第1章开标一览表（报价表）

开标一览表（报价表）

杭州市人力资源和社会保障政务服务中心、浙江天弘招标代理有限公司：

按你方招标文件要求，我们，本投标文件签字方，谨此向你方发出要约如下：如你方接受本投标，我方承诺按照如下开标一览表（报价表）的价格完成2024-2025年度杭州市人力社保网络安全维护项目【招标编号：THZB-24PC35039】的实施。

开标一览表（报价表）(单位均为人民币元)

序号	名称	服务范围	服务要求	服务时间	服务标准	服务人数	备注
1	网络安全驻场	杭州市人力社保所有信息系统	1、协助加固服务 根据安全评估结果的具体情况，制定加固建议，协助进行安全漏洞加固处理，包括漏洞补丁更新，安全防护策略优化，指导开发修复漏洞代码等，并检验漏洞修复完成情况，形成漏洞跟踪管理闭环。 2、主机安全管理服务	2024年9月1日--2025年8月31日	《系统资产清单》、《漏洞扫描报告》、《基线检查报告》、《日志分析报告》、《网络安全工作月报》，《网络安全工作	2	无

			为服务器提供针对性的技术手段对服务器进行防护，对终端资产和安全情况进行全面掌握、清晰、准确判断存在的安全风险，对终端发生的安全事件及时响应处理。 3、组织协调渗透测试服务 梳理确认各项目实施阶段需要开展渗透测试的对象，组织协调供应商内部渗透测试实施团队进行远程或者入驻现场开展渗透测试工作，把握渗透测试实施进度，进行结果汇总，向政务服务中心相关部门反馈结果。 4、漏洞扫描服务 采用远程安全评估系统，通过定制的扫描规则，形成安全扫描策略文档，对服务器、网络设备、安全设备等进行自动化安全扫描，人工验证扫描结果并输出安全扫描报告及修复建议。 5、基线核查服务 根据既定的检查规范及方法，采用人工检查用表（checklist）、脚本程序或基线扫描工具对评估目标范围内的主机系统安全、数据库安全、中间件安全等进行系统的策略配置、服务配置、保护措施以及系统和软件升级、更新情况，是否存在后门等内容进		年报》		

			行检查。 6、协助安全检查 协助市人力社保局编制安全检查方案，采用各种网络安全检测手段，对人力社保局指定的下属单位的信息系统网络安全状况展开全面的安全检查，对于存在安全隐患的单位提出整改建议，配合人力社保局督促下属单位开展整改工作。 7、日志审计服务 定期对内网全网所有日志中的高级别日志进行分析，对安全事件进行溯源，并出具分析报告。结合人工方式，结果综合日志审计平台、设备、系统自身的日志数据进行综合分析，判断网络、操作系统、应用中间件、网络安全设备等资产的整体运行情况、安全状况等。 8、数据库审计服务 开展数据库审计分析服务，监视并记录对数据库服务器的各类操作行为，通过对访问数据库相关数据的分析，实时地、智能地解析对数据库服务器的各种操作，并记入审计数据库中以便日后进行查询、分析、过滤，实现对目标数据库系统的用户操作的				

			监控和审计。 9、综合日志分析服务 通过综合日志审计平台，提供审计服务。通过全面收集云内安全设备、主机、应用及数据库的 Syslog、SNMP 等日志协议信息。 10、定期汇报网络安全整体状况 每月定期向中心相关管理人员和领导汇报网络安全运营情况，使相关领导能够及时掌握网络安全漏洞检测与整改情况、网络安全技术措施推进进程和成效、网络安全整体状况等。				
2	专网管控驻场	杭州市人力社保专网管控平台	1、保障杭州市人力资源和社会保障专网管控平台的正常运行，包括平台的 WEB 页面、数据库、管理器、服务器的正常运行。主要包括以下服务内容： （1）入网设备及应用系统的注册管理工作：对新入网注册的设备进行安全检查，包括杀毒软件是否安装、是否安装违规软件等。对应注册未注册的设备实施阻断。 （2）对各类违规事件的监测、提醒、预警、通报工作，以及对预警告知书回执和整改通知书回执的初审、催交等工作。 （3）根据用户的管理需求，对平台的策略配置进行修改，并统	2024 年 9 月 1 日--2025 年 8 月 31 日	《专网管控工作周报》	1	无

			计、导出用户管理所需的数据。 （4）协助用户做好监测到违规事件的查处工作。 （5）根据用户的需求，做好平台的相关培训工作。 2、为保证杭州市人力资源和社会保障局安全管理平台的稳定运行，参与本维护项目的技术人员必须经过平台原厂培训，在投标文件中进行相应承诺，否则按无效标处理。中标后若无法兑现的，视为违约处理。 3、要求技术维保人员无违反犯罪记录，品行良好，责任心强，能严格遵守杭州市人力资源和社会保障局各项规章制度。 4、根据平台的运行情况，免费对平台进行完善升级，升级后向杭州市人力资源和社会保障局提交新版本介质和相关说明。 5、故障应急响应服务。提供7*24小时技术支持热线，平台出现故障和问题时，技术人员必须提供技术服务，并解决故障和问题。如远程无法解决的问题，技术人员必须1小时内响应，2小时内到现场提供技术服务。				
3	数据安全驻场	杭州市人力社保所有信	1、负责使用数据库安全产品（数据库准入系统、数据库防火墙，数据库综合运维系统），对数据库进行日巡检、周巡检、月度巡	2024年9月1日--2025年	《数据安全工作周报》	1	无

		息系统的数据库	检、季度巡检；保障数据库正常运行。负责配合杭州市人力社保中心DBA团队处理数据库相关故障；如用户有需要，能不限次的配合DBA团队进行数据库的性能优化调整、数据库索引调整建议、SQL语句优化建议、数据库升级和数据迁移服务。 2、配合杭州市人力社保中心DBA团队进行业务系统的数据库数据同步，保障相关数据安全，包括数据同步、数据备份部署、巡检、性能优化、对特定数据源按指定规则进行一次性脱敏处理等。 3、用户数据库系统发生安全故障时，驻场工程师应立即进行故障分析、判定等准备工作并立即着手解决故障，如驻现场工程师解决不了，服务商要及时派其他相关工程师做现场服务，现场服务次数和时间不限。对于严重故障（影响核心业务正常运行的故障），要求半小时内修复。对于一般故障（影响用户一般业务正常运行的故障），要求 4 小时内修复。对于轻微故障（不影响用户业务正常运行的故障），要求24小时内修复。在规定的时间内无法修复系统，服务商须及时采取应急措施，确保系统的正常运行。故障处理完毕三个工作日内，服务商须提供“故障报告”	8月31日			

			给用户。 4、数据库版本升级BUG修复 配合杭州市人力社保中心DBA团队进行数据库升级、打补丁和BUG修复。负责提供升级数据安全评估规划，制定在线升级方案，使数据库升级后运行效率更高，包括： 评估数据库升级带来的优点和可能产生的问题； 保证产品升级的过程中数据的安全性； 顺利、快速地从一个软件版本升级到另一个版本，减少业务的停机时间； 服务团队要求精通达梦、Oracle、Mysql、Oceanbase数据库各种升级方法，精通各种在线维护和在线割接技术。 5、数据库安全隐患排查，安全分析和管理 数据库安全至关重要，数据库的可用性、机密性和完整性缺一不可。每月至少提供一次数据库安全隐患的排查服务，如需使用相关工具完成检查工作的，由服务提供方自行解决。 服务提供方需提供检查报告，报告中的内容至少包括： 数据库核查包括：用户帐号、密码策略（密码复杂度）、日志配				

			置、权限控制、版本补丁等。 漏洞覆盖：SQL注入漏洞、权限绕过漏洞、缓冲区溢出漏洞、访问控制漏洞等。 6、数据资产与流动管理平台管理和运维 做好数据资产与流动管理平台管理和运维，包括程序优化改造、数据统计、数据处理、新增需求开发等相关工作，保障统一身份管理平台与人社统一门户的信息同步。				
4	设备维保服务	13台设备	针对市人力社保局政务服务中心机房网络信息安全设备的维保服务，包括设备故障处理、备件更换和软件升级等技术支持服务。	2024年9月1日--2025年8月31日	《设备维保报告》	2	无
5	网络安全资产管理	所有内网IT资产	提供资产管理软件，软件使用开源架构，支持定制开发，梳理杭州市人力社保内外网所有信息系统涉及的信息化资产（服务器、网络设备、安全设备、数据库等），将信息化资产录入到产管理软件，要求能够直观的对信息化资产进行展示、统计、查询和导出。	2024年9月1日--2025年8月31日	《资产管理报告》《信息化资产列表》	3	无
6	等级保护咨询	三个三级、五个二级	针对等级保护定级、设计、实施、整改、运行等各阶段工作内容和工作重点进行梳理，提供等级保护全阶段过程的支持和服务。	2024年9月1日--2025年	《信息系统定级报告》、《信息系统备案	3	无

	服务			8月31日	表》、《信息系统等级保护差距评估报告》、《信息系统整改建设方案》等。		
7	等级保护测评服务	三个三级、五个二级	由拥有公安部颁发的等级测评资质的测评机构开展等级测评工作，完成信息系统安全等级测评工作，出具加盖测评机构公章的信息系统安全等级测评报告，根据公安机关要求完成备案。	2024年9月1日--2025年8月31日	《信息系统等级测评报告》	2	无
8	渗透测试服务	所有信息系统	通过模拟黑客使用的工具、分析方法对网站进行安全测试，并结合智能工具扫描结果，由高级工程师进行深入的手工测试和分析，识别工具弱点扫描无法发现的问题。主要分析内容包括逻辑缺陷、上传绕过、输入输出校验绕过、数据篡改、功能绕过、异常错误以及其他专项内容。	2024年9月1日--2025年8月31日	《信息系统渗透测试报告》	3	无
9	新系统上线前检测	新上线系统	针对新上线的信息系统开展安全性渗透测试和整体安全评估。模拟黑客对信息系统等进行非破坏性质的攻击性测试，及时发现存在的安全漏洞，提出安全建设整改建议，作为漏洞修复和加固整改的参考依据。	2024年9月1日--2025年8月31日	《新系统上线前检测报告》	2	无
10	安全大	所有信息系	定期对内网全网日志中的高级别日志进行分析，对安全事件进	2024年9月	《安全大数据分析报	3	无

	数据分析服务	统	行溯源、满足《网络安全法》日志存储不少于6个月的要求，并出具分析报告。结合人工方式，结果综合日志审计平台、设备、系统自身的日志数据进行综合分析，判断网络、操作系统、应用中间件、网络安全设备等资产的整体运行情况、安全状况等。直观展现上述内容给杭州人社。提出整改意见，帮助整改。	1日--2025年8月31日	告》		
11	高级威胁分析服务	所有信息系统	通过专业的APT检测工具和人工分析相结合的方式，定期深入分析信息系统中存在的高级安全威胁，提升信息系统的防护水平。	2024年9月1日--2025年8月31日	《APT威胁分析报告》	1	无
12	网络安全攻防演练服务	所有信息系统	根据杭州市人力社保政务服务中心安排，参加公安、人社部等相关部门组织的护网行动，负责承担网络安全攻防演练相关工作，确保杭州市人力社保在演练中排名前列。	2024年9月1日--2025年8月31日	《攻防演练总结报告》	6	无
13	重要时期安全保障	所有信息系统	在两会、护网行动等重要活动时期，为确保市人力社保局信息系统及设备安全性、保密性、服务可用性,安排安全专家现场驻场值守，必要时提供7*24小时人员现场值守，提供重要时段安全保障技术服务，对发现的可疑情况和网络攻击行为，及时与政务服务中心值班人员联系，并协助进行事件处理。	2024年9月1日--2025年8月31日	《重大活动保障报告》	4	无

14	应急预案建设	所有信息系统	为了保障应急响应的服务质量，定期修订、完善应急预案，通过专业化的网络安全应急咨询服务，帮助建立健全应急响应组织以及预防、预警机制，针对信息系统特点和可能的突发性安全事件拟制规范的应急处理流程，落实物质条件、人力和技术支撑等保障措施，制定出规范、全面、体系化的应急预案。	2024年9月1日--2025年8月31日	《网络安全应急预案》	2	无
15	应急演练服务	所有信息系统	根据应急预案规定的应急处理流程协助用户编制应急演练方案，并进行相应模拟演练，一方面使相关方熟悉应急响应流程，提高对安全事件的响应能力；另一方面验证预案正确性和适用性，进行总结分析，根据需要对应急预案进行修订。使得相关人员了解应急流程和自己的责任，在安全事件发生时，能够有条不紊开展工作，最大程度降低安全事件带来的负面影响和损失。	2024年9月1日--2025年8月31日	《网络安全应急演练总结》	8	无
16	应急响应服务	所有信息系统	根据事件类别，通过远程和现场支持的形式协助客户对遇到的突发性安全事件进行紧急分析和处理。主要工作内容包括：突发事件相关信息的收集、事件的分析、报告提交、问题解决建议等。紧急事件主要包括：病毒和蠕虫事件、黑客入侵事件等。	2024年9月1日--2025年8月31日	《网络安全事件应急处置报告》	3	无
17	安全规划服务	所有信息系统	根据国家信息安全相关规定，分析信息系统安全现状和需求，结合国际和国内信息安全发展动态，编制信息安全规划。	2024年9月1日--2025年	《安全规划方案》	2	无

				8月31日			
18	网站安全监测服务	所有信息系统	提供7*24小时监测服务，主要包括漏洞扫描、木马分析、篡改监测、关键字监测、网站可用性监测，提供全面的事前、事中的安全监测。（先知、云监测）	2024年9月1日--2025年8月31日	《监测月报》、《监测季报》、《监测年报》、《重大事件报告》	2	无
19	云防护服务	外网所有信息系统	提供7*24小时云安全防护服务，完成WEB安全防护、DDOS防护等。	2024年9月1日--2025年8月31日	《防护报告》、《重大安全事件告警》	2	无
20	安全通告服务	所有信息系统	定期提供最新病毒的防御方案、最新系统漏洞信息及其修复方法、最新发生的安全事件等内容的安全通告报告。	2024年9月1日--2025年8月31日	《网络安全通告》	2	无
21	数据安全服务	所有信息系统	提供根据用户需要负责数据库访问控制、脱敏、安全审计运维服务。	2024年9月1日--2025年8月31日	《数据安全维护报告》	2	无
22	安全咨询服务	所有信息系统	安排资深专业的安全专家作为人社局的网络安全顾问，根据局网络安全建设、维护、整改、审查等方面方案评审、实施落地的需求，采用远程或者现场的方式不定期提供专业、可行、超前的建设性建议。	2024年9月1日--2025年8月31日	《安全咨询服务报告》	2	无

23	安全培训服务	所有信息系统	面向采购单位全员开展专业的网络与信息安全意识培训，提高受众个人隐私保护、常规攻击防护、信息安全管理等能力，增强个人网络安全防护意识，规避网络攻击风险。	2024年9月1日--2025年8月31日	《网络安全培训大纲》《网络安全培训课件》	4	无
24	云平台安全服务和密码服务	所有信息系统	政务云平台上的等级保护安全服务（防病毒、日志审计、数据库审计）和商用密码服务	2024年9月1日--2025年8月31日	《信息系统商用密码应用安全性评估报告》	2	无
25	商用密码应用安全性评估与加固服务	等保三级系统	由拥有商用密码应用安全评估资质的测评机构开展商用密码应用安全性评估工作，根据评估进行相关加固，出具加盖测评机构公章的评估报告，并完成相关备案。	2024年9月1日--2025年8月31日	《信息系统商用密码应用安全性评估报告》	3	无
投标报价（小写）				3089000元			
投标报价（大写）				叁佰零捌万玖仟元整			

注：

1、投标人需按本表格式填写，**否则视为投标文件含有采购人不能接受的附加条件，投标无效；**。

2、有关本项目实施所涉及的一切费用均计入报价。**采购人将以合同形式有偿取得货物或服务，不接受投标人给予的赠品、回扣或者与采购无关的其他商品、服务，不得出现“0 元”“免费赠送”等形式的无偿报价，否则视为投标文件含有采购人不能接受的附加条件，投标无效；采购内容未包含在《开标一览表（报价表）》名称栏中，投标人不能作出合理解释的，视为投标文件含有采购人不能接受的附加条件的，投标无效。**

3、特别提示：采购代理机构将对项目名称和项目编号，中标供应商名称、地址和中标金额，主要中标标的名称、服务范围、服务要求、服务时间、服务标准等予以公示。

4、符合招标文件中列明的可享受中小企业扶持政策的投标人，请填写中小企业声明函。注：投标人提供的中小企业声明函内容不实的，属于提供虚假材料谋取中标、成交，依照《中华人民共和国政府采购法》等国家有关规定追究相应责任。