

内蒙古自治区人大常委会机关信息系统网络及数据安全防护服务项目采购需求

一、项目名称：内蒙古自治区人大常委会机关信息系统网络及数据安全防护服务项目。

二、服务范围：包括不限于内蒙古人大门户网站、内蒙古人大 APP、信访小程序、综合应用平台、无纸化会议系统、自治区人大代表履职平台、干部考核系统、规范性文件备案审查系统、法规规章规范性文件数据库等业务系统的等保测评、密码测评和信息网络安全防护、检测、预警和安全行为管理等。

三、服务地点：根据招标方要求。

四、服务期：1 年

五、付款方式：

1 期：支付合同金额的 40%，于合同签订后收到发票之日起 15 个工作日内支付；

2 期：支付合同剩余款项，待投标方完成全部服务并通过验收后，依据合同履行情况验收成果，于收到发票之日起 30 个工作日内支付。

六、服务配套要求：由投标方提供本项目所需技术人员及相关服务设备。

七、商务条款：

1. 资质要求：等级保护测评机构为持有公安部认证的《网络安全等级测评与检测评估机构服务认证证书》，且已列入中国网络安全等级保护网发布的《全国网络安全等级测评与检测评估机构目录》。商用密码测评的机构为持有由国家密码管理局颁发的在有效期内的《商用密码检测机构资质证书》，且已列入国家密码管理局公布取得资质证书的商用密码检测机构名录。

2. 人员要求：

- (1) 项目经理具备信息安全工程师或同等经验；
- (2) 项目驻场人员不少于 1 人；安全服务人员不少于 3 人，且具备从事相关工作的资质；
- (3) 驻场人员需通过投标方组织的背景审查，无网络安全违法犯罪记录、失信记录，承诺所提供的资质、履历信息真实有效，若存在造假，招标方有权要求投标方立即更换人员或解除合同。

3. 费用调整：合同签订后，若因业务调整导致服务涉及的应用系统数量减少（或增加），服务费用均确定于中标金额。

八、服务评价：服务期内，将依据本项目服务内容及要求，从方案报告质量、项目人员服务能力、保密工作质效、应急管理响应、培训开展效果等维度进行综合评价，评价结果作为项目验收、费用支付的重要参考依据。

九、其他要求

1. 投标方需确保驻场人员的数量、专业能力满足项目工作需求。驻场服务期间，若投标方需更换驻场人员，需提前 15 个工作日向招标方提交书面申请，说明更换原因及新人员的资质材料，新人员需满足招标中对驻场人员的所有要求，更换过程中不得影响招标方安全防护工作的连续性。

2. 若驻场人员存在以下情形，招标方有权要求投标方 24 小时内更换人员：①违反招标方行为规范，造成招标方信息泄露或网络安全隐患；②资质造假或能力不足，无法完成约定的安全防护工作；③存在违规操作、消极怠工等影响服务质量的行为。

3. 投标方需对驻场人员进行持续管理，配合招标方开展人员绩效评价；若因驻场人员过错导致招标方遭受损失（如数据泄露、系统故障），投标方需承担全部赔偿责任。

十、违约责任

1. 任何一方无约定理由单方解除本合同的，需向对方支付合同金额 20% 的违约金；若违约金不足以弥补对方实际损失的，违约方还应就差额部分承担赔偿责任。

2. 投标方未按合同约定时间（如漏洞扫描周期、应急响应时限）提供服务，每逾期

1 日，需向招标方支付合同总金额 0.5% 的违约金；逾期超 15 日，招标方有权单方解除合同，并要求投标方退还已支付但未实际履约部分的服务费用。

3. 投标方提供的防护服务未达到合同约定标准（如防护系统频繁失效、未拦截已知风险攻击），招标方有权要求投标方在 3 个工作日内整改；整改后仍不达标，招标方可扣减对应比例服务费（最高扣减合同总金额的 30%），或解除合同并索赔损失；若因投标方原因导致招标方发生网络安全事件、数据安全事件或攻防演练失守等情形，由此造成招标方损失的，投标方应根据实际损失情况承担赔偿责任。

十一、服务要求详情：

服务要求一览表

序号	服务项	服务内容要求
1	主机防护服务	<p>主机安全防护服务主要是通过人工和主机安全软件相结合，对主机安全脆弱性进行加固整改，对恶意病毒程序进行查杀、检测，并对主机安全风险进行预警，隔离风险程序，保障主机系统的安全，为业务平稳运行提供计算环境安全，防止因主机安全风险造成的业务中断，阻止和降低安全威胁对业务工作带来的影响。</p> <p>主机防护服务主要包括：</p> <p>1) 主机基线加固服务；</p> <p>2) 主机漏洞加固服务；</p> <p>3) 主机病毒防护服务；</p> <p>4) 资产盘点与风险可视服务。</p> <p>服务频率：1 次/月</p> <p>交付成果：《资产清单》《基线加固报告》《漏洞加固报告》《主机防护服务报告》</p>
2	云防护服务	<p>对内蒙古人大门户网站、内蒙古人大 APP、综合应用平台、信访小程序、无纸化会议系统、自治区人大代表履职平台、干部考核系统、规范性文件备案审查系统、法规规章规范性文件数据库等系统进</p>

		<p>行安全 7×24 小时防护，需使用符合国家相关标准的云安全产品。</p> <p>通过 DNS 域名解释引流至云端网站安全防护系统，对网站的恶意扫描、篡改、挂马、黑客攻击等所有的访问流量进行 L2-L7 层的清洗，将恶意攻击、异常访问全部阻断，放通正常访问流量，实现统一防护。</p> <p>服务频率：1 次/月</p> <p>交付成果：《云防护服务报告》</p>
3	日常漏洞扫描服务	<p>定期对服务包含的 9 套系统的服务器、PC 终端、网络设备、安全设备、门户网站及各类应用系统、平台等开展安全扫描，编制详细处置意见；协助完成服务器及安全设备的操作系统的漏洞修复与测试。通过漏洞扫描工具，对各个系统的 WEB 页面、应用程序、中间件、数据库和服务端操作系统，开展网络层、系统层、数据库、应用层的全面系统探测，收集被测系统基本信息，发现活动目标主机、端口、系统指纹，对被测系统进行脆弱性扫描，扫描后人工验证操作系统漏洞、数据库漏洞、弱口令、信息泄露及配置不当等脆弱性问题，出具精准有效的扫描报告；针对漏洞扫描中发现的问题提供解决方案，协助招标方完成整改。</p> <p>漏洞扫描前，由招标方明确测试目标及测试范围；安全服务工程师使用国内主流厂商自主研发的专用漏扫设备现场进行漏洞扫描，发现高级别安全漏洞时，即时告知招标方安全负责人。</p> <p>服务频率：1 次/月</p> <p>交付成果：《漏洞扫描报告》</p>
4	网站安全及渗透测试服务	<p>提供渗透测试服务，主要针对网络层、系统层、应用层三个维度开展，基于待检测信息系统的安全弱点，模拟黑客入侵攻击方法，以人工渗透为主，漏洞扫描工具为辅，在可控、可调整范围内，尽可能获取目标信息系统的管理权限及敏感信息。</p> <p>根据渗透测试服务需求，对系统进行渗透测试，排查应用层业务流程和逻辑层面的安全漏洞和敏感信息泄露的风险，出具渗透测试报告。</p>

		<p>服务频率：2 次/年</p> <p>交付成果：《渗透测试报告》</p>
5	重要时期保障服务	<p>根据招标方要求，在“两会”等重大活动期间和春节、国庆等法定节假日以及国家、自治区、行业组织的重要保障时期（特别是网络安全攻防演练期间），按招标方工作时间提供现场驻场服务，保障系统稳定可靠运行。</p> <ol style="list-style-type: none"> 1. 保障前：协助用户进行系统安全检查、加固，并制定网络安全保障方案。 2. 保障期间：对系统可疑攻击行为进行实时监测、分析、处置，并形成报告及时上报；每日对安全事件和攻击行为进行溯源分析，会同招标方应急处突并出具相应报告。 3. 针对攻防演练：提供驻场网络安全防护服务，对标靶系统开展安全自查、加固、团队组建、防护措施部署、演习工具梳理、值守人员排班等工作；期间，对可疑攻击行为进行分析、处置并形成报告，及时上报至招标方及演习平台；根据实际需要动态调整防护策略，针对攻击方及趁机发起的恶意攻击进行应急处置；结束后，对演习过程进行复盘总结，为提升网络安全治理水平提供实践数据支撑。 <p>服务频率：至少 4 次/年（根据招标方要求开展）</p> <p>交付成果：《重要时期保障服务方案》《重要时期保障服务排班表》《网络安全自查方案》《攻击溯源报告》《网络安全加固报告》《重要时期保障总结报告》等</p>
6	新业务上线前安全检测服务	<p>依据 GB-T22239-2019《信息安全技术网络安全等级保护基本要求》8.1.9.7 测试验收条款开展业务上线安全评估，具体技术手段包括但不限于漏洞检测、基线配置检查、人工渗透测试、安全进程检测、资源配比检测等。</p> <p>服务频率：按需</p> <p>交付成果：《新业务上线前网络安全检测服务报告》</p>

7	应急演练	<p>按照招标方网络与信息安全事件应急预案以及相关法律法规要求，在服务期内组织开展至少 1 次符合《网络安全事件应急预案编制制度指南》规定的相关标准要求的网络安全事件应急演练；制定应急演练工作方案，明确演练方式、演练场景，选定应急演练脚本，搭建应急演练模拟环境等，且在演练结束后形成演练总结，及时会同招标方修订完善应急预案。</p> <p>服务频率：至少 1 次/年</p> <p>交付成果：《应急演练方案》《应急演练脚本》《应急演练总结报告》等。</p>
8	网络与数据安全培训服务	<p>在服务期内组织不少于 2 次的网络与数据安全培训服务；培训内容包括但不限于：网络安全意识培训、数据安全意识培训、网络安全的法律法规、数据安全的法律法规、网络安全事件案例分析、数据安全事件案例分析等；每次培训时长不少于 2 小时，培训师资由中标单位负责，培训讲师应为具备相应资质或相关从业经验的专家学者和机关企事业单位人员。</p> <p>服务频率：2 次/年</p> <p>交付成果：《培训内容》《培训师资情况》《培训过程记录》等。</p>
9	应用系统个人信息合规评估及检测服务	<p>依据《中华人民共和国个人信息保护法》等法律法规要求，对招标方机关涉及个人信息处理的全部应用系统开展个人信息保护影响评估及合规性检测，检测内容包含但不限于个人信息收集范围，个人信息使用目的、方式、范围，APP 权限申请范围，权限申请细则，是否超范围收集个人信息等，并协助招标方完成整改。</p> <p>服务频率：2 次/年</p> <p>交付成果：《APP 及小程序合规检测服务报告》</p>
10	网络安全风险评估服务	<p>依据国家标准《GB/T 20984 信息安全技术 信息安全风险评估规范》，对业务系统的安全现状开展全面评估。通过识别信息资产、分析面临的威胁和存在的脆弱性，评估现有防护措施的有效性，综合判断安全风险发生的可能性，并据此提供风险处置方案。</p>

		<p>服务内容：资产识别、安全基线核查、Web 漏洞扫描、主机漏洞扫描、威胁识别、风险分析。</p> <p>服务频率：至少 1 次/年</p> <p>交付成果：《网络安全风险评估报告》</p>
11	数据安全风险评估	<p>1. 能够依据《数据安全法》《个人信息保护法》及相关国家标准（如《网络数据安全风险评估实施指引》），在数据分类分级基础上，对招标方数据安全状况、数据处理活动、数据安全保护措施及个人信息保护情况开展差异化风险评估。</p> <p>2. 对被评估系统或平台本身的安全风险进行识别，识别手段至少包括漏洞扫描、渗透测试等，并基于评估结果编制数据安全风险评估报告。</p> <p>3. 投标方须具备符合国家标准的数据安全风险评估能力，并配备相应评估工具。该工具应能够围绕数据安全、数据处理活动、数据安全等方面，辅助分析潜在数据安全风险，并自动化输出高质量的评估报告。</p> <p>4. 数据安全风险评估工具应支持在招标方隔离网络环境中部署，所有服务过程中产生的材料、数据及报告均须留存于招标方本地。</p> <p>5. 工具应设有授权有效期，授权过期后工具应自动失效，且工具内留存的任何数据均不得以明文形式显示或通过任何方式被逆向获取。</p> <p>6. 工具应具备环境绑定功能，仅可在经授权的特定计算机环境中运行。一旦脱离授权环境，工具应无法使用，且其中留存的数据应无法被读取或逆向获取。</p> <p>服务频率：至少 1 次/年</p> <p>交付成果：《数据安全风险评估报告》</p>
12	7×24 小时网络安全运营及网络安全事件	<p>1. 资产安全托管服务：提供不少于 40 个 IP 地址的政务系统安全托管服务，服务期限不少于 1 年。</p> <p>2. 互联网暴露面梳理服务：使用专业安全工具，对招标方资产开</p>

	报告服务	<p>展互联网暴露面探测，梳理资产在互联网的开放情况，及时发现违规暴露资产及潜在风险并进行处置，实现暴露面资产的可管可控，降低安全风险。</p> <p>服务工具须支持“全资产”与“精确资产”两种暴露面发现模式。发现的暴露面信息至少须包括：域名、域名标题、IP 地址、开放端口、资产指纹、网站截图、移动端暴露面信息，并能提供对应暴露资产的访问截图作为举证材料。</p> <p>投标方须在投标文件中提供工具具备上述能力的证明截图。</p> <p>3. 脆弱性管理服务：针对服务范围内资产扫描发现的高危、可利用漏洞，投标方应为招标方提供全面的防护支持，包括但不限于：提供漏洞修复方案；提供安全设备防护策略；配置防护规则，须提供其服务平台具备高危漏洞自动匹配防护规则功能的证明，确保招标方不因相关漏洞导致安全事件或损失。</p> <p>4. 威胁管理服务：投标方应具备云端安全检测与分析平台，能够采集招标方安全设备及系统的安全告警与日志，并基于大数据分析、人工智能等技术，提供 7×24 小时持续不间断的安全威胁分析与鉴定服务。</p> <p>分析鉴定服务包括但不限于对脆弱性、异常流量、攻击日志、病毒日志等数据的采集与实时分析研判；支持将同一资产的多个告警进行聚合分析，发现安全事件后自动生成处置工单；告警详情中须清晰展示基本信息、涉及的业务、攻击趋势、威胁详情、攻击原理、处置建议等内容，同时支持根据招标方实际情况添加备注。投标方需提供云端服务平台告警鉴定功能的界面截图，并附告警聚合分析案例及告警详情展示（需体现上述能力）。</p> <p>个性化检测规则定制：为保障安全监测的准确率与服务质量，投标方应支持招标方自定义配置安全规则，以满足日益复杂的安全态势下的安全监测需求；需提供投标方服务平台支持用户自定义配置安全规则的界面截图。</p> <p>受影响资产排查与加固：安全专家应结合威胁情报主动排查资产</p>
--	------	---

	<p>是否对服务资产造成影响，及时通知招标方并协助开展安全加固工作。</p> <p>安全策略检查：投标方安全专家需每月对招标方安全设备的防护策略进行检查，确保安全设备的防护策略始终处于最优水平。针对威胁防范效果良好的防护策略，投标方云端服务平台应配备策略检查工具（要求不少于 40 种策略检查工具），支持检查安全设备防护策略配置的合理性。</p> <p>5. 服务团队配置：为保障服务质量、强化与招标方的沟通，投标方应承诺为招标方配备 1 名经验丰富的安全专家担任专属服务经理以及满足需求的安全人员，保证及时响应招标方咨询的网络安全相关问题。同时，投标方需为招标方提供 7 × 24 小时安全值守服务，且节假日及重保期间应每日向招标方提交《值守总结》。</p> <p>6. 交付物管理：投标方需为招标方提供服务成果展示门户（即用户 Portal），支持直观管理服务过程中产生的服务报告与交付物，包括但不限于《准备阶段文件》《特殊时期值守报告》《运营周报》《运营月报》《运营季报》《威胁情报》《年度汇报》《事件总结报告》《安全防护策略检查记录》《安全防护策略调整审批记录》等。同时，该成果展示门户需支持下载、管理上述交付物对应的的相关佐证材料。</p> <p>7. 平台合规要求：投标方用于提供安全托管服务的云端平台，必须已通过国家相关部门联合组织的云计算服务安全评估，并入选中央网信办官方网站发布的《通过云计算服务安全评估的云平台》名单。须提供该名单的官方网站截图作为证明，截图中应能清晰辨识其平台名称及“安全托管服务”相关标识或说明。</p> <p>8. 服务流程引擎：为确保服务效率与质量，投标方的云端平台需具备可视化服务流程编排引擎，支持根据客户实际需求灵活定义服务流程与服务等级协议（SLA），并能将各服务环节按预定规则与顺序进行自动化组织和调度。投标方须提供平台流程编排功能的相关界面截图或技术说明文件作为证明。</p>
--	---

		<p>9. 服务成果展示门户要求：服务成果展示门户（或用户 Portal）应具备服务质量可视化展示功能，投标方需通过可视化数据呈现安全专家的服务水平。展示维度至少包括：脆弱性闭环率、脆弱性平均响应时长、脆弱性平均闭环时长、威胁闭环率、威胁平均响应时长、威胁平均闭环时长、事件闭环率、事件平均闭环时长。</p> <p>10. 驻场服务人员要求：需配备至少 1 名驻场服务人员，该人员须具备 CISP 证书或数据治理工程师资质等至少 1 项国家级或行业权威认证。</p> <p>11. 网络安全事件报告要求：按照《国家网络安全事件报告管理办法》协助招标方开展网络安全事件处置报告等有关工作。</p>
13	上网行为管理服务	<p>上网行为管理服务：对办公人员的上网行为进行合规性管理，降低因接入互联网引发的安全风险。可完整记录办公人员的上网行为，支持审计网站、软件、邮件、办公类应用等访问记录；一旦发生网络违规违纪事件，可追溯源头，实现事前防范、事后溯源，全面保障办公信息安全。同时，对邮件等应用内的敏感信息提供预警，对文件对外发送行为实施全面管控，以满足政务服务的安全需求，保障政务工作的正常开展。</p> <p>服务频率：4 次/年</p> <p>交付成果：《上网行为管理服务报告》</p>
14	网络安全等级保护测评服务	<p>根据《信息安全等级保护管理办法》《信息安全技术网络安全等级保护基本要求（GB/T22239-2019）》的有关规定和《内蒙古自治区计算机信息系统安全保护办法》（内蒙古自治区人民政府令第 183 号）的要求，构对招标方的内蒙古人大门户网站、内蒙古人大 APP、综合应用平台、信访小程序、无纸化会议系统、自治区人大代表履职平台、干部考核系统、规范性文件备案审查系统、法规规章规范性文件数据库等 9 个三级系统进行网络安全等级保护测评，且出具相应资质的测评报告，测评不通过的协助招标方整改至通过测评。</p>

		<p>服务频率：1 次/年</p> <p>交付成果：《XX 系统等级保护测评报告》</p>
15	商用密码应用安全性评估	<p>根据《密码法》和《商用密码管理条例》（国务院令第 760 号）及《商用密码应用安全性评估管理办法》（国家密码管理局令第 3 号）的规定和 GB/T39786-2021《信息安全技术信息系统密码应用基本要求》等标准，对招标方的无纸化办公会议系统、自治区人大代表履职平台、法规规章规范性文件数据库 3 个系统进行商用密码应用安全性评估，且出具相应资质的测评报告，测评不通过的协助招标方整改至通过测评。</p> <p>服务频率：1 次/年</p> <p>交付成果：《XX 系统商用密码应用安全性评估报告》</p>
16	网络安全、数据安全合规性检测服务	<p>根据国家、自治区网络安全和数据安全、密码安全有关法律法规要求，对招标方相关网络、系统、数据法律合规性予以梳理，补充和完善，达到全面、规范符合国家有关法律法规和技术标准的规范要求。</p> <p>服务频率：2 次/年</p> <p>交付成果：《网络安全和数据安全、密码安全合规及整改报告（上、下）》</p>

2、网络安全服务工具要求：

①为了保障服务质量，主机防护系统应能够支持如下功能：

序号	指标要求
1	安全策略模板一体化设置，全网资产盘点与风险可视，自动化日志可视化报表一键导出，管理账号分权分域，总分平台级联控制。
2	支持对系统账号信息进行梳理，了解账号权限分布概况以及风险账号分布情况，可按照隐藏账号、弱密码账号、可疑 root 权限账号、长期未使用账号、夜间登录、多 IP 登录进行账号分类查看，支持统计最近一年未修改密码的账户。

3	流量线详情支持展示该流量线对应的控制策略；图形化显示服务器间流量关系，包括访问详情、流量趋势等。
4	基于勒索病毒攻击过程，建立多维度立体防护机制，提供事前入侵防御-事中反加密-事后检测响应的完整防护体系，展示勒索病毒处置情况，对勒索病毒及变种实现专门有效防御。（需提供产品截图证明）
5	支持客户端的错峰升级或灰度升级，可根据实际情况控制客户端同时升级的最大数量，避免大量终端程序同时更新造成网络拥堵或 I/O 风暴。（需提供产品截图证明）
6	支持展示终端检测到的 WebShell 事件及事件详情，包括：恶意文件名称，威胁等级，受感染的文件，发现时间，检测引擎，文件类型，文件名，文件 Hash 值，文件大小，文件创建时间；可配置 WebShell 实时扫描，一旦发现 WebShell 文件，可自动隔离或仅上报不隔离。（需提供产品截图证明）。
7	支持用户直接对勒索病毒的家族名、病毒名、加密文件后缀名执行链接查询，可通过直接上传加密文件的方式确定勒索病毒类型，如果能解密可以提供必要的解密工具。

②为了保证服务质量与有效性，投标方所使用的云防护产品应具备：

序号	指标要求
1	支持针对主流 Web 服务器及插件的已知漏洞防护。Web 服务器应覆盖主流服务器：apache、tomcat、lighttpd、NGINX、IIS 等插件应覆盖：dedecms、phpmyadmin、PHPWind、shopex、discuz、ecshop、vbulletin、wordpress 等，提供 Java 反序列化漏洞（Jboss）防护插件。
2	支持 CSRF（跨站请求伪造）防护。
3	支持 Cookie 安全机制，包括 Cookie 加密和 Cookie 签名的防护算法。支持过期兼容时间配置以及*配置。
4	支持 XML 防护，包括 XML 基础校验（包括最大树深度、元素名长度、元素个数、子节点个数等参数配置）、Schema 校验以及 SOAP 校验。
5	提供 10 个子域名，共享 10M 防护带宽；支持 http/https 协议，提供远程技术支

	持及专家服务。
--	---------

③针对政务应用的特殊性，投标方所使用的上网行为管理产品需要具备：

序号	指标要求
1	支持攻击、双机切换告警、移动终端管理告警、风险终端发现告警、web 关键字过滤告警、杀毒告警、设备流量超限告警、磁盘/CPU/内存异常告警等。
2	能够对 teamview、QQ 远程桌面等远程控制应用做细分控制，如：接受对方远程控制。
3	支持终端调用管理员指定脚本/程序以满足个性化检查要求，比如检测系统更新是否开启、开放端口、已安装程序列表、终端发通知等对不满足检查要求的终端可弹窗提示、禁止上网。（提供截图证明文件）
4	支持在设置流量策略后，根据整体线路或者某流量通道内的空闲情况，自动启用和停止使用流量控制策略，以提升带宽的高使用率；空闲值可自定义。（提供产品界面截图）
5	设备必须支持能自动发现网络中通过无线上网的热点和移动终端的 IP 和终端类型，支持移动终端型号识别，至少识别不少于 10 种移动终端型号。（提供产品界面截图）
6	支持通过抑制 P2P 的上行流量，来减缓 P2P 的下行流量，从而解决网络出口在做流控后仍然压力较大的问题。

3、网络安全等级保护测评服务要求：

（1）系统安全等级定级和备案

投标方需协助招标方对所部署的政务应用系统参照《信息安全技术网络安全等级保护定级指南》（GB/T22240-2020）进行安全定级备案，并提供备案证明作为测评前提。

（2）等级保护测评服务

投标方按照国家及行业信息安全等级保护管理规范和技术标准，判断信息系统的安全保护能力与国家及行业要求之间的符合程度的差距分析测评方案。测评技术方案应包括但不限于：对本次测评工作的说明、定级梳理、备案、采用的技术方案、测试方法、测试工具使用，测评过程中的风险控制，以及需要招标方了解的其他问题。针对本项目的等保服务技术方案：

其中二级系统测评项不少于 135 项，三级系统测评项不少于 211 项。服务期内首次等保测评未通过的，投标方必须对相关问题进行整改至符合国家有关要求并测评通过。

（3）安全物理和环境

物理安全测评通过访谈和检查的方式评测物理环境安全保障情况。主要涉及对象为信息系统机房。具体测评内容包括：①物理位置的选择；②物理访问控制；③防盗窃和防破坏；④防雷击；⑤防火；⑥防水和防潮；⑦防静电；⑧温湿度控制；⑨电力供应；⑩电磁防护。

（4）安全通信网络

安全通信网络测评通过访谈、检查和测试的方式评测信息系统的网络安全保障情况。主要涉及对象为信息系统的网络拓扑结构、网络设备以及网络安全设备等三大类。具体的测评内容如下所示：①网络架构；②通信传输；③可信验证。

安全区域边界：①边界防护；②访问控制；③恶意代码防范；④安全审计；⑤入侵防范；⑥可信验证。

（5）安全计算环境

主机系统安全测评通过访谈、检查和测试的方式，测评信息系统主要服务器操作系统和主要数据库管理系统安全保障情况。具体测评内容包括：①身份鉴别；②访问控制；③安全审计；④入侵防范；⑤恶意代码防范；⑥可信验证；⑦数据完整性；⑧数据保密性；⑨数据备份恢复；⑩剩余信息保护；⑪个人信息保护。

安全管理中心：①系统管理；②审计管理；③安全管理；④集中监控。

（6）安全管理制度

安全管理制度测评通过访谈和检查的形式评估安全管理制度的制定、发布、评审和修订等情况。主要涉及安全主管人员、安全管理人员、各类其他人员、各类管理制度、各类操作规程文件等对象。具体测评内容包括：①管理制度；②安全策略；③制定和发布；④评审和修订。

（7）安全管理机构

安全管理机构测评通过访谈和检查的形式评估安全管理机构的组成情况和机构工作组织情况。主要涉及安全主管人员、安全管理人员、相关的文件资料和工作记录等对象。具体测评内容包括：①岗位设置；②人员配备；③授权和审批；④沟通和合作；⑤审核和检查。

安全管理人员：①人员录用；②人员离岗；③安全意识教育和培训；④外部人员访问管理。

（8）安全建设管理

系统建设管理测评通过访谈和检查的形式评估系统建设管理过程中的安全控制情况。主要涉及安全主管人员、系统建设负责人、各类管理制度、操作规程文件、执行过程记录等对象。具体测评内容包括：①定级和备案；②安全方案设计；③产品采购和使用；④自行软件开发；⑤外包软件开发；⑥工程实施；⑦测试验收；⑧系统交付；⑨等级测评；⑩服务供应商选择。

（9）安全运维管理

通过访谈和检查的形式评测系统运维管理过程中的安全控制情况。主要涉及人员有安全主管人员、安全管理人员、各类运维人员，涉及内容有开发方的运维管理制度、信息中心关于运维服务团队的各项管理制度、操作规程文件、执行过程记录等对象。具体测评内容包括：①环境管理；②资产管理；③介质管理；④设备维护管理；⑤漏洞和风险管理；⑥网络和系统安全管理；⑦恶意代码防范管理；⑧配置管理；⑨密码管理；⑩变更管理；⑪备份与恢复管理；⑫安全事件处置；⑬应急预案管理；⑭外包运维管理。

4、商用密码应用安全性评估服务要求：

依据《信息安全技术信息系统密码应用基本要求》（GB/T39786-2021）《信息系统密码测评要求》《商用密码应用安全性评估测评过程指南》和系统自身的安全性需求分析，对上线后的系统商用密码应用的合规性，正确性，有效性进行安全性评估，提供相应《密码应用安全性评估报告》，通过密码应用安全性评估深入查找密码应用的薄弱环节和安全隐患，分析面临的风险，为提升信息系统安全奠定基础。服务期内首次密码测评未通过的，必须将相关问题整改至符合国家有关要求，并测评通过。

（1）通用要求

- a) 信息系统中使用的密码算法应符合法律、法规的规定和密码相关国家标准、行业标准的有关要求；
- b) 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；
- c) 信息系统中使用的密码产品、密码服务应符合法律法规的相关要求；
- d) 密码测评机构需持有商用密码应用性安全性评估机构资质证书。

（2）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。

a) 物理和环境安全测评

分析评估信息系统是否合规、正确、有效的使用商用密码技术对信息系统的物理和环境层面各对象进行保护,包括但不限于下列典型因素:物理访问身份鉴别,保证重要区域进入人员身份的真实性;保证电子门禁系统进出记录数据的存储完整性;保证视频监控音像记录数据的存储完整性。

b) 网络和通信安全测评

分析评估信息系统是否合规、正确、有效的使用商用密码技术对信息系统的网络和通信层面各对象进行保护。包括但不限于下列典型因素:对通信实体进行身份鉴别,保证通信实体身份的真实性;保证通信过程中数据的完整性;保证通信过程中数据的机密性;保证网络边界访问控制信息的完整性;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。

c) 设备和计算安全测评

分析评估信息系统是否合规、正确、有效的使用商用密码技术对信息系统的设备和计算层面各对象进行保护。包括但不限于下列典型因素:对登录设备的用户进行身份鉴别,保证用户身份的真实性;采用密码技术建立安全的信息传输通道;保证系统资源访问控制信息的完整性;保证设备中的重要信息资源安全标记的完整性;保证日志记录的完整性;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;

d) 应用和数据安全测评

分析评估信息系统是否合规、正确、有效的使用商用密码技术对信息系统的应用和数据层面各对象进行保护。包括但不限于下列典型因素: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;对应用的访问控制信息的完整性;对应用的信息资源安全标记的完整性;对应用的数据在传输过程中的机密性;对应用的数据在存储过程中的机密性;对应用的数据在传输过程中的完整性;对应用的数据在存储过程中的完整性;对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;

(3) 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:密钥产生,密钥分发、密钥存储,密钥使用,密钥更新、密钥备份,密钥归档,密钥撤销,密钥恢复,密钥销毁等。

(4) 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

限于下列内容：管理制度、人员管理、建设运行、应急处置等。

a) 管理制度：包括但不限于下列内容与措施：密码建设、运维、人员、设备、密钥管理内容，密码相关操作规范、安全操作规范，安全管理制度的合理性和适用性论证与审定，安全管理制度的改进和修订，安全管理制度的发布，安全管理制度的执行等。

b) 人员管理：包括但不限于下列内容与措施：了解并遵守密码相关法律法规，密码产品使用，关键岗位划分，相关人员职责与权限划分，岗位责任制与人员制约、监督机制，管理和使用账号，人员培训、人员选拔，人员考核、奖惩与调离，人员保密等措施。

c) 建设运行：包括但不限于下列内容与措施：信息系统规划，信息系统建设方案，信息系统密码产品、服务选用，信息系统运行前与定期评估，信息系统整改等。

d) 应急处置：包括但不限于下列内容与措施：应急预案，应急资源准备，应急情况与处置，同级主管部门应急报告，同级密码主管部门应急报告等。

评分细则

(一) 基本评分标准

评分因素 及权重	分值	评分标准	说明
报价 10%	10 分	<p>本次招标面向中小微企业（监狱企业、残疾人福利单位视同小微企业），有效的最低投标报价为基准价，投标报价得分=（基准价/投标报价）×10 分×100 %</p> <p>参加政府采购活动的中小企业应当提供《中小企业声明函》原件，监狱企业应当提供《监狱企业证明》原件，残疾人福利性单位应当提供《残疾人福利性单位声明函》原件。</p>	
技术服务要求 20%	20 分	<p>1. 主机防护服务工具功能满足程度： 投标服务自带工具完全满足磋商文件规定的技术参数和要求的得 8 分，技术参数 1 项不满足扣 1 分，扣完为止。</p> <p>2. 云防护服务工具功能满足程度： 投标服务自带工具完全满足磋商文件规定的技术参数和要求的得 5 分，技术参数 1 项不满足扣 1 分，扣完为止。</p> <p>3. 上网行为管理工具功能满足程度： 投标服务自带工具完全满足磋商文件规定的技术参数和要求的得 7 分，技术参数 1 项不满足扣 1 分，扣完为止。</p>	

投标方服务能力 8%	8分	<p>服务人员能力要求,标准如下:</p> <p>1. 项目经理具备以下证书可加分:</p> <p>(1) CIPS 资质; (2) CISP-PTE 资质; (3) 数据安全评估师资质。具备 1 项得 1 分, 最高 3 分。</p> <p>2. 安全服务项目组人员能力要求:</p> <p>(1) 项目驻场人员不少于 1 人, 要求具备 CISP 证书或数据治理工程师证书等至少 1 项国家级或行业权威认证; 具备 1 项能力证书得 1 分, 最高得 2 分。</p> <p>(2) 安全服务人员不少于 3 名, 要求具备信息安全工程师资质 (CISP)、CISAW 信息安全保障人员认证证书 (认证方向: 应急服务)、数据治理工程师, 具备 1 项能力证书得 1 分, 最高得 3 分, 不提供不得分。</p>	项目经理及团队人员需提供在职证明材料, 未提供不得分。所有证书需提供复印件并加盖投标方公章。
项目经验 3%	3分	<p>近三年与本项目同类的项目业绩, 以服务合同为准 (每有一个得 1 分, 最高得 3 分)。注: 近三年是指 2023 年至今, 提供合同复印件加盖投标方公章 (鲜章)。</p>	
服务方案 50%	50分	<p>1. 主机防护服务方案 (3 分): 从①工作思路和详细实施方案②项目风险点的理解以及应对措施③完整合理的质量控制方案和现场人员考核措施等方面进行综合评审, 每项内容完整, 适用符合行业特征和本项目项目特点得 3 分, 每缺失 1 项扣 1 分, 每项中每有一处表述不清楚、针对性不强、逻辑不清晰的扣 0.5 分, 扣完为止。</p> <p>2. 云防护服务方案 (3 分): 从①工作思路和详细实施方案②项目风险点的理解以及应对措施③完整合理的质量控制方案和人员考核措施等方面进行综合评审, 每项内容完整, 适用符合行业特征和本项目项目特点得 3 分, 每缺失 1 项扣 1 分, 每项中每有一处表述不清楚、针对性不强、逻辑不清晰的扣 0.5 分, 扣完为止。</p> <p>3. 漏洞扫描服务方案 (3 分): 从①工作思路和详细实施方案②项目风险点的理解以及应对措施③完整合理的质量控制方案和现场</p>	

	<p>人员考核措施等方面进行综合评审，每项内容完整，适用符合行业特征和本项目项目特点得 3 分，每缺失 1 项扣 1 分，每项中每有一处表述不清楚、针对性不强、逻辑不清晰的扣 0.5 分，扣完为止。</p> <p>4. 网站安全及渗透测试服务方案 (3 分)：从①工作思路和详细实施方案②项目风险点的理解以及应对措施③完整合理的质量控制方案和现场人员考核措施等方面进行综合评审，每项内容完整，适用符合行业特征和本项目项目特点得 3 分，每缺失 1 项扣 1 分，每项中每有一处表述不清楚、针对性不强、逻辑不清晰的扣 0.5 分，扣完为止。</p> <p>5. 重要时期保障服务方案 (3 分)：从①工作思路和详细实施方案②项目风险点的理解以及应对措施③完整合理的质量控制方案和现场人员考核措施等方面进行综合评审，每项内容完整，适用符合行业特征和本项目项目特点得 3 分，每缺失 1 项扣 1 分，每项中每有一处表述不清楚、针对性不强、逻辑不清晰的扣 0.5 分，扣完为止。</p> <p>6. 新业务上线前安全检测服务方案 (3 分)：从①工作思路和详细实施方案②项目风险点的理解以及应对措施③完整合理的质量控制方案和现场人员考核措施等方面进行综合评审，每项内容完整，适用符合行业特征和本项目项目特点得 3 分，每缺失 1 项扣 1 分，每项中每有一处表述不清楚、针对性不强、逻辑不清晰的扣 0.5 分，扣完为止。</p> <p>7. 应急演练服务方案 (3 分)：从①工作思路和详细实施方案②项目风险点的理解以及应对措施③完整合理的质量控制方案和现场人员考核措施等方面进行综合评审，每项内容完整，适用符合行业特征和本项目项目特点得 3 分，每缺失 1 项扣 1 分，每项中每有一处表述不清楚、针对性不强、逻辑不清晰的扣 0.5 分，扣完为止。</p> <p>8. 网络与数据安全培训服务方案 (2 分)：从①工作思路和详细实施方案②完整合理的培训内容设计及讲师的设置等方面进</p>	
--	--	--

	<p>行综合评审，每项内容完整，适用符合行业特征和本项目项目特点得 2 分，每缺失 1 项扣 1 分，每项中每有一处表述不清楚、针对性不强、逻辑不清晰的扣 0.5 分，扣完为止。</p> <p>9. APP 及小程序合规检测服务方案（3 分）：从①工作思路和详细实施方案②项目风险点的理解以及应对措施③完整合理的质量控制方案和现场人员考核措施等方面进行综合评审，每项内容完整，适用符合行业特征和本项目项目特点得 3 分，每缺失 1 项扣 1 分，每项中每有一处表述不清楚、针对性不强、逻辑不清晰的扣 0.5 分，扣完为止。</p> <p>10. 网络安全风险评估服务方案（3 分）：从①工作思路和详细实施方案②项目风险点的理解以及应对措施③完整合理的质量控制方案和现场人员考核措施等方面进行综合评审，每项内容完整，适用符合行业特征和本项目项目特点得 3 分，每缺失 1 项扣 1 分，每项中每有一处表述不清楚、针对性不强、逻辑不清晰的扣 0.5 分，扣完为止。</p> <p>11. 数据安全风险评估服务方案（3 分）：从①工作思路和详细实施方案②项目风险点的理解以及应对措施③完整合理的质量控制方案和现场人员考核措施等方面进行综合评审，每项内容完整，适用符合行业特征和本项目项目特点得 3 分，每缺失 1 项扣 1 分，每项中每有一处表述不清楚、针对性不强、逻辑不清晰的扣 0.5 分，扣完为止。</p> <p>12. 7×24 小时网络安全运营服务方案（4 分）：从①工作思路和详细实施方案②项目风险点的理解以及应对措施③服务内容与交付物清晰④完整合理的质量控制方案和现场人员考核措施等方面进行综合评审，每项内容完整，适用符合行业特征和本项目项目特点得 4 分，每缺失 1 项扣 1 分，每项中每有一处表述不清楚、针对性不强、逻辑不清晰的扣 0.5 分，扣完为止。</p> <p>13. 上网行为管理服务方案（3 分）：从①工作思路和详细实施方案②项目风险点的理解以及应对措施③完整合理的质量控制方</p>	
--	---	--

	<p>案和人员考核措施等方面进行综合评审，每项内容完整，适用符合行业特征和本项目项目特点得 3 分，每缺失 1 项扣 1 分，每项中每有一处表述不清楚、针对性不强、逻辑不清晰的扣 0.5 分，扣完为止。</p> <p>14. 网络安全等级保护测评服务（4 分）：从①方案严格遵守国家网络安全等级保护制度的相关法律法规、政策文件和技术标准，方案覆盖所有适用测评项②方案设计的科学性和可操作性③项目风险点的理解以及应对措施④方案规划清晰、有价值的输出成果，并能应对测评不通过情况下如何整改通过测评等方面进行综合评审，每项内容完整，适用符合行业特征和本项目项目特点得 4 分，每缺失 1 项扣 1 分，每项中每有一处表述不清楚、针对性不强、逻辑不清晰的扣 0.5 分，扣完为止。</p> <p>15. 商用密码应用安全性评估服务（4 分）：①方案覆盖密码应用主要环节，严格遵守国家及行业相关法律法规、技术标准和规范②方案设计的测评路线和指标科学、合理，流程清晰具体③项目风险点的理解以及应对措施④方案规划清晰、有价值的输出成果，并能应对测评不通过情况下如何整改通过测评等方面进行综合评审，每项内容完整，适用符合行业特征和本项目项目特点得 4 分，每缺失 1 项扣 1 分，每项中每有一处表述不清楚、针对性不强、逻辑不清晰的扣 0.5 分，扣完为止。</p> <p>注：“表述不清楚、针对性不强、逻辑不清晰”是指投标方提供的内容存在不适用项目实际情况的情形、套用其他方案、凭空捏造、逻辑漏洞、科学原理错误以及不可能实现的夸大情形等情况。</p> <p>16. 网络安全、数据安全以及其他合规性服务方案（3 分）：从①方案概述与目标明确性②合规依据全面性与时效性③检查内容与检查点细致度④方案内容与方法的可操作性⑤检查方法与流程的科学性，每项内容完整合理，符合行业特征和本项目项目特点得 3 分，每缺失 1 项扣 0.6 分，每项中每有一处表</p>	
--	--	--

		述不清楚、针对性不强、逻辑不清等的扣 0.3 分，扣完为止。	
售 后 服 务 9%	9 分	<p>投标方编制售后服务方案，方案内容包括：①售后服务内容；②售后服务机构网点清单及服务电话；③售后服务人员名单及联系电话；④售后服务流程⑤应急方案⑥维保能力等因素。投标方编制的售后服务方案包括以上内容、具有针对性且不存在不适用项目实际情况的情形，不存在凭空编造、逻辑漏洞、科学原理错误以及不可能实现的夸大情形等情况的得 6 分，每有 1 项不满足或未提供扣 1 分，扣完为止。</p> <p>投标方编制的售后服务方案有更利于采购人对本项目的工作实施开展并且细节分析到位的，每有 1 项加 1 分，最多加 3 分。</p>	