项目采购需求

本项目需落实的政府采购政策：《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）、《关于政府采购支持监狱企业发展有关问题的通知》（财库〔2014〕68号）、《关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）等。

本项目为服务类项目，中小企业划分标准所属行业为：软件和信息技术服务业。

**一、项目概况**

（一）项目名称

省生态环境监测中心政务信息化运维运营（2024年）项目省生态环境监测中心网络安全运营服务。

（二）采购人

广东省生态环境监测中心。

（三）项目预算

人民币1,100,800.00元。

（四）服务地点

广东省生态环境监测中心指定。

1. 项目目标

帮助省生态环境监测中心在信息化基础设施和业务应用系统的安全运行上建立可靠的网络安全运营体系，提升安全防护与预警、监测与分析、事件响应及处置、网络安全风险管理以及安全支撑服务的能力，保障省生态环境监测中业务信息系统持续安全稳定可靠地运行，确保业务正常有序开展。

**二、服务期限**

本项目委托服务期限以合同签订之日为服务起始时间，服务期为12个月。

**三、服务内容**

1. **重大节日（活动）网络安全保障**

提供在重大节日（活动）期间的网站安全保障服务，重大节日（活动）指春节、“五一”劳动节、国庆节等大型节假日和全国“两会”、“粤盾杯”网络安全攻防演练等重大活动/事件。保障期间根据甲方要求，通过现场、远程或两者结合的方式提供威胁监控、安全预警、突发事件处置等服务，保障重大节日（活动）期间甲方的网络运行安全。

服务频率：1次/季度

服务成果：《重大节日（活动）网络安全保障报告》（具体以每节日/活动为准）

1. **网络安全应急演练支撑服务**

按照省生态环境监测中心的网络安全监管需求，开展一次网络安全应急演练支撑服务，编制《网络安全应急演练报告》，并协助甲方完善《网络安全应急预案》。

通过网络安全应急演练，可以使省监测中心相关技术人员掌握网络安全应急处理的正确方法，熟悉预案的相关流程序，确保在网络安全事件发生时，能快速、高效、有序地进行，从而最大限度地保护信息系统的保密性、完整性和可用性。同时通过演练，不断提高团队掌握应急工作的水平和效率，发现预案设计的不足，进一步完善应急预案。

服务频率：1次/年

服务成果：《网络安全应急预案》、《网络安全应急演练报告》

1. **网络安全事故处置**

对省监测中心的服务对象进行网络安全事故处置服务。在目标系统遭受黑客入侵攻击时，现场值守人员立即对入侵事件进行分析，结合应急响应预案开展处置，如无法第一时间处置，要立即增派技术专家到现场开展支撑，对入侵事件进行检测、抑制、处理，查找入侵来源并恢复系统正常运行。

应对突发事件，以防范信息系统风险为目的，建立统一指挥、协调有序的应急管理机制和相关协调机制，以落实和完善应急预案为基础，全面加强安全事故处置工作，并制定有效的问责制度。

坚持以预防为主，建立和完善信息系统突发事件风险防范体系，对可能导致突发事件的风险进行有效地识别、分析和控制，减少重大突发事件发生的可能性，加强应急处置队伍建设，提供充分的资源保障，确保突发事件发生时反应快速、报告及时、措施得力操作准确，降低事件可能造成的损失。

服务频率：6次/年

服务成果：《网络安全事故处置报告》

1. **安全风险评估服务**

信息资产：梳理内容应包含硬件设备型号、IP地址、系统版本信息、数据库版本信息、所属人、使用人；

基础架构：梳理内容应包含机房位置、设备机柜号、设备类型、设备标签、综合布线图等，应用与设备切实做到基础架构图和实物对应；

信息系统梳理：梳理内容应包含信息系统名称、开发环境、开发语言、中间件类型、中间件版本信息、数据库类型、数据库版本信息、系统所属人、系统使用人、系统基础硬件（服务器）托管/存放位置。

服务频率：1次/半年

服务成果：《信息安全综合评估报告》、《信息资产清单》。

1. **应用安全渗透测试服务**

服务期内对服务对象定期开展应用安全渗透测试服务，编制形成《应用安全渗透测试报告》。

1) 明确安全隐患：渗透测试是一个从空间到面再到点的过程，测试人员模拟黑客的入侵，从外部整体切入最终落至某个威胁点并加以利用，最终对整个网络产生威胁，以此明确整体系统中的安全隐患点。

2) 提高安全意识：任何的隐患在渗透测试服务中都可能造成“千里之堤溃于蚁穴”的效果，因此渗透测试服务可有效督促管理人员杜绝任何一处小的缺陷，从而降低整体风险。

3) 提高安全技能：在测试人员与用户的交互过程中，可提升用户的技能。另外，通过专业的渗透测试报告，提供当前流行安全问题的参考。

服务频率：1次/月

服务成果：《应用安全渗透测试报告》

1. **漏洞扫描服务**

服务期内定期对服务对象开展全面漏洞扫描（包括主机、操作系统、应用、设备等），并提供漏洞扫描报告。

主机系统漏洞扫描：操作系统猜测、端口服务扫描、系统漏洞扫描、弱口令破解、用户权限认证、磁盘共享等。

应用系统漏洞扫描：SQL注入、脚本跨站攻击、路径泄漏、后台验证漏洞、文件上传漏洞、远程文件包含漏洞、已知WEB应用程序公开漏洞、弱口令猜解、补丁、账号管理、口令强度和有效期检查、远程登陆和远程服务等。

网络设备漏洞扫描：弱口令猜解、补丁、账号管理、口令强度和有效期检查、IOS信息、端口服务等。

服务频率：1次/月

服务成果：《漏洞扫描报告》

1. **基线核查服务**

依据安全基线合规配置要求，对中心系统主机服务器主动提前进行安全的弱点排查和管理，检查范围包括管理远程工具、访问控制、限制系统无用的默认账号登录、root远程登录、口令策略、FTP用户账号控制、日志记录、日志存储、日志保存、日志系统配置文件保护、日志文件保护、服务优化、Umask权限、控制用户登录会话、关键文件的安全保护等相关配置等。

服务频率：1次/季度

服务成果：《安全配置核查报告》

1. **安全加固服务**

对以上第4/5/6/7项服务实施过程中发现的漏洞、基线不合规等隐患，建议风险隐患清单，开展整改加固并跟踪闭环。

服务频率：根据第4/5/6/7项服务频率开展。

服务成果：《风险隐患清单》、《安全加固报告》

1. **应用安全监测服务**

针对服务对象进行7\*24小时实时安全监测，并定期形成应用安全监测报告，监测内容包括但不限于可用性、安全漏洞、访问并发等。

可用性监测：对应用系统的可用性进行实时的监控，一旦发现网站无法访问，第一时间通知用户。

运行状态监测：对应用系统状态进行监测和分析，包括应用系统的网络流量、各协议流量、会话流量、应用操作行为统计、安全事件报警信息、任意时间段内被访问情况的分布等，从多个角度展现应用系统的运行状态。

异常行为流量监测：监测内部用户违规使用数据扒取软件情况、监测的流量数据、IP频繁访问应用且流量的等进行监测，如出现异常则将会进行报警。对重要的数据信息进行监测保护，保护敏感信息不被违规删除、恶意篡改，在出现类似行为时进行报警。

安全漏洞监测：通过定期的安全漏洞监测能力，及时发现应用系统上的安全漏洞，并报警给对应的管理员，帮助管理员及时修复安全漏洞，保障应用系统安全运行。

支持与监测中心本地安全设备进行联动。

服务频率：1次/季度

服务成果：《应用安全监测报告》

1. **云防护服务**

采购云防护服务对服务对象进行安全防护。云防护服务应对主动外联行为进行监控。支持对互联网访问流量进行分析。支持内网ECS互访流量分析。支持业务可视，可全面了解资产的信息和访问关系，从而及时发现异常流量。

云防护支持同时控制入流量和出流量的访问。支持基于域名的访问控制，严格控制主动外联的出流量。支持主动外联分析，有助于省生态环境监测中心主动发现主机的异常行为。

云防护提供流量日志，可查看经过云防火墙的所有流量数据。省生态环境监测中心可在威胁事件发生的时候通过查看流量日志进行流量和访问源分析，并查看配置的访问控制策略是否生效。

云防护共享100M防护带宽；支持http/https协议，远程技术支持、专家服务和云防护报告。

支持与监测中心本地安全设备进行联动。

服务频率：2个域名/年

服务成果：《云防护报告》

1. **蜜罐服务**

采购蜜罐服务。通过布置作为“诱饵”的主机、网络服务或者其他信息，诱使攻击方对蜜罐实施攻击，通过对攻击行为进行捕获分析，了解攻击方的使用的工具与方法，推测攻击意图和动机，能够使省生态环境监测中心各系统了解目前所面对的安全威胁，帮助省生态环境监测中心利用技术和管理手段来增强各系统的安全防护能力。

服务频率：1次/季度

服务成果：《蜜罐服务报告》

1. **数据安全与备份服务**

基于目前省监测中心内大部分业务都需要产生大量的业务数据，依赖于业务数据进行各类业务处理活动，数据已经成为省监测中心不可或缺的一部分，对省监测中心内决策、指挥、实施等活动都有重要影响，因此保障数据安全和数据备份是省监测中心发展的一大方向。需要安排人员对各类系统的数据进行安全维护，利用已有的资源对数据进行备份处理，完成数据定期备份、备份数据核验、数据表字段更新、数据恢复。

服务频率：1次/月

服务成果：《数据恢复预案》、《数据备份日志》、《备份数据核验报告》

1. **第三方安全审计**

对省监测中心直属部门（处室）以及21个地市相关部门开展网络安全第三方审计工作，主要包括：网络安全责任制落实情况、网络安全组织控制、审批策略、风险管理、质量管理、服务管理、项目管理、业务连续性管理、应用系统生命周期管理等方面进行全面审计，形成网络安全管理总体控制的审计评价和考核结论，为省监测中心提供网络安全整体管理提供决策支撑。

服务频率：1次/半年

服务成果：《网络安全第三方审计报告》

1. **日志审计服务**

本次日志审计服务针对省生态环境监测中心的所有应用系统进行日志收集审计工作。

通过日志采集、日志分析、告警展示、日志检索、日志数据储存，对服务对象开展日志审计服务。通过日志审计满足网络安全管理部门对业务系统日志管理的要求，并可以实现对网络安全事件产生原因的定位。

服务频率：1次/半年

服务成果：《日志审计报告》

1. **安全制度完善**

在制度设计方面，从管理机制、监督机制等方面进行设计，协助建立持续的网络安全培训计划。

构建涵盖顶层设计、方针策略、安全管理规范、安全技术标准、记录表单等五个维度的制度体系规划文件，明确网络安全管理各项要求，形成由安全方针、管理制度、细化流程等构成的全面的网络安全管理制度体系。

通过对制度的完善，加强省监测中心网络安全管理，落实网络安全责任，提高网络安全保障水平。

服务范围：制度完善服务范围为省监测中心的相关网络安全制度。

服务频率：1次/年

服务成果：《安全组织及职责管理规定》、《安全审核与检查管理制度》、《授权和审批管理规定》、《内部人员信息安全管理规定》、《外部人员信息安全管理规定》、《机房安全管理规定》、《系统安全管理规定》、《防病毒管理规定》、《安全事件预警处置规定》、《安全服务规范》、《安全服务考核制度》

1. **安全培训与安全宣传**

每年对省监测中心全体人员进行一次网络安全教育培训，使省监测中心全部人员能够从不同层级了解国际、国内、单位、个人日常工作生活中面临的信息安全风险，理解个人信息安全意识在整体组织的信息安全保障体系中的重要性，学会如何养成良好的信息安全习惯、具备正确的信息安全意识，使个人能够依靠自身良好的信息安全意识与素养支持所在单位的信息安全保障体系建设、理解和遵守单位的信息安全管理制度、维护组织的信息安全和工作秘密、以及保护个人的信息安全和隐私。

每年对省监测中心网络安全关键岗位人员进行两次专业网络安全培训，，使关键岗位人员及时更新法律法规、管理和技术知识，从而提高省监测中心的信息化网络安全的保障能力、防护水平以及建设水平，确保基础信息网络和重要信息系统的安全稳定运行。

服务频率：3次/年

服务成果：《网络安全培训方案》、《网络安全培训教材》、《网络安全培训总结》

1. **驻场服务**

服务期限内应安排2人进行驻场服务。随着信息系统运行，其自身存在的脆弱性和面临的威胁都在发生变化，安全运维就是在系统运行期间，不断的发现问题和解决问题，并优化安全策略，建立防护、检测和恢复的闭环安全机制，保证业务系统持续安全。通过驻场人员，为省监测中心提供专网络安全监测、策略配置、设备巡检、资产管理同时满足日常安全检查的需求。

服务范围：根据省监测中心所有业务系统的安全情况，安排2位有5年以上安全维护经验的高级技术工程师进行5\*8小时驻场服务。

服务成果：《网络安全工作月报》、《网络安全工作进度报告》、《网络安全工作总结报告》

**四、管理要求**

1. 服务人员

★投标人需承诺投标文件中所列项目经理和驻场服务人员为本项目专用人员，在项目实施期内均需在采购人现场驻场服务，由采购人统一组织考勤，中标人不得在合同签订后更换其他人员进行项目交付；如中标人未经采购人同意更换人员，采购人有权终止合同，并按投标人违约向同级财政部门投诉并追究相关法律责任。

项目经理需具备本科或本科以上毕业证书、信息安全保障人员认证证书-应急服务方向（专业级）、网络工程师（软考）、国家信息安全水平证书（NISP）、云计算安全CCSK证书、注册信息安全工程师(CISP-CISE)。

**驻场工程师1主要承担渗透测试、安全溯源、应急支撑、安全基线检查等工作；**应具备以下证书：（1）工作年限不少于5年，提供本科或本科以上毕业证书（工作年限以提供毕业证书颁发日期计算）；（2）注册信息安全工程师(CISP-CISE)；（3）国家信息安全水平证书（NISP）。

**驻场工程师2主要承担设备巡检、策略配置、安全值守等工作；**应具备以下证书：（1）工作年限不少于5年，提供本科或本科以上毕业证书（工作年限以提供毕业证书颁发日期计算）；（2）注册信息安全专业人员（CISP）。

除项目经理和驻场服务人员外，需提供不少于8人的二线技术支持团队，二线技术支持人员同时具有以下资质：（1）本科或以上学历；（2）信息安全相关的认证证书，满足以下任一安全证书即可：国家信息安全水平证书（NISP）、采用服务工具的认证工程师、信息安全工程师（计算机软考）、注册信息安全专业人员（CISP）。

投标人须承诺，如在项目实际执行过程中发生项目经理或驻场人员不能按采购文件要求胜任相关工作的，采购人有权要求更换项目经理，投标人必须在3天内调整为符合采购文件要求且能胜任相关工作的项目经理并到位开展工作。

1. 进度要求

本项目自合同签订之日起10个工作日完成安全服务方案的编制，具体时间以项目合同约定为准。

1. 组织实施要求

为使项目按质、按量、按时及有序实施，投标人应建立完善、稳定的项目团队、内部组织管理方式及管理机构、协调机制、技术基础，支撑保障要求及其他相关要求。服务工具全部安装完成且连接完毕进行系统测试，应严格按测试计划进行，做好各项原始记录。

1. 文档管理要求

投标人应在项目完成时，将本项目所有文档、资料汇集成册交付给采购人，所有文件要求用中文书写或有完整的中文注释。验收后，投标人按国家、省以及采购人档案管理要求，向采购人提供装订成册的纸质文档至少 1 套，电子文档 1 套。

1. 质量保证要求

为保证本项目能按时高质的顺利完成，规避项目风险或将风险降至最低程度，投标人应建立项目质量管理体系，包括但不限于质量目标、质量指标、岗位责任、问题处理计划、质量评价、整改完善等内容，并建立奖惩制度。

**五、验收标准**

本项目的验收应符合广东省信息化项目相关验收管理办法的要求，同时应遵循下列标准：

1. 实现合同和根据招标文件所编写的投标文件中列举的全部工作内容。

2. 验收项目包括按照合同和根据招标文件所编写的投标文件中所标明的项目实施方案、培训教材和使用说明书等项目文件。

3. 服务期间，中标人应按照合同、招标文件的要求和投标文件的服务承诺提供稳定、可靠、优质的服务，每月提交《项目进度报告》；服务期满后，提交《项目总结报告》。

**六、其他要求**

1. 服务响应要求

本项目服务响应可通过现场、远程等方式提供，由此产生的一切费用均由投标人承担。

1. 服务方式包括：包括但不限于电话服务、远程服务和现场服务等。

2. 系统运行维护：提供7\*24小时响应服务（包括但不限于现场服务、紧急事件响应、系统升级等），出现故障时，快速受理服务请求，根据不同的故障等级在不同时间内进行响应，对于远程或电话无法解决的问题，安排技术人员现场处理，重大故障提供故障分析报告，保证市内2小时内（地市6小时内）到达现场解决重大系统故障。

1. 资产权属
2. 本项目所涉服务成果的知识产权归属处理方式：服务成果的知识产权归采购人所有。

2. 本项目所涉及的数据所有权归采购人所有。

3. 投标人提供的相关软件应是自行开发的产品或具备合法、合规授权，满足知识产权、安全等级保护三级等方面的有关规定和要求。

4. 投标人保证向采购人提供的服务成果是其独立实施完成，不存在任何侵犯第三方专利权、商标权、著作权等合法权益。如因投标人提供的服务成果侵犯任何第三方的合法权益，导致该第三方追究采购人责任的，投标人应负责解决并赔偿因此给采购人造成的全部损失。

1. 保密要求
2. 投标人须签订保密协议，对其因身份、职务、职业或技术关系而知悉的采购人商业秘密和党政机关保密信息应严格保守，保证不被披露或使用，包括意外或过失。
3. 投标人不得以竞争为目的、或出于私利、或为第三人谋利而擅自保存、披露、使用采购人商业秘密和党政机关保密信息；不得直接或间接地向无关人员泄露采购人的商业秘密和党政机关保密信息；不得向不承担保密义务的任何第三人披露采购人的商业秘密和党政机关保密信息。投标人在从事政府项目时，不得擅自记录、复制、拍摄、摘抄、收藏在工作中涉及的保密信息，严禁将涉及政府项目的任何资料、数据透露或以其他方式提供给项目以外的其他方或投标人内部与该项目无关的任何人员。
4. 投标人对于工作期间知悉采购人的商业秘密和党政机关保密信息（包括业务信息在内）或工作过程中接触到的政府机关文件（包括内部发文、各类通知及会议记录等）的内容，同样承担保密责任，严禁将政府机关内部会议、谈话内容泄露给无关人员；不得翻阅与工作无关的文件和资料。
5. 严禁泄露在工作中接触到的政府机关科技研究、发明、装备器材及其技术资料和政府工作信息。
6. ★在项目服务期到期后，服务工具所生产或者承载的数据内容属于采购人所有，中标服务商需在采购人完成数据迁移和清理后方可收回工具，并且采购人有权拆卸工具的存储设备。（投标人提供承诺函，格式自拟）
7. 监理要求

投标人须承诺，在项目开展过程中接受采购人指定的咨询监理机构的监理。

1. 考核要求

1、被信息安全主管部门通报的，1次扣3分；

2、甲方信息系统出现安全故障，乙方未能及时协助处理的，1次扣2分；

3、未按要求进行安全通告与咨询服务的，1次扣1分；

5、考核得分在98分或以上时，视为合格，低于98分时视为不合格。考核得分低于98分时，每差1分扣除合同总额的1%，惩罚金总额不超过合同总金额的30％。

###### （六）廉洁承诺

###### 投标人在投标时需签订《廉洁承诺书》（格式附后）。

**七、付款方式**

（一）本项目计划分 3 期支付，具体支付方式和时间如下：

**首期款：**支付比例60%，签订合同后5个工作日内，中标人书面提出支付申请函及拟支付金额等额的符合采购人财务管理要求的相应发票，采购人确认后启动首期款支付流程，占合同总金额的60%。

**进度款：**支付比例30%，服务满3个月后，在采购人和监理方对中标人提交相应进度的服务报告审核通过后，中标人书面提出支付申请函及拟支付金额等额的符合采购人财务管理要求的相应发票，支付申请函和拟支付金额等额的符合采购人财务管理要求的相应发票，采购人确认后启动支付流程，占合同总金额的30%。

**尾款：**支付比例10%，项目通过专家验收后15个工作日内，中标人书面提出支付申请函及拟支付金额等额的符合采购人财务管理要求的相应发票，采购人确认后启动支付流程，占合同总金额的10%。

（二）履约保证金要求

1、中标人在收到第一笔款后，须在20个工作日内向采购人提供项目中标价的5%保证金。完成项目服务工作并通过采购人组织的验收，采购人在完成验收后20个工作日内无息退还保证金。

2、中标人未按约提交保证金的，无权要求采购人支付后续款项。因中标人违约引起的采购人逾期付款，采购人无需承担违约责任。

3、采购人有权直接从保证金内扣除违约金、赔偿金、考核不合格应扣减的服务费等。