湖北中心2024-2027年内外网信息化维保服务采购项目

采购需求

一、项目基本情况

1、项目编号：HBT-13324115-241653

2、项目名称：湖北中心2024-2027年内外网信息化维保服务采购项目

3、预算金额：一年服务预算不超过人民币213万元，三年总服务预算不超过人民币639万元，具体如下：

服务名称	服务期	年服务预算（万元）	总服务预算（万元）
内外网信息化维保服务	3年	179.90	539.70
内网邮件运维服务	3年	23.10	69.30
网络安全服务	3年	10.00	30.00
一年服务预算不超过213万元，三年总服务预算不超过：639万元。			

二、采购内容

1、维保服务内容

内外网信息化系统运维服务包括：内网设备运维、外网设备运维、其他网络设备、服务器及语音网关、内网邮件系统运维、网络安全服务。具体设备涵盖网络设备、安全设备、存储设备、服务器及操作系统、应用软件等。投标人应充分了解维保的所有设备类型、配置、系统软件等情况，一旦中标，对于出现的任何故障将认为投标人认同并提供服务。

2、服务时间：

（一）内外网信息化维保服务内容清单（维保服务期：3年。合同签订日起）

内网设备	序号	设备名称	规格用途	单位	数量	厂家	备注
	1	内网路由器	NE40E-X8全业务路由	台	2	华为	

			器				
	2	内网核心交换机	S12708 敏捷交换机	台	2	华为	
	3	内网汇聚交换机	S9706 核心路由交换机	台	3	华为	
	4	内网服务器接入交换机	S7706 智能路由交换机	台	2	华为	
	5	内网 WEB 应用防火墙	WEB 应用防护系统	台	2	深信服	含特征库升级
	6	内网防火墙	第二代防火墙	台	4	深信服	含特征库升级
	7	内网入侵防御系统	网神 SecIPS3600 入侵防御系统	台	4	网神	含特征库升级
	8	内网防毒墙	网神 SecAV 3600 防毒墙	台	2	网神	含特征库升级
	9	内网运维审计系统	网神 SecFox 运维安全管理与审计系统	台	1	网神	含特征库升级
	10	内网网络审计	互联网网络审计系统	套	1	深信服	含特征库升级
	11	内网漏洞扫描	漏洞扫描系统 V6.0	台	1	网御	含特征库升级
	12	财务专网接入交换机	华为 S5720 以太网交换机	台	1	华为	
	13	财务专网统一安全网关	第二代防火墙	台	2	深信服	含特征库升级
	14	财务专网数据库安全审计	网神 SecFox 安全审计系统	台	1	网神	含特征库升级
	15	内网基础应用服务器	HP DL380 Gen9 8SFF CTO Server	台	13	紫光华山	
	16	邮件服务器	HP DL580 Gen9 CTO Svr	台	2	紫光华山	

	17	虚拟化服务器	HP DL580 Gen9 CTO Svr	台	2	紫光华山	
	18	统一存储系统	3Par 20800	台	1	紫光华山	
	19	NAS 网关（双节点）	StoreEasy 3850	台	1	紫光华山	
	20	光纤交换机	OceanStor SNS2248	台	2	华为	
	21	服务器操作系统	服务器操作系统	套	17	微软	
其他网络设备、服务器及语音网关	**序号**	**项目名称**	**设备名称**	**单位**	**数量**	**厂家**	**备注**
	1	防病毒服务器	HP DL580	台	1	HP	
	2	防病毒服务器	DELL PowerEdge R910	台	1	DELL	
	3	虚拟化	HUWEI RH5885H V3	台	1	华为	
	4	视频会议测试	HUWEI RH5885H V3	台	1	华为	
	5	深信服 VPN	HUWEI RH5885H V3	台	1	华为	
	6	人力资源服务器	IBM Systemx 3650 M4	台	1	IBM	
	7	人力资源服务器	IBM Systemx 3650 M4	台	1	IBM	
	8	中心内网服务器	DELL PowerEdge R720	台	1	DELL	
	9	FTP 服务器	SUGON1620-G10	台	1	SUGON	
	10	老集群打印	HP DL380	台	1	HP	
	11	新集群打印	HP DL380	台	1	HP	
	12	财务服务器	DELL PowerEdge R720	台	1	DELL	
	13	财务服务器	DELL PowerEdge R720	台	1	DELL	
	14	内网资产服务器	DELL PowerEdge R910	台	1	DELL	
	15	cas.hub 服务器	HP DL580	台	1	HP	
	16	cas.hub 服务器	HP DL580	台	1	HP	
	17	Mailbox 服务器	HP DL580	台	1	HP	
	18	Mailbox 服务器	HP DL580	台	1	HP	
	19	DHCP 服务器	HP DL380	台	1	HP	

	20	DHCP 服务器	HP DL380	台	1	HP	
	21	AD 域/DNS 服务器	HP DL380	台	1	HP	
	22	AD 域控	HP DL380	台	1	HP	
	23	AD 域/DNS 服务器	HP DL380	台	1	HP	
	24	AD 域控	HP DL380	台	1	HP	
	25	OA 服务器	IBM Systemx 3650 M4	台	1	IBM	
	26	OA 服务器	IBM Systemx 3650 M4	台	1	IBM	
	27	网站使用	HP DL380	台	1	HP	
	28	网站使用	HP DL580	台	1	HP	
	29	华为 eSpace 语音网关	华为 eSpace U1980	台	1	华为	
			华为 eSpace U1980	台	1	华为	
			HUWEI RH2285 V2	台	1	华为	
			HUWEI RH2285 V2	台	1	华为	
			HUWEI RH2285 V2	台	1	华为	
			HUWEI RH2285 V2	台	1	华为	
	30	接入交换机	华三 LS-5120-28SC-HI	台	**31**	华三	
	31	接入交换机	华三 LS-5120-28P-HPWR-SI-H3	台	1	华三	
	32	接入交换机	华三 S5120-48P-EI	台	**5**	华三	
	33	接入交换机	华三 S5120-28C-PWR-EI	台	1	华三	
	34	接入交换机	华三 S5120-52C-PWR-EI	台	**2**	华三	
	35	核心路由器	华三 SR6608-X	台	**2**	华三	
外网设备	**序号**	**项目名称**	**设备名称**	**单位**	**数量**	**厂家**	**备注**
	1	链路负载均衡	NS-SecPath L1000-M	台	2	H3C	含特征

							库升级
	2	行为管理+流控	ASG2200-AC	台	1	华为	含特征库升级
	3	下一代防火墙(出口)	USG6530	台	2	华为	含特征库升级
	4	服务器防火墙	USG6330	台	1	华为	含特征库升级
	5	核心交换机	S9706	台	2	华为	
	6	接入层 POE 交换机（24 口）	S5710-28C-PWR-EI-AC	台	10	华为	
	7	无线 AP	AP4030DN-AC	台	180	华为	
	8	无线 AP（86 盒）	AP2010DN	台	60	华为	
	9	无线 APP(高功率)	AP7030DE	台	39	华为	
	10	控制器	AC6605-26-PWR	台	2	华为	
	11	配套光模块		个	20	华为	
	12	配套光模块		个	50	华为	
	13	接入认证模块	Agile Controller 模块	个	1	华为	

（二）内网邮件系统运维服务内容（运维服务期：3年。2024年9月17日-2027年9月16日）

湖北中心目前内网邮件系统使用的为：国产的亿邮电子邮件系统，包含2000点的亿邮电子邮件系统客户端主平台软件、网关子系统、归档子系统、邮件收发客户端的运维服务和双机备份服务。

（三）网络安全服务内容（服务期：3年。2024年11月22日-2027年11月21日）

中心外网网站网络云安全服务。对网站的业务流量进行恶意特征识别及防

护，避免网站服务器被恶意入侵，保障业务的核心数据安全。

为主机提供云安全服务。实时识别、分析、预警安全威胁，防勒索、防病毒、防篡改、合规检查等安全服务。

中心信息系统漏洞扫描服务。在服务期内根据审协湖北中心网络安全要求，每季度至少提供1次的漏洞扫描和安全加固服务。

节假日及重大敏感时期7×24小时安全值守。在节假日及重大敏感时期，根据中心要求安排技术人员提供7×24小时信息安全值守。

三、维保要求

（一）总体维保要求：确保所有设备的安全、正常运行

1、建立维保技术服务项目组。组织相对固定的技术人员，人员结构要合理、技术全面。

2、采用项目经理负责制。指定专门的项目经理提供服务管理和协调，负责服务的组织管理、服务质量监控、服务资源的调度和与项目有关的重要文档的签署。

3、提供7×24×365小时维修服务电话和专人值班手机，7×24×365小时E-Mail服务；同时投标人提供服务工程师、客户经理、售后服务部经理三个联系电话，便于招标方机房值班人员7×24小时联系。

4、提供7×24×4小时现场支持。在合同有效期内的每周7天、每天24小时内，招标人可以通过电话反映合同产品内的问题，如果故障现象不能通过电话支持方式解决，中标单位技术人员需在接到电话后4小时内到达招标人现场提供现场支持服务。

5、提供软、硬件更新信息通知。针对招标文件中的设备清单，提供与该设备有关的关键性技术改进、产品重要的升级、可能对招标人应用有关的关键性BUG补丁等的发布信息，以便招标人可以根据其具体应用情况作出是否升级和安装补丁程序的决定。

6、提供系统联调与支持服务。当招标人根据需求对系统进行调整时（包括并不限于新增软硬件、软硬件升级更新、软硬件配置调整等），需根据招标

人需求，参与系统联调及实施方案制订，并完成招标范围内软硬件设备配置调整变更，配合完成系统联调及测试。

7、提供预防性维保服务：每年进行四次预防性维保服务或每三个月进行一次预防性维保服务。预防性维保服务包括现场巡检、调整优化以及为需要的部分更换设备。预防性维保及检测的时间应在不影响招标人设备使用的情况下进行协商确定。预防性维保服务具体内容至少包括如下方面：

①现场巡检包括检查、分析相关日志、诊断设备的运作状态，进行性能分析和评估，并提供巡检报告及故障处理报告等。

②调整优化包括优化系统软件和硬件，软件策略上的调整和补充以及硬件方面的规划和使用的优化，对设备进行保养和正常维保并提交维保报告等。

③更换设备包括为招标人提供招标范围内必要设备的备件。为使招标人设备处于良好的运行工作状态，提供与损坏的部件性能，质量，数量同等的备件。当招标人因部件影响正常任务，提供需更换的部件。

8、提供特征库升级服务：根据产品原厂商的升级信息，经招标人同意，为招标人提供特征库升级服务。

9、提供项目配合服务：招标人在实施重大项目，如系统切换、系统升级或机房搬迁等时，需要维保方配合或协助的，中标单位积极响应及时指派资深系统人员现场协助及指导，并提供现场技术支持。

10、服务许可：为了保障系统的安全，无论是远程操作还是现场支持，应事前得到招标人的同意，才能进行系统维保的相关操作。

11、服务期内，中标单位需按招标人的要求提供不限次数的配置更改、系统安装以及跟所维保设备相关的其他服务，如协助用户进行系统备份、保存和恢复等。

12、每次现场维保、维修后，须给出详细故障维修报告。内容应包括：详细记录故障设备型号、故障时间、故障类型、维保措施、维保时间及维修人员等信息，并交招标人签字认可，双方各留一份以备存档。每个月应提交：设备巡检报告、每个三个月应提交：故障维修汇总报告、健康性检查报告。每年必须提交年度工作总结报告，为下一年提供服务建议和服务方案。

13、中标单位需为招标人建立维保服务档案，记录所有设备系统配置、维

保记录等信息。

14、设备或材料产生损坏时，中标单位负责进行维修，8小时无法解决问题的，提供同等级别型号的备机，直至故障解决。

15、在维保期间，提供设备及系统的保修服务。保修服务包括维保、检测、设备免费维修和更换，提供的更换件不低于需要维修或现使用的产品档次。维保服务期内所有维保费用，包括人工费、设备更换费用、协调费用等均由中标单位方承担。

（二）内外网信息化维保服务具体要求

1、预防性维护

1)及时发现并通知招标方影响系统安全运行的软件漏洞和修补方法，经过招标方允许，方可实施。

2）根据招标方的要求，制定服务方案，按照日、月、季度等对本项目范围内对象进行预防性维护服务，包括系统巡检、设备巡检等，除特殊紧急情况下，预防性维护及检测的时间均在工作日内进行，具体时间双方商定确定。

3）中标方提供由高级工程师开展的每月的深度健康检查，每季度的预防性维护服务。深度健康检查方案由双方确定。

4）每年从网络拓扑结构、数据包分析、用户反馈问题等多角度多方面，完成年度网络、存储系统整体运行分析与报告。

2、故障处理

1）在招标方要求的时限内排除故障，恢复系统运行，包括进行故障定位、部件更换、故障分析报告等全部工作；中标方应承诺如果无法及时解决设备故障问题，需要在 4 小时内获得设备制造商后台技术力量的远程或现场支持服务。在设备发生故障而投标人无法及时解决，需要对设备配件更换时，投标人应提供与该产品相匹配的备件，如无法提供与之相匹配的配件的，投标人应提供同档次的产品替换故障设备，并完成原设备上系统及应用的转移工作。投标人应充分考虑该风险与责任，并将其成本计入投标报价，服务期内招标方不再额外付费。

2）针对网络及存储系统的整体故障，中标方要由专人负责跟踪落实，做好

详细记录。

3）中标方接到甲方故障报修后，24 小时内仍未解决问题，招标方有权调用第三方服务商的技术力量和备品备件用于本项目的服务，产生费用由中标方承担。

3、安全要求

1）中标方对运维工作的所有运维人员，必须进行安全教育，未经安全培训和教育者不得进入施工现场。

2）中标方运维人员应遵守招标人的相关安全规定。

3）中标方工作人员必须在招标人指定的工作范围内开展工作，不得跨越、移动其他设备缆线等；不得进入非工作区以外的设备运行区域进行其它活动。

4）中标方须与招标方签订保密协议，对招标方各种数据、各应用和设备相关情况严格保密。此保密义务不因合同的终止而免除。

5）在运维维护期间，中标方承诺按照二级等级保护相应级别要求维护系统运行。针对发现的安全问题，及时开展安全整改工作并提供报告。

6）配合整理信息安全检查及风险评估等相关材料。配合信息安全检查及风险评估，对信息安全检查及风险评估中发现的相关问题进行整改，直至通过整改等要求。

7）服务许可：为了保障系统的安全，无论是远程操作还是现场支持，中标方应事前得到招标方的同意，才能进行系统维护的相关操作；中标方工作人员进入招标方机房前应征得招标方的同意，并办好相应的登记手续，离开时按招标方要求留下相应的操作记录。

8）中标方需遵守招标方及受托管理方关于人员管理、机房管理、设备管理、运维管理、安全管理等方面的规章制度。

4、文档要求

1）每次技术支持需提供事件维护记录单，每次重大故障解决后的 24 小时内，或者按招标方要求时间提交重大故障报告。

2）中标方需为招标方建立维护服务档案。通过相关文档的完善，提升运维工作的效率，完善网络拓扑图、维护记录等信息，便于查询和管理。

5、应急保障

1）7×24 小时应急响应服务。接到招标人应急响应需求后，在 4 小时内到达现场，迅速解决问题。

2）严格按照相关流程进行应急故障处理各项工作，在过程完成前有专人在现场进行保障，对相关操作需要进行审核，应急故障处理的过程必须满足相应的流程和制度。

3）在网络设备、主机、操作系统等出现网络服务异常时，配合招标方进行相关网络排查工作，以便迅速分析网络或系统异常原因，在最短时间内恢复正常。

（三）内网邮件系统运维具体要求

1、以下故障须提供现场支持服务，并提交故障分析报告及解决方案。

1）系统宕机：邮件系统不能正常工作，包括

系统中止(不能保存进行中的工作)；

系统功能性故障导致数据丢失或系统不可用；

系统功能性故障致使系统失效；

系统故障致使关键任务应用程序重新启动/运行；

发现安全性易遭到破坏的脆弱点。

2）系统损坏：系统不能完好地运行，但仍可运行，包括

功能受到损坏或破坏，对应用程序产生重大影响；

应用程序频繁发生故障，但并未导致数据丢失；

管理系统发生了严重的故障；

系统性能严重降低。

2、提供支持服务范围：在技术支持与服务期内，中标方保证对系统应用数据进行维护。

3、中标方支持服务的内容：

1）应用软件使用的技术咨询及培训

针对在应用系统软件使用过程中出现的有关使用方面的疑问进行解答、培训、咨询。每年应至少提供一次针对招标方运维的技术培训，培训应使招标方的工程师能够熟练操作应用软件。

2）应用软件重新安装、调试

针对在系统宕机、系统损坏后所需要的应用系统软件的重新安装、调试。

3）每季度对内网邮件系统进行巡检。

4）中标方负责免费对邮件系统进行升级服务，升级服务包括小版本的升级。应保证在各功能模块有最新版本时主动针对用户方提供个性化的升级服务，升级的过程中应始终保证系统的平稳运行。系统升级前须提供新版本的介绍，风险分析报告，详细的升级计划和回退方案。升级结束后提供测试报告，并为用户提供培训。

4、服务文档要求

1）有完善的项目档案管理机制，能够建立完整的项目运维相关的知识库体系，各类工作记录单样例齐全，需向甲方提交季报、年度报告等文档大纲清晰，内容完整。

2）季度巡检报告，巡检报告中至少应包含根据巡检结果做出的针对招标方系统的合理化建议和提高系统安全稳定性的建议。

3）发生故障提供现场服务后，提交故障分析报告及解决方案。

（四）网络安全服务具体要求

中心外网网站部署于云端，为增强外网网站的安全防护能力，需提供云安全服务。

1、Web 应用防火墙：对网站的业务流量进行恶意特征识别及防护，避免网站服务器被恶意入侵，保障业务的核心数据安全。

2、云安全中心：实时识别、分析、预警安全威胁，防勒索、防病毒、防篡改、合规检查等安全服务。

3、漏洞扫描和安全加固服务

在服务期内，为审协湖北中心提供每季度 1 次的漏洞扫描和安全加固服务。具体要求如下：

1）漏洞扫描内容:

使用扫描工具（公安部或网信办认可的扫描工具）进行系统漏洞扫描，对需要被检测的信息资产进行专业安全分析和评估，及时了解和掌握信息资产的脆弱性，并出具脆弱性评估报告，对扫描分析结果提供可落地的漏洞解决方案，包括但不仅限于漏洞详情，漏洞描述，修复建议等；对漏洞修复结果进行验证；对漏洞修复与处置情况进行追踪；配合整改至符合相应等级的安全要求。

范围:中心指定的信息系统资产。

频次:该项工作服务期内每季度开展 1 次。

成果:《信息系统漏洞扫描报告》

2）安全加固内容:

在漏洞扫描的基础上，结合日常安全监测分析结果、当前安全漏洞最新进展的分析，编制加固方案，对信息系统进行安全加固优化。按照已制定安全加固方案，采用补丁升级、关闭不必要端口和服务、优化访问能控制策略、增加安全机制等措施对被加固对象存在的安全缺陷和隐患漏洞进行弥补和修复。安全加固操作以不影响业务和维护运行需求为标准，通过解决存在的主要安全漏洞和强化系统本身的安全设置，保证系统更加稳定、安全、可靠的运行。

4、重要敏感时期值守

提供网络安全应急及重要时期值守服务，配合中心及中心指定运维单位在重大节日、会议等敏感时期提供信息化保障工作，完成中心交办任务。成立专门的服务小组，小组成员必须包含（但不限于）网络技术专业人员、信息安全专业人员等，该小组紧密配合中心要求工作。小组成员保证 7×24 小时手机待机状态，在突发安全事件时，立即与中心取得联系，启动中心应急响应机制。此期间人员随叫随到，提供针对性的方案，实时地进行阻断行为，恢复信息系统运营使用单位系统的机密性、完整性和可用性。

★在重要敏感时期内，根据中心有要求，免费指派至少 1 名专业安全运维人员，专门负责中心 7×24 小时的信息安全值守工作，以便快速对突发状况进行响应和处理。需提供服务承诺并加盖投标人公章。

（注：2023 年湖北中心重要敏感时期 7×24 小时的信息安全值守一共有 49

人天，投标方应充分了解其工作内涵，须免费提供值守服务）

四、其他要求

（一）服务团队要求

运维团队要求：针对本项目设立专门的运维团队，人数不少于 7 人，包括运维服务项目经理、运维服务团队。应保证服务团队稳定性，服务团队人员变动须书面申请，招标人同意后方可变更，接替人员的资质、能力不低于原技术人员。

1、运维服务项目经理要求：投标人须指定专职项目经理，负责本项目的所有运维管理工作，负责协调相关专业资源为中心提供优质服务。项目经理应具备丰富的服务项目管理、IT 服务管理经验，以及风险控制、应急处理方面相关能力。提供其相关资格证书。

2、运维服务团队要求：投标人需要提供针对此项目至少 7 人（含运维服务项目经理）且工作经验 3 年以上的运维服务团队的名单，团队成员中除具备专业认证证书的服务人员外，还应含有具备安全运维、风险控制、应急处理方面相关能力的人员。

★3、驻场人员要求：除上述的运维团队要求外，投标人需要针对此项目安排提供至少 2 名 5×8 小时工程师驻场在审协湖北中心机房进行技术支持服务。要求服从招标人管理，遵守招标人工作时间要求，具备相应运维服务技能，提供其相关资格证书。需提供服务承诺函并加盖投标人公章。

（二）合同签订与支付

1、因本项目分三项服务内容，且各项服务期起始与终止日均不相同，因此本项目为合并招标一次招三年，根据服务内容分三项分别签订 3 份合同，三项服务期均为 3 年，合同一年一签。

2、一年一签的 3 份合同，在每个合同服务年度，采购人均根据进程分阶段向投标方支付款项：

A 首付款：双方签署合同后 10 个工作日内，采购人收到与付款金额一致的增值税专用发票向供应商支付合同款的 45%；

B 第二次付款：在服务工作开展一年服务的最后一个月，投标方提出年度

验收申请。经采购人验收合格双方签署验收报告后，采购人收到与付款金额一致的增值税专用发票 10 个工作日内，甲方向供应商支付合同款的 55%。

3、合同价已包含供应商履行本合同全部义务所应获得的价格，包括但不限于：开发费用、服务费用、通信费用、数据加工费用，供应商不得以任何理由要求增加费用，双方书面同意的除外。

4、在采购人付款前，供应商应向甲方提交当期双方签字且验收合格的验收文档并开具正规增值税专用发票（注：首付款不需要验收文档）。供应商出示的发票应包含采购人应向供应商支付的当期款项所有金额，并应包含足够详细的内容，使采购人能够确定金额的准确性。采购人根据供应商提供的合格发票及服务验收文档支付相应款项，如供应商提交的发票或服务验收文档不合格，甲方可延迟付款。

（三）考核与年验收

1、供应商于每个月末、季度末起 5 个工作日内向甲方提供月度、季度报告，其中至少包括以下内容：

故障情况和维护记录；

运行情况月度报表及总结、季度服务情况小结；

后续维护建议。

2、一年服务期结束前最后一个月，供应商向采购人提出验收申请并提交验收文档。验收文档应包括年度维护服务总结报告及乙方签字盖章的验收报告。

3、如验收未通过，采购人有权暂不签署验收文档及支付剩余服务费用，供应商应在 5 个工作日内按照验收意见进行弥补、改进或完善，待甲方重新组织验收并且验收合格后，采购人再向供应商支付剩余服务费用。如果投标方在规定的验收日后的一个月内，经改进仍达不到验收标准的，采购人有权终止合同并拒绝支付服务费用。

4、如供应商在上述规定的合同期满后的一个月内仍未向采购人提出验收请求并提交验收文档，采购人有权终止合同并拒绝支付剩余费用。

（四）违约责任

1、供应商未能按照招标文件、投标文件的约定提供技术支持与服务，采购人有权将此记为技术支持和服务中断，对于技术支持和服务中断，每中断一

次，扣除中标总价款的1%作为违约金。经采购人通知之日起五日内仍未按采购人要求补正的，每逾期超过一日应向采购人支付中标总价款的5‰作为违约金。

2、当违约金发生并达到合同总金额的10%后，采购人有权解除本合同，并有权要求供应商退回已支付的金额，及赔偿采购人因此遭受的全部经济损失。

3、若因违约，采购人终止全部或者部分合同的，采购人有权按照其认为适当的条件和方法向任何第三方购买与供应商未提交的可交付物类似的产品或服务，供应商应承担采购人为此所支付的额外费用。就合同中未终止部分，供应商应继续执行。因合同终止而造成的损失由供应商承担全部责任。