2026年度武汉市政府网站集约化平台基础资源安全运维及监测服务采购需求

一、采购背景

武汉市政府网站集约化平台（以下简称“平台”）是全市政府网站的数字基座，承载着统筹整合全市政府网站数据资源、聚合应用服务供给的核心使命。该平台有效实现政务信息高效传递、赋能共享，为打造智慧化、开放型、服务型政府筑牢关键支撑。为保障平台在2026年度始终保持稳定、高效、安全的运行状态，进一步提升政务服务质量与效能，同时满足安全合规性要求，现计划采购平台基础资源及安全运维相关服务。

二、服务期限

自合同签订之日起，交付的全部资源及服务达到采购方要求后，至项目服务期满（365个日历天）。

三、采购内容

序号	名称	数量	单位
1	平台基础资源服务	1	套
2	平台安全服务	1	套
3	平台技术运维服务	1	套
4	配套支撑服务	1	套

四、采购要求

本项目在承接2025年度运维服务的基础上，将保障平台持续稳定运行的基础资源及安全运维服务列为核心内容。各参与投标的供应商需编制详实的投标方案，同时郑重承诺所提方案真实、合规、有效，能够全面契合采购方的各项需求，从而保障平台运维服务新旧交替阶段平稳、安全过渡。

（一）平台基础资源服务

1.云主机技术要求

（1）支持整机备份与快照备份双重服务模式，备份数据可灵活恢复至原服务器或新部署的服务器。

（2）创建环节支持配置多个网卡，并可分别为其分配不同的IP地址。

（3）提供虚拟主机动态升级、快照备份、异常告警、日志管理等功能，支持按需自定义CPU、内存、网络、磁盘等各项属性来创建虚拟主机。

（4）支持计算能力的水平弹性伸缩。

2.云存储技术服务要求

（1）云硬盘具备共享功能，提供SATA、SAS、SSD三种类型可选，其最大IOPS数值不低于33000；单台云主机可加挂载16块云硬盘。

（2）海量数据存储系统支持访问控制功能，可针对用户及用户组配置对应的权限策略；同时支持块、文件、对象多协议存储服务；该存储服务的设计可用性不低于99.95%，数据设计持久性不低于99.9999999%。

3.云机房服务要求

（1）投标人须具备自有产权的云机房，且机房需达到国标A级机房标准，并需提供相应的机房权属证明文件。

（2）可提供项目所在地的其他IDC机房供采购方选择，且该类机房支持现场考察；同时需具备位于国内不同地点的容灾机房能力，以满足应急故障场景下的容灾需求。

（3）若候选机房为自有产权，需提供权属证明；若为租用机房，则需提供租赁相关材料，或承诺在中标后按照合同要求完成机房租赁事宜。

（二）平台安全服务要求

需严格遵循《中华人民共和国网络安全法》《中华人民共和国密码法》《关键信息基础设施安全保护条例》《信息安全等级保护管理办法》等相关法律法规要求，符合等级保护2.0三级“一个中心、三重防护”的标准规范，提供兼具合规性、全面性、自主性与可控性的安全运营管理服务。

1.合规安全服务

服务范围涵盖但不限于防火墙服务、主机安全防护服务、入侵防御服务、数据库安全审计与防护服务、运维审计服务、应用安全防护服务、应用安全基础服务、应用系统威胁捕获服务、综合安全监控分析服务、网页防篡改服务、互联网安全服务、日志审计服务、IPv4/IPv6支持服务、网站证书服务、应急保障服务等。同时需严格遵照相关管理要求，提供安全评估、重要时期安全保障、应急响应处置等多元化配套服务。

2.应用密码保护

需严格遵循国家标准GB/T39786-2021《信息安全技术信息系统密码应用基本要求》的第三级要求，从真实性、机密性、完整性、不可否认性四个维度，对平台物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个层面实施加密保护，并建立对应的管理制度。提供加解密服务、国密IPsec/SSLVPN服务、数据完整性保护服务、数据加密传输服务、智能密码钥匙服务、国密域名证书服务等全链条密码支撑服务，全面夯实平台安全运行的密码基石。

（三）平台技术运维服务要求

严格遵循国家、湖北省及武汉市关于政府网站及平台建设发展的相关政策文件要求，保障平台安全稳定运行，持续完善平台功能、优化服务质量，为全市各区、各部门的政府网站提供坚实可靠的支撑。服务范围涵盖但不限于网站集约化平台、统一信息资源库、数据集约与对接服务、与省级集约化平台的对接联动等技术运维服务，具体包含功能巡检、配置调整、故障排查、升级优化、应急响应等全流程保障工作。同时，根据政务公开规范要求，提供以“wuhan.gov.cn”为后缀的独立专属政务邮箱服务，保障服务高效、稳定、安全可靠，全面满足政务沟通及信息传递工作需求。

（四）配套支撑服务要求

对全市范围内正常运行的政府网站开展全面监测与抽查工作，采取7×24小时系统自动监测与定期人工核查相结合的方式，及时发现各类突出问题并督促完成整改，确保所

有网站整体达标。

1.监测服务

监测范围涵盖网站可用性、文本表述重大错误、无效链接、暗链与伪链，以及涉密涉敏信息等内容，并据此出具月度监测报告。

2.抽查服务

为进一步推进全市政府网站和政务新媒体健康有序发展，依据国家制定《政府网站与政务新媒体检查指标》，提供监测及多渠道预警机制等配套服务，并出具季度抽查报告。

五、其他要求

（一）服务方式

中标供应商须提供7×24小时远程协助、上门服务、电话咨询、电子邮件等多渠道技术支持服务，确保响应及时、处置高效。

（二）人员要求

投标人拟投入运维服务的人员数量不少于10人，团队成员均须具备相应技术资质，其中至少1人持有有效期内的PMP或同等效力资质证书，至少1人持有有效期内的CISP（注册信息安全人员）资质证书；同时须指定1名人员驻场开展相关运维工作。

（三）验收要求

严格按照政府采购相关法律法规及《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》（财库〔20

16〕205号）要求验收。

1.资源交付阶段

中标供应商在合同签订后14日历天内交付全部满足采购需求的资源，方可启动运维服务期计算。

2.项目终验阶段

服务期满前，中标供应商应向监理服务商提交终验申请，采购方依据合同约定及验收相关程序组织竣工验收。供应商须将服务期内形成的平台运维文档、云资源管理资料、安全运行维护资料等汇编成册移交，资料不齐全的，不予通过验收。

（四）技术服务要求

运维期间，供应商须提供现场及远程技术维护方案，负责云资源与链路功能优化完善、应急响应处置及产品迭代升级；系统出现故障或存在瑕疵缺陷时，须在10分钟内响应，2小时内完成故障排除，故障处置完毕后3个工作日内提交《故障处理报告》。

（五）保密要求

中标供应商须严格遵守采购方各项管理规定，并签订保密协议；严禁擅自复制、传播、引用业务数据、工作要求等相关信息，非开发工作需要不得查询前述信息，未经采购方授权不得向任何第三方演示系统相关内容，采购方保留追究其相关法律责任的权利。

（六）培训要求

为集约化平台管理员及全市各政府网站相关管理人员

提供专项技术培训，投标人在投标阶段须同步提交相关的培训方案。

（七）报价要求

报价应涵盖人工费、通讯费、交通费、培训费、检测认证费等项目实施所需全部费用。凡出现漏报、少报情形，均由供应商自行承担相关责任与损失，采购方不另行予以补偿。报价总额不得超过315万元，超预算报价视为无效报价。具体费用明细，待合同签订环节另行协商约定。

附件 1：基础资源服务

云主机					
序号	**服务项目**	**服务说明**	**计费单位**	**数量**	**备注**
1	云主机	vCPU≧8核、内存≧16GB	台/年	24	免费操作系统
2	云主机	vCPU≧16核、内存≧16GB	台/年	36	
3	云主机	vCPU≧16核、内存≧32GB	台/年	12	
4	云主机	vCPU≧32核、内存≧64GB	台/年	6	
合计				78	
云存储					
序号	**服务项目**	**服务说明**	**计费单位**	**数量**	**备注**
1	云硬盘	高速云硬盘	1TB/年	90	
2	云备份	本地备份存储	1TB/年	10	
其它服务					
序号	**服务项目**	**服务说明**	**计费单位**	**数量**	**备注**
1	短信服务	短信服务套餐（50万条/年）	套/年	1	
（注：供应商所投入基础资源不得低于以上内容，并提供相关证明材料。）					

附件2：云安全服务清单

序号	服务项目	服务说明
1	防火墙服务	包括但不限于提供防火墙吞吐量≥10Gbps，最大并发连接数≥1000万，每秒新建连接数≥16万，包含100个SSLVPN授权服务。具备容器化服务能力，对NAT地址池中的地址进行有效性探测服务，在出现地址池地址不可用的时候自动排除，保障互联网业务安全稳定运行。支持动态负载均衡技术采用自适应创新链路选择控制算法，可实时主动探测链路的连通状况、延迟情况及抖动，形成智能闭环，以便根据当前时刻的链路状况作出最优选路。支持嵌套式流控功能服务能力，具备至少两个维度的流量控制。上述功能需提供相关功能截图或证明文件复印件，并加盖原厂公章。
2	主机安全防护服务	包括但不限于提供专业主机安全防护服务，针对服务器物理机、虚拟机和容器环境提供一站式安全防护能力，支持自动获取主机信息，主机信息包

		括硬件类型，操作系统版本，系统内核版本，CPU数量，内存，主机IP等。提供微隔离功能服务，支持主机与主机之间的网络访问，外部地址与主机之间访问，部署微隔离策略，持续评估基础设施安全，实时检测安全威胁，主动实施行为管控，具备精准发现并处置恶意文件能力，上述功能需提供相关功能截图或证明文件复印件，并加盖原厂公章。
3	入侵防御服务	包括但不限于提供专业入侵检测系统，支持多重威胁检测和防御能力，支持对僵尸网络攻击、DDoS攻击、已知协议漏洞利用、Web攻击、垃圾邮件、钓鱼、木马病毒和恶意软件等一系列网络入侵威胁进行检测及防御。上述功能需提供相关功能截图或证明文件复印件，并加盖原厂公章。
4	数据库安全审计和防护服务	包括但不限于提供采用精准协议解析、海量日志存储和检索等技术，通过对访问数据库的行为、内容等进行采集、存储、分析，实现完全独立于数据库的审计功能服务，一套系统内即可同时支持包括数据库审计、数据库防火墙、数据脱敏、风险扫描、状态监控、运维审计等功能。上述功能需提供相关功能截图或证明文件复印件，并加盖原厂公章。
5	运维审计服务	包括但不限于提供运维管理和运维安全融合服务，通过身份认证、权限控制、账户管理、操作审计等多种手段，完成对资产的统一认证、统一授权、统一审计，全方位提升运维风险控制能力。满足任意浏览器播放审计日志视频回放、监控、切断；所有审计日志以会话为单位，支持完整回放；正在连接中的会话支持实时监控与阻断。同时加载水印在播放页面。上述功能需提供相关功能截图或证明文件复印件，并加盖原厂公章。
6	应用安全防护服务	包括但不限于提供web应用安全防护，采用深层代理、应用漏洞扫描、日志聚合、智能自学习等多项技术，从TCPO武汉市政府网站集约化平台ion获取源IP地址（TOA）、支持移动运维与“一键应急断网功能服务”、用户会话跟踪功能的服务；支持攻击检测双引擎，即语义解析引擎+规则防护引擎，语义解析引擎通过词法分析、语法分析及语义分析对报文进行检测。上述功能需提供相关功能截图或证明文件复印件，并加盖原厂公章。
7	应用安全基础服务	包括但不限于提供全方位的系统扫描检查和安全评估，协助管理者高效、准确的对内部系统进行实时自检，以针对性提升网络的整体安全性。本次服务所用工具，支持与态势感知服务工具联动，进行全网脆弱性分析。上述功能需提供相关功能截图或证明文件复印件，并加盖原厂公章。
8	应用系统威胁捕获服务	包括但不限于提供模拟不同类型的服务，并在设置一些常规漏洞，诱骗攻击者利用漏洞对其实施攻击，触发攻击告警，继而进行攻击溯源并做及时处置，有效防止攻击者在内网中横向扩散。上述功能均需提供相关功能截图或证明文件复印件，并加盖原厂公章。
9	综合安全监控分析服务	包括但不限于聚合从威胁探针、防火墙、应用安全防护、应用安全基础等服务的流量和日志数据，实现全网流量安全分析。自动识别流量中常见的应用协议，并按照应用维度进行流量统计与分析。支持的应用协议包含不限于RDP、SSH、HTTP、SNMP、FTP-DATA、微信文件传输、UDP下载及视频等至少5000种以上的应用协议；支持按照IP地址、通讯协议、端口等自定义应用识别规则。提供自动化编排响应剧本服务，实现全网联防联动，实时检测出问题并下发处置动作到联动设备（防火墙、WAF等），作出及时响应，并形成相应的安全任务，通过邮件、短信等方式推送给对应的管理员。提供以图形等展示每个终端在不同时期的流量数据情况的服务能力，包括但不限于，目的IP、目的端口、服务、基线学习状态。提供重保工作

		台：包括实时告警、溯源模式、一键阻断、重保报告、重保配置助手功能模块；提供挖矿专项服务：主要包括挖矿阶段分布、挖矿币种分布、挖矿资产、受害资产列表及详情，支持筛选、导出、批量标记、加白及处置等操作。防勒索专项：勒索阶段分布、勒索事件分布、受勒索资产、受害资产列表及详情，支持筛选、导出、批量标记、加白及处置等操作；弱密码专项：主要弱密码事件、弱密码目的IP、弱密码清单列表及详情，支持筛选、导出等操作。提供基线学习结果作为流量异常检测依据，如出现异常流量，会进行异常流量告警，并提供安全事件自定义处置，实现事件规则匹配、因果关系关联、可视化、大模型解读等服务。上述功能均需提供相关功能截图或证明文件复印件，并加盖原厂公章。
10	网页防篡改服务	包括但不限于提供基于内核驱动级文件保护技术，支持各类网页格式，包含各类动态页面脚本；支持大规模连续篡改攻击防护；支持断线状态下阻止篡改；完全杜绝被篡改内容被外界浏览；支持单独文件、文件夹及多级文件夹目录内容篡改保护保护站点内容安全，防止黑客非法篡改网页，保护公众形象。系统通过服务器文件访问底层驱动技术，对保护的对象(静态网页、动态执行脚本、文件夹)实时监测其属性。上述功能均需提供相关功能截图或证明文件复印件，并加盖原厂公章。
11	互联网安全服务	包括但不限于提供互联网线路的互联网安全配套服务。服务内容为对客户的网站域名提供防篡改服务，对互联网流量提供抗D攻击保护和流量清洗服务。实时流量监控和全面风险评估，当流量出现异常或者超过预先设置的阈值时可启动防护清洗，并与攻击结束后及时提供攻击报告。上述功能均需提供相关功能截图或证明文件复印件，并加盖原厂公章。
12	日志审计服务	包括但不限于提供日志审计服务，实现网络日志的集中采集、分析挖掘、合规审计、实时监控及安全告警、报表生成等，可关联策略产生审计事件、如时间、IP地址、方式等，对于相符合的结果，系统将在关联事件中呈现，并为用户提供自定义日志查询功能服务。上述功能均需提供相关功能截图或证明文件复印件，并加盖原厂公章。
13	IPv4/IPv6支持服务	包括但不限于采用IPv6反向代理功能，进行IPv4到IPv6的转换，实现使用IPv6的公网资源访问集约化系统的内部站点。支持用户通过IPv4/IPv6双协议访问并获取服务，同时进行安全性加固。上述功能均需提供相关功能截图或证明文件复印件，并加盖原厂公章。
14	应急保障服务	包括但不限于在特殊时期、重要活动、重大节假日，提供合规专业安全工具或人员对平台系统、应有软件、数据库和中间件、等相关体系进行全面与深度安全检测，并对发现的问题及时修复加固。且具有应急响应处置、安全事件溯源的服务能力，并派遣专业安全事件应急服务人员协助分析或上门处置等相关服务。每年至少组织1次安全演练，并提供演练报告。
15	加解密服务	包括但不限于提供基于SM2算法的数字签名和认证服务，可用于证书生成和验证、身份认证等。提供国家标准的SM1算法和SM4算法，用于数据的加解密；提供符合《GM/T0018-2012密码设备应用接口规范》的SDK编程接口服务，为业务应用提供对称加解密、非对称加解密、数据签名、数据签名验证等密码服务，同时提供密钥管理、密钥配发、密码模块集群管理等管理服务。上述功能均需提供相关功能截图及商用密码认证证书，并加盖原厂公章。
16	国密IPsec	包括但不限于提供VPN服务，密码算法至少支持支持SM1、SM2、SM3、SM4

	/SSLVPN服务	密码算法；至少支持ECC(SM2)-SM4-SM3、ECC(SM2)-SM1-SM3算法套件；支持SM2+SM1+SM3+ESP、SM2+SM4+SM3+ESP隧道模式。支持NAT穿越和双向NAT穿越。提供支持静态路由、动态路由。支持基于源/目的地址、端口、协议及接口的策略路由。上述功能均需提供相关功能截图及商用密码认证证书，并加盖原厂公章。
17	数据完整性保护服务	包括但不限于提供支持动态文件的数据完整性保护服务，即添加定义保护对象的时候可以指定被保护的数据文件对象是动态的文件；提供国产数据库达梦、人大金仓等服务，添加结构化数据库的数据保护对象的时候支持国产达梦、人大金仓等数据库。 提供支持HMAC-SM3和SM2算法的选择服务，定义完整性保护对象的时候可以指定使用HMAC-SM3或者SM2算法。上述功能均需提供相关功能截图及商用密码认证证书，并加盖原厂公章。
18	数据加密传输服务	包括但不限于提供数据加密传输服务，支持国密ECC-SM4-GCM-SM3算法套件，通过页面用户可以指定支持的HTTPS代理转发的SSL密码套件包含ECC-SM4-GCM-SM3； 提供自适应匹配服务，根据客户端浏览器匹配不同算法套件，某个HTTPS代理转发管理中可以同时指定RSA和国密SM2证书，使用国密浏览器访问该代理转发抓包截取国密TLCP的协议协商过程，使用非国密浏览器访问该代理转发抓包截取TLS1.2/1.3协议协商过程。上述功能均需提供相关功能截图及商用密码认证证书，并加盖原厂公章。
19	智能密码钥匙服务	包括但不限于提供智能密码钥匙服务支持SM1、SM2、SM3、SM4国密算法，支持集成第三方CA机构签发的国密数字证书服务，具备适配国产化操作系统、国产化处理器。上述功能均需提供商用密码认证证书。
20	国密域名证书服务	包括但不限于提供国密域名证书服务支持国密SM2算法，服务上是采用自主可控密码技术保护数据机密性、完整性，实现HTTPS网站加密传输，防止数据在传输过程中被窃取或篡改，确保通信主体身份真实性、完整性。
21	国密浏览器服务	包括但不限于提供国密浏览器服务支持国密算法，包括:SM2/SM3/SM4;具备适配国产化操作系统、国产化处理器。 上述功能均需提供商用密码认证证书。

附件3：平台技术运维服务

序号	服务名称	服务内容	备注
技术支持			
1	平台功能技术支持	提供平台整体软件环境、资源部署的技术运维。包括但不限于站点管理、栏目管理、信息采编发布、模板管理、用户和组织管理、政府信息公开、互动信箱、在线调查、在线访谈、意见征集、智能搜索等模块的功能、配置调整，确保平台所有功能模块 7×24 正常运行。同时，根据采购用户要求对入驻平台的所有网站提供技术支持、问题咨询等各项技术服务。	
2	对平台进	检查服务器运行状况、存储空间状况、软件运行状况、硬件运行状况、备份系统状况等。并提出现有问题和解决方法，及时发现和排除潜在	

	行定期或不定期巡检	问题或故障隐患，保证系统的稳定运行。（基于应用软件的系统运行日志、服务器的运行监控软件、数据库日志等多种方式进行运行状况的检查）。	
3	平台升级	提供集约化平台各子系统的功能优化升级、安全补丁修复服务。	
4	网站性能优化	定期对全市政府网站 web 应用做优化服务，以提升网站的运行性能。	
5	系统故障维修	及时处置平台和各政府网站使用过程中的故障、系统安全、系统漏洞等；对第三方提出的安全报告及时调整处理，并对事件处理全流程进行跟踪监督，确保相关问题得到及时的响应与处理。接到报障通知后，须在 10 分钟内通过电话等方式响应回复，并在 2 小时内解决故障，故障排除后 3 个工作日内提交《故障处理报告》。	
6	应急保障	提供重保或节假日期间 7×24 小时值班备勤服务，包括但不限于现场、远程等支持方式，并按照采购方要求提供技术人员现场驻场值守驻场和其他保障等服务。	
7	搜索服务优化	在原运行平台的基础上，持续优化相应的功能，提供智能语义搜索引擎服务，支持结构化文本的多条件搜索能力，提供可视化配置后台，轻松实现搜索系统的搭建与运营，提供智能提示、智能纠错、拼音搜索、敏感词屏蔽、百姓体搜索、全文检索、智能高亮、智能排序、热词推荐和相关推荐等服务能力，以及关键词聚合应用、框计算应用、地图服务应用和主题场景应用等场景应用，实现“搜索即服务”，提高平台工作效率。	
8	网站“一号登录”优化	在原运行平台的基础上，根据反馈，结合用户新需求，对网站“一号登录”进行功能和性能优化。	
9	全文检索模块优化	在原运行平台的基础上，根据反馈，结合用户新需求，对全文检索模块进行功能和性能优化。	
10	互动模块优化	在原运行平台的基础上，根据反馈，结合用户新需求，对网民互动模块进行功能和性能优化。	
11	其它类服务	根据采购方需求，及时完成平台相关接口对接（含开发）、应用调整、突发性及其它技术支持等服务。	
应用邮箱			
12	数量与存储空	包括但不低于提供 100 个“wuhan.gov.cn”邮箱用户，每用户邮箱存储空间不少于 10G。上述功能均需提供相关功能截图或证明文件复印件，并加盖原厂公章。	

	间需求		
13	功能需求	包括但不限于支持邮件待办、邮箱代收代发、附件预览、自动回复、快速查找、日程管理、企业与个人网盘、超大文件上传与存储及移动端等。上述功能均需提供相关功能截图或证明文件复印件，并加盖原厂公章。	
14	管理需求	包括但不限于支持群发权限管控、定期自检、设置部门群发、邮箱功能权限自定义、网盘操作日志及密码策略设置等。上述功能均需提供相关功能截图或证明文件复印件，并加盖原厂公章。	
15	安全需求	包括但不限于支持邮件加密、防暴力破解、HTTPS 协议访问、登录限制策略、可疑邮件隔离、收发双向过滤检测、SPF 域名校验、钓鱼邮件识别过滤及垃圾邮件管控等保障能力，上述功能均需提供相关功能截图或证明文件复印件，并加盖原厂公章。	

附件4：配套支撑服务要求

序号	服务项目	服务说明
监测服务		
1	可用性监测服务	包括但不限于每月监测网站首页可用性并统计各网站首页可用性百分比进行年度排名统计。
2	网站严重表述错误检测服务	包括但不限于每月利用软件检测武汉市政府网站群历史信息中的严重表述性错误，并要求人工核实问题属实后汇总成相关检测报告。
3	网站无效链接检测服务	包括但不限于每月对武汉市政府网站群的无效外站链接、网站无效图片、无效的文字链接、无效的附件文件等问题进行检测，形成网站无效链接检测报告。
4	网站暗链、伪链检测服务	包括但不限于每月通过软件检测出网站的全部站外链接，并经过人工核实各链接的合法性，判断外链链接是否存在黄、赌、毒或者其他商业链接等情况，定期为各网站形成独立外链检测报告。
5	网站涉密、涉敏信息监测服务	包括但不限于每月通过相关软件检测手段检测网站中隐藏的部队番号、涉密文件及维稳等信息，并经过人工核实后形成相关检测报告。
抽查服务		
1	单项否决检查服务	包括但不限于每季度完成对全市政府网站的安全、泄密事故等严重问题、站点长期无法访问、首页不更新、互动回应差、服务不实用等内容开展检查，出具整改意见。
2	发布解读检查服务	包括但不限于每季度每季度完成对全市政府网站概况、职能、领导信息、政策文件、解读比例等全栏目覆盖检查，查摆问题并出具整改咨询及优化建议。
3	办事服务检查	包括但不限于每季度完成全市政府网站事项公开、在线申请、办事指南等全要素核查，查摆内容精准性、表格规范性等问题，提供针对性整改咨询

		与实操性优化方案。
4	互动交流检查服务	包括但不限于每季度对全市政府网站信息提交、统一登录、留言公开、办理答复等核心互动功能开展全覆盖、标准化核查，精准排查流程堵点与服务短板，靶向出具整改优化方案，推动线上互动渠道规范高效运行。
5	功能设计检查服务	包括但不限于每季度对全市政府网站域名名称、网站标识、我为政府网站找错、站内搜索、一号登录、页面标签、兼容性、IPv6改造等功能全维度排查，出具优化整改建议。
6	重保专项检查服务	包括但不限于结合全年政府网站重大活动保障任务及上级专项检查部署要求，提供全领域、全覆盖检测服务；并按需开展政务新媒体检查，形成并提交包含整改建议的专项检查报告等。