结论				

二、评标委员会

1、按照《中华人民共和国政府采购法》和国家有关规定，依法组建评标委员会，评标委员会由采购单位熟悉相关业务的代表，和有关技术、经济等方面的评审专家组成，评审专家不得少于成员总数的三分之二。

2、评标由评标委员会负责，与投标供应商有利害关系的人不得进入评标委员会。

3、评标委员会成员名单在中标结果确定前保密。

三、评标方法

1、本次评标采用**综合评分法**。

2、综合评分法，是指投标文件满足采购文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标供应商为中标候选人的评标方法。

3、评分的主要因素分为价格因素、技术因素和商务因素。评分因素详见评分表。评标分值保留至两位小数。评标时，评标专家依照评分表对每个有效投标供应商的投标文件进行独立评审、打分。

四、评标标准

评标形式（采用以下具体步骤）

第一步：由本项目评标委员会对各投标文件进行符合性审查，符合的进入下一步评审阶段。不符合的其投标作为无效标。

第二步：确定中标候选人（按评分细则对入围投标供应商给相应的评分，并计算其总得分，按各项评标因素计算各有效投标供应商的最终得分，以评分从高到低的顺序推荐前 3 名投标供应商作为中标候选人）。

（一）符合性审查表

序号	符合性审查内容 \ 投标供应商名称		投标供应商 1	投标供应商 2	投标供应商 3	…
1	商务符合性	商务要求是否完全满足				
2	投标保证金	是否满足采购文件要求				
2	无效标审查	按本项目采购文件无效标条款规定，审查是否通过。				
审查结论（通过或不通过）						

（二）评分细则及各项评标因素如下：

评分细则	**实得分值**	**总分**
报价分	**20 分**	**100 分**
技术分	**65 分**	
商务分	**15 分**	

注：评分标准涉及到的佐证材料必须真实有效且清晰可辨认，如提供的佐证材料不清晰，无法有效辨认的，将视为该佐证材料未提供。

评标步骤	序号	评审因素	评审标准	分值
报价评审	1	价格评审	价格分=（评标基准价 / 有效投标报价）×20 备注： 1.评标基准价指满足采购文件要求且投标报价最低，其报价分为满分。 2.得分取两位小数点，第三位四舍五入。 3.投标报价超过采购文件要求采购限价的，其投标文件按废标处理，评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响服务质量或者不能诚信履约的，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。 4. 因落实政府采购政策进行价格调整的，以调整后的价格计算评标基准价和投标报价。所报价均以扣除后的价格参与评审（若有）。报价扣除说明：小微型企业价格扣除率：10%，监狱、福利性企业视为小微型。企业扣除后的金额报价=金额报价*（1-扣除率）；扣除后的下浮率报价=下浮率报价*（1+扣除率）；扣除后的折扣报价=折扣报价*（1-扣除率）。投标人或产品若同时享有以上价格扣除情况的，仅对“投标报价分”进行一次价格扣除，并不作叠加扣除。	20 分
商务评审	1	企业实力	1.投标人具备有效的 ISO9001 质量管理体系认证证书、ISO20000 信息技术服务体系认证证书、ISO27001 信息安全管理体系认证证书、ITSS 信息技术服务运行维护符合性证书，每提供 1 个证书得 3 分，满分 12 分。 2.投标人具备有效的 CCRC 信息安全服务资质认证证书-信息安全风险评估，一级得 5 分，二级的得 3 分，三级得 1 分。 注：提供相关证书复印件或扫描件加盖投标人公章，未提供不得分。	17 分

	2	项目团队	1.项目负责人（1 人）： （1）投标人需指定专门的项目负责人服务本项目，项目负责人具备高级网络安全等级测评师证书、信息系统项目管理师（高级）证书，每提供 1 个得 3 分，未提供不得分，本项最多得 6 分。 2.技术负责人（1 人）： 投标人需指定专门的技术负责人服务本项目，技术负责人具备高级网络安全等级测评师证书的，得 3 分，具备中级网络安全等级测评师证书的，得 2 分，未提供不得分，本项最多得 3 分。 3.服务团队人员（不含项目负责人和技术负责人）： （1）投标人为本项目配备 3 人或 3 人以上的服务团队得 6 分，2 人或 2 人以下不得分。 （2)配备的服务团队人员中具备中级或高级网络安全等级测评师或测试工程师（CISP-PTE）,每提供 1 个证书得 2 分，本项最多得 6 分。 注： 1.项目负责人、技术负责人、服务团队人员互斥，同一人员只计分 1 次。 2.需提供以上人员身份证、证书复印件并加盖投标人公章单位； 3.需提供以上人员 2024 年任意三个月社保证明材料； 4.投标人需提供承诺：我单位提供的项目团队在项目实施过程中不得随意更换，更换人员须获得采购人同意，否则采购人有权单方面解除合同。 未提供承诺，“项目团队”项不得分。（自行承诺，格式自拟）	21 分
	3	服务响应承诺	服务期内响应甲方服务需求 （1）服务期内，按要求开展等级保测评、出具报告，并提交相关材料； （2）承诺参与众测人员的资质、能力、背景，众测平台均满足招标需求，确保众测平台安全可控。 提供此承诺的得 5 分，未提供不得分。	5 分
	4	业绩	提供投标人 2022 年 1 月 1 日以来类似业绩，以合同签订日期为准，每提供 1 个业绩得 4 分，未提供不得分，本项最多得 16 分。 注：提供合同复印件或扫描件加盖投标人公章。	16 分
	5	满意度评价	投标人提供 2022 年 1 月 1 日至今所服务过的类似项目业主评价，且评价为满意，提供 1 份评价意见得 3 分，本项最多得 6 分，未提供不得分。以合同签订日期为准，提供盖有业主单位公章的评价意见。	6 分

技术评审（主观分）	1	服务实施方案	投标人提供服务实施方案，包括但不限于：项目范围、项目流程、工作内容、测评指标、测评工具、报告编制步骤等内容。根据方案进行综合评分： 1.方案完整，合理性、可行性及针对性强的得 5 分； 2.方案完整，合理性、可行性及针对性一般的得 3 分； 3.方案完整，合理性、可行性及针对性差得 1 分； 4.方案不完整或未提供不得分。	5 分
	2	服务风险管理方案	投标人提供服务风险管理方案，包括但不限于：风险识别措施、风险分析措施、风险处置策略、风险监控策略、专门针对本项目可能发生的风险以及相应的应对措施。根据方案进行综合评分： 1.方案完整，合理性、可行性及针对性强的得 5 分； 2.方案完整，合理性、可行性及针对性一般的得 3 分； 3.方案完整，合理性、可行性及针对性差得 1 分； 4.方案不完整或未提供不得分。	5 分
	3	服务质量保障方案	投标人提供服务质量保障方案，包括但不限于：保密措施、应急保障、风险分析及规避措施、应急响应措施。根据方案进行综合评分： 1.方案完整，合理性、可行性及针对性强的得 5 分； 2.方案完整，合理性、可行性及针对性一般的得 3 分； 3.方案完整，合理性、可行性及针对性差得 1 分； 4.方案不完整或未提供不得分。	5 分

注：

① 评分标准中要求提供的证明材料，未明确要求提供原件的，均提供扫描件并加盖公章，否则视为未提供；要求提供的证明材料，投标供应商须按要求提供且提供齐全，否则不得分；要求提供的证明材料，不清晰或无法识别的视为未提供。 ② 除标注有“主观分”以外，其余评分均为客观分，专家对客观分的评审 须保持一致。

（三）价格分的计算：

1、价格分采用低价优先法计算，即满足采购文件要求的前提下，最低有效投标报价作为评标基准价，其价格分为满分。其余投标供应商价格分统一按照下列公式计算：

投标报价得分＝（评标基准价 / 投标报价）×价格权值×100

2、评标过程中，不得去掉报价中的最高报价和最低报价。

（四）评标总得分计算方法：

评标总得分＝F1＋F2＋…＋Fn

F1、F2…Fn 分别为各项评审因素的得分；

注：以上打分计算最终得分保留小数两位。

（五）排序原则：

采用综合评分法的，评标结果按评审后得分由高到低顺序排列。得分相同的，按投标报价由低到高顺序排列；得分且投标报价相同的并列。投标文件满足采购文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标供应商为排名第一的中标候选人。

五、本评标办法的解释权归采购代理机构。

特别说明：本公示内容仅为采购人对本项目的需求公示，具体内容以最终采购文件发售稿为准！

采购需求

按照《中华人民共和国网络安全法》、公安部《关于开展信息系统等级保护安全建设整改工作的指导意见》（公信安〔2009〕1429 号）、人力资源和社会保障部《关于进一步推进人力资源社会保障信息安全等级保护工作的通知》(人社部函〔2011〕246 号)等文件要求，开展人力资源社会保障信息系统网络安全等级保护测评（以下简称“等保”）、信息系统风险评估以及数据安全风险评估工作。

一、整体要求

根据 2025 年公安部要求，开展省人社厅 29 个系统等级保护测评相关工作，28 个系统风险评估，以及不少于 50 个资产的网络和数据安全众测服务，并出具相应的报告。

二、等保工作需求

（一）系统定级工作要求

按照等保规范要求，配合招标人初步确定系统等保级别，负责组织专家评审，承担专家评审所需的各类费用。

（二）系统预评估工作要求

测评系统定级工作完成后，中标人需按照等保规范要求，对本项目中要求测评的信息系统进行备案前的预评测，协助招标人查找不符合性问题，并出具《信息系统等保符合性报告》。

（三）系统等保备案工作要求

招标人将根据中标人出具的《信息系统等保符合性报告》开展符合性整改工作，整改完成后，中标人需按照等保测评要求，开展正式评测，并完成到公安机关的备案，取得定级备案证明。

（四）等保评测依据

等级测评是标准符合性活动，依据网络安全等级保护的最新国家标准或行业标准，按照特定方法对信息系统的安全保护能力进行科学公正的综合评判过程。本次开展测评活动所依据的主要文件及标准如下（不局限以下依据文件）：

1.《关于信息安全等级保护工作的实施意见》（公通字〔2004〕66 号）

2.《信息安全等级保护管理办法》（公通字〔2007〕43 号）

3.《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》（发 改高技〔2008〕2071 号）

4.GB 17859-1999《计算机信息系统安全保护等级划分准则》

5.GB/T 22239-2019《信息安全技术信息系统安全等级保护基本要求》

6.GB/T28448-2019《信息安全技术网络安全等级保护测评要求》

7.GB/T25070-2019《信息安全技术网络安全等级保护安全设计技术要求》

8. GBT 20984-2022《信息安全技术 信息安全风险评估规范》

9.《信息安全技术信息系统安全等级保护测评要求》（国标报批稿）

10.GB/Z 24363-2023《信息安全风险管理指南》

11.GB/T 22080-2008《信息安全管理体系要求》

12.GB/T 22081-2008《信息安全管理实用规则》

13.GB/T 20269-2006《信息系统安全管理要求》

14.GB 50173-2008《电子信息系统机房设计规范》

15.GB/T 25062-2010《信息安全技术服务器测评要求》

16.GB/T 20010-2005《信息安全技术包过滤防火墙评估准则》

17.GB/T 20011-2005《信息安全技术路由器安全评估准则》

18.GA/T 672-2006《信息安全技术终端计算机系统安全等级评估准则》

19.GA/T 712-2007《信息安全技术应用软件系统安全等级保护通用测试指南》

（五）测评内容

等级测评的现场实施过程由单元测试和整体测评两部分构成。单元测试是对应《信息安全技术信息系统安全等级保护基本要求》GB/T 22239-2019，各安全控制点的测评称为，具体可分为安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全制度管理、安全管理机构、安全管理人员、安全建设管理和安全运维管理等 10 个测评任务。整体测评是在单元测评的基础上，通过进一步分析信息系统安全保护功能的整体相

关性，对信息系统实施的综合安全测评。

测评工程师在进行各单元测评之前，需获得被测评方的授权，并签署安全保密协议，在现场测评过程中，需要对设备和系统进行一定验证测试工作，部分测试内容需要上机查看一些信息，可能会影响系统的正常运行。因此，在进行验证测试和工具测试时，应尽量避开业务高峰期，同时还应对关键数据做好备份工作，并对可能出现的影响制定相应的处理方案。上机验证测试原则上应是测评人员提出需要查看或验证的内容，由测评委托单位的相关技术人员进行操作，测评人员根据操作结果进行记录。测评工程完成后，测评人员应交回测评过程中获取的所有特权，归还测评过程中借阅的相关资料文档，并严格清理测评过程中植入被测评系统中的相关代码/程序。

（1）安全物理环境：物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护；

（2）安全通信网络：网络架构、通信传输、可信验证；

（3）安全区域边界：边界防护、访问控制、入侵防范、恶意代码防范和垃圾邮件防范、安全审计、可信验证；

（4）安全计算环境：身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护；

（5）安全管理中心：系统管理、审计管理、安全管理、集中管控；

（6）安全制度管理：安全策略、管理制度、制定与发布、评审和修订；

（7）安全管理机构：岗位设置、人员配备、授权和审批、沟通和合作、审核和检查；

（8）安全管理人员：人员录用、人员离岗、安全意识教育培训、外部人员访问管理；

（9）安全建设管理：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、工程实施、测试验收、系统交付、服务供应商选择、等级测评；

（10）安全运维管理：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、网络和安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理、外包运维管理。

（六）测评清单

序号	系统名称	测评级别
1	贵州省社保基金财务管理系统	3
2	贵州省社保三险合一系统	3
3	贵州省社会保障卡一卡通综合服务平台	3
4	贵州省劳动关系管理信息系统	3
5	贵州省全民参保信息系统	3
6	贵州省社会保险基金收支安全管理平台	3
7	贵州省社会保障卡持卡人员基础库系统	3
8	贵州省机关事业单位养老保险及职业年金信息系统	3
9	贵州省人力资源社会保障生物识别综合服务平台	3
10	贵州省社会保险网上服务系统	3
11	贵州省机关事业单位工资管理信息系统	3
12	贵州省电子社保卡综合服务平台	3
13	贵州省职业年金代理人受托监督平台	3
14	人社统一门户系统	3
15	贵州省工伤认定鉴定系统	3
16	贵州人力资源社会保障网	3
17	贵州省劳动力培训就业信息系统	3
18	贵州省人才人事综合业务管理服务平台	3
19	贵州省劳动人事争议调解仲裁办案系统	3
20	贵州省流动人员人事档案管理系统	3
21	贵州省“互联网+人社”公共服务平台和监管平台	3
22	贵州省劳动用工大数据综合服务平台	3
23	贵州省劳务就业大数据平台	3
24	贵州省专业技术人员继续教育平台	3
25	跨部门大数据应用平台	3
26	贵州省人才博览会系统	3
27	贵州省实名制职业培训管理信息系统（二期）	3
28	贵州人事考试信息系统	3
29	地理应用（GIS）平台	2

三、风险评估需求

根据《GBT 20984-2022 信息安全技术 信息安全风险评估规范》按如下要求开展风险评估。

（一）资产识别

1.全面梳理资产清单。需对信息系统涉及的所有资产进行详细梳理，包括但不限于硬件资产（如服务器、存储设备、网络设备、终端设备等）、软件资产（如操作系统、数据库管理系统、业务应用程序、中间件等）、数据资产（如用户数据、业务数据、系统配置数据等）、人员资产（如系统管理员、业务操作人员等）以及服务资产（如云计算服务、网络通信服务等）。

2.确定资产属性。明确每项资产的关键属性，例如硬件资产的型号、配置、购置时间、使用年限等；软件资产的版本号、授权情况、开发商信息等；数据资产的类型（结构化数据、非结构化数据）、敏感程度（公开数据、内部数据、敏感数据、机密数据等）、存储位置等；人员资产的岗位职责、权限等级等；服务资产的服务级别协议（SLA）、服务提供商等。

3.分析资产价值。依据资产在业务运营中的重要程度、对组织的影响程度以及遭受破坏后可能造成的损失等因素，采用定性与定量相结合的方法对资产价值进行评估。例如，对于存储核心业务数据的服务器，由于其数据丢失或损坏将严重影响业务正常运转，可赋予较高的价值评分；而普通办公用打印机对业务影响较小，价值评分相对较低。

（二）威胁识别

1.收集威胁信息。通过多种渠道收集与信息系统相关的威胁信息，包括行业安全报告、安全漏洞库、网络安全事件案例、供应商安全通告等。同时，结合网络运营者所在行业特点和业务场景，分析可能面临的特定威胁。

2.识别威胁类型。对收集到的威胁信息进行分类和整理，识别出常见的威胁类型，如自然灾害（地震、洪水、火灾等）、人为失误（操作错误、配置不当等）、恶意攻击（网络攻击、病毒感染、数据窃取等）、设备故障（硬件损坏、软件崩溃等）、外部环境变化（政策法规调整、市场竞争等）。

3.分析威胁来源。针对每种威胁类型，进一步分析其来源，例如恶意攻击的威胁来源可能是黑客组织、竞争对手、内部不满员工等；自然灾害的威胁来源则是自然环境因素。同时，评估威胁发生的可能性，可根据历史数据、行业统计信息以及专家经验进行判断。

（三）脆弱性识别

1.技术脆弱性识别。采用多种技术手段对信息系统进行脆弱性检测，包括漏洞扫描（使用专业的漏洞扫描工具对系统进行全面扫描，检测操作系统、数据库、应用程序等存在的已知漏洞）、渗透测试（模拟黑客攻击，对系统进行深度测试，发现潜在的安全漏洞和薄弱环节）、代码审计（对应用程序的源代码进行审查，查找代码层面的安全缺陷，如 SQL 注入漏洞、跨站脚本攻击漏洞等）。

2.管理脆弱性识别。对信息安全管理制度、流程和人员管理等方面进行评估，查找管理上的漏洞。例如，检查安全管理制度是否完善，是否涵盖了人员管理、访问控制、数据备份、应急响应等关键环节；安全流程是否合理，是否存在冗余或缺失的步骤；人员安全意识培训是否到位，员工是否具备基本的信息安全知识和操作技能等。

3.物理环境脆弱性识别。对信息系统所处的物理环境进行评估，检查物理安全措施是否有效，如机房的防火、防水、防盗、防雷击等设施是否齐全；设备的摆放是否合理，是否便于管理和维护；物理访问控制是否严格，是否存在未经授权人员进入机房的风险等。

4.管理脆弱性识别。应深入到每个管理流程的细节，通过访谈、文档审查和实地观察等方式，发现潜在的管理风险。对于发现的管理问题，需制定具体的整改计划和时间表。物理环境脆弱性识别要进行至少 3 次不同时间段的实地检查，确保评估结果的准确性和全面性。

（四）风险计算分析

1.确定风险计算方法。根据资产价值、威胁发生的可能性和脆弱性严重程度，选择合适的风险计算方法，如矩阵法、定量分析法等。制定风险评估标准和等级划分规则，明确不同风险等级对应的风险值范围。

2.计算风险值。将资产识别、威胁识别和脆弱性识别的结果代入风险计算模型，计算每项资产面临的风险值。例如，对于某项资产，若其资产价值为高，面临的威胁发生可能性为中，脆弱性严重程度为高，则通过风险计算模型得出该资产的风险值，并根据风险等级划分规则确定其风险等级。

3.分析风险结果。对计算得出的风险值和风险等级进行分析，识别出高风险、中风险和低风险资产，以及需要优先处理的风险点。分析风险之间的关联关系，评估风险对信息系统整体安全和业务运营的影响程度。同时，提出风险应对策略建议，包括风险规避、风险降低、风险转移和风险接受等措施。

四、网络与数据安全众测服务

开展全省人社业务系统众测，众测过程除使用常用的渗透方法外，众测团队还可运用自身开发的拥有专利的检测工具。测试内容包括但不限于如下内容：

（一）逻辑安全

1.业务逻辑缺陷：验证关键业务流程（如身份核验、审批流转）是否存在逻辑冲突、验证机制薄弱（如 OTP 可重复使用）等问题。

2.业务流程合规性：检查业务执行是否符合规范，防范因流程错误导致的数据篡改或越权操作。

（二）身份认证与权限控制

1.越权漏洞

水平越权：验证同权限用户间数据隔离（如 A 用户访问 B 用户社保数据）。

垂直越权：测试普通用户能否提权至管理员功能（如配置修改）。

2.登录凭证缺失：检测接口/功能是否未校验 Token 或 Session，导致未授权访问敏感操作。

3.Cookie/Session 设计：检查 Cookie 生成算法复杂度、Session 超时机制，防止会话劫持。

（三）输入验证与注入防护

1.SQL/OS 命令/XXE 注入：测试所有输入点（表单、API 参数）是否存在注入风险，验证过滤规则。

2.XSS 漏洞：验证反射型、存储型、DOM 型 XSS，检查输入输出编码（如<script>是否转义）。

3.文件上传漏洞：尝试上传 webshell（如.php 文件），验证黑白名单策略及内容扫描机制。

（四）接口与数据安全

1.接口防护

枚举攻击：关键接口（如短信验证码、密码重置）是否设置速率限制、验证码或锁定策略。

数据暴露：检查 API 返回数据是否包含多余字段（如数据库 ID、未脱敏信息）。

2.数据脱敏一致性：比对前端展示与后端接口数据，确保全链路脱敏（如身份证号仅

显示前 3 位）。

3.批量导出管控：验证数据导出功能是否限制单次数量、需二次认证（如短信确认）。

（五）服务与配置安全

1.组件安全配置：扫描 FTP/Redis/Docker 等服务，检测弱密码、未授权访问及冗余端口。

2.解析漏洞：检查 IIS/Apache/Nginx 版本及配置，避免畸形文件名解析（如 test.jpg/.php 执行）。

3.SSRF 防护：测试内网探测能力（如 http://内网 IP:端口请求），验证 URL 过滤有效性。

（六）会话与请求安全

1.CSRF 漏洞：检查关键操作（如密码修改）是否校验 Referer 或 Token，防止跨站伪造请求。

2.信息泄露：检索 GitHub 等平台是否泄露源码，审查错误页面是否暴露路径或版本信息。

（七）用户管理

1.注册安全：验证是否要求实名认证，是否存在自动登录漏洞及批量注册防护（如 IP 限制）。

2.登录设计：检查免登录查询功能是否依赖敏感标识（如身份证号），防止信息泄露。

五、服务要求

（一）定级备案要求

1.合同签订后 180 个工作日内完成公安部门系统定级评审；信息系统的评测和复测工作，并出具《信息系统等保符合性报告》、《网络安全等保测评报告》。

2.依据现有安全防护措施、管理制度及公安部相关要求，编制《信息系统保护工作方案》，并将方案及时报送属地公安部门备案。

3.按照公安部具体规范与要求，整理、编写配套支撑资料，与工作方案同步提交至属地公安部门，确保符合监管标准。

（二）网络与数据安全众测要求

1.众测数量与要求

（1）服务期内需提供1次至少50个资产的众测服务，参与众测人员不少于30人，众测时间不少于15日，众测内容禁止在互联网上公开发布，众测活动须经省人社厅书面授权后方可开展，具体时间、范围及要求以通知为准。

（2）众测人员可为自有人员或定向邀请人员，众测人员需在互联网应急中心报备。

（3）需对参与众测人员须的身份信息、无犯罪记录证明及技能水平证明等材料（近五年内取得的CNVD原创高危漏洞证明）进行审核确认，最终人员名单由省人社厅审查确定。

（4）需配备项目负责人统筹众测全流程，包括活动组织、结果核实、漏洞通报与复核。发现高危漏洞及时反馈并跟踪修复情况，众测结束后15个工作日内完成统计分析并提交总结报告。

2.众测平台要求

（1）需提供安全可靠的众测平台开展本次众测服务。

（2）平台须具备对众测活动全程管控功能，能实时展示众测进度、漏洞提交、验证、修复、跟踪等数据。

（3）平台须具备统一出口IP并且提前向省人社厅报备。

3.人员管理与保密

（1）所有众测人员需签署保密协议，禁止利用测试权限进行非法操作，禁止泄露测试中接触的省人社厅业务数据、系统架构、用户信息等内容。

（2）众测人员通过 VPN 等方式接入众测平台的专属虚拟测试终端，虚拟终端禁止导出相关数据。众测结束后，众测人员需彻底删除存储数据，包括测试日志、截图等。众测过程中若产生测试数据，应及时告知省人社厅并对测试数据进行标记。

4.审计要求

（1）在众测过程中，需通过技术、管理等手段控制风险，保障不发生风险事件。

（2）应对众测人员的测试过程实施审计监控，确保其行为符合法律法规及测试规范。

（三）验收条件

（1）完成等保测评并出具《信息系统等保符合性报告》《信息系统安全等级测评报告》，同步完成公安机关备案工作，取得定级备案证明；按要求制定《信息系统安全保护工作方案》并提交。

（2）根据法律法规及标准要求，开展信息系统风险评估工作，按规定出具报告，并就报告中的安全风险进行详细阐述说明。

（3）完成众测服务并出具《众测服务报告》，同时提交众测人员保密协议及其它材料（身份信息、无犯罪记录证明及技能水平证明等）。

（四）交付物

序号	交付物	备注
1	29 个系统的《信息系统备案证明》	每个系统一份
2	29 个系统的《信息系统等保符合性报告》	每个系统一份
3	29 个系统的《信息系统安全等级测评报告》	每个系统一份
4	28 个系统的《信息系统风险评估报告》	每个系统一份
5	1 份《众测服务报告》《人员保密协议》	
6	1 份《信息系统保护工作方案》	

六、商务条款

（一）服务期及服务地点

服务期：1 年，从签订合同之日起计算。

服务地点：采购人指定地点。

（二）付款方式

签订合同满足付款条件后 10 个工作日内，支付合同金额的 100%，中标单位向采购人提交合同款项的 70%的银行保函，开具的保函有效期至少一年，保函内需明确只有通过采购人验收后，才能解锁保函资金。如在保函有效期内未按规定完成服务或无法通过采购人组织的验收，需延长保函授权。待全部项目服务期满并通过验收后，退还银行保函。具体付款

方式以合同约定为准。

（三）其他要求

1.投标人的投标报价包括但不限于人员工资、团队建设、运维费用、专用工具价、培训费、咨询服务费、各种税费等完成本项目所需的一切费用及所有风险防范费用，即总价包干。投标报价为一次性报价，即在投标有效期和合同有效期内，该报价固定不变。

2.如因国家政策或法规变化、项目财政预算调整或技术要求变化、其他不可抗力等原因造成采购人需求变更的，采购人有权根据实际情况调整采购需求，直至合同取消，采购人对此变更不承担任何责任。

3.实施过程中，投标人履行安全职责，对安全负责，应采取必要的安全措施，并按照国家有关法律、行政法规、操作规程等开展运维服务，服从采购人的要求,保障采购人系统及数据安全。

4.安全监督和管理。由投标人责任造成的人身伤亡、机械事故及其他财产损失均由投标人承担，此风险费已包含在投标人投标报价中。

5.投标人须承诺：若成为中标人将无条件接受采购人为保证项目运行而进行的安排调度，如因不服从采购人安排调度造成项目服务中断的，采购人有权终止合同另行选择投标人，中标人须赔偿因此产生的费用及影响进度对采购人造成的损失。

6.采购人有权在与中标单位签订合同前核验其提供的证明文件、业绩及各种投标文件内提供的证书的原件。原件不齐或与发证机构、签约单位等核实原件存在不实的，采购人有权取消其中标资格并上报相关监管部门进行处理，给采购人造成的损失，中标单位应当予以承担赔偿责任。

7.投标人须承诺：单位负责人为同一人或者存在直接控股、管理关系的不同投标人，不同时参加同一合同项下的政府采购活动。

8.其他未尽事宜，待中标签约时双方再议。

9.本项目中所有信息只能用于评估，未经授权不应泄露、出售或者非法向他人提供。