省生态环境监测中心政务信息化运维运营（2025年）项目网络安全运营服务项目

采购需求

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（2025 年）项目网络安全运营服务

（二）项目预算

本项目预算最高限价为人民币 278 万元（以实际批复文件为准）。

（三）服务时间

共 12 个月，以合同签订后实际开始服务时间为准。

（四）服务范围

1. 省生态环境监测中心本部;

2. 驻市站：珠海、佛山、韶关、河源、梅州、惠州、中山、江门、阳江、茂名、潮州。

3. 具体的服务内容以实际文件批复为准。

（五）服务地点

由采购人指定。

（六）项目目标

为省生态环境监测中心（以下简称省中心本部）及 11 个驻市站信息化系统提供专业的网络安全运营服务，保障政务网络及业务系统的稳定性、可靠性、安全性，确保应用系统的可用性、业务连续性，为省中心本部及相关驻市站营造一个健康、有序的信息化办公环境，充分发挥信息化技术对省中心本部及相关驻市站业务开展的服务作用、支持作用、规范作用和促进作用。

通过本项目的建设，预期达成关键目标：一是进一步完善和提升省中心本部信息化系统的服务质量，保障省中心本部信息系统的正常

运行，确保在有效工作时间内正常运行。通过本项目加强系统运营能力和网络安全服务，提高系统用户的使用体验和支持力度，提高用户日常工作的效率，提升省中心整体网络安全能力。二是帮助省中心本部及相关驻市站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，保障省中心本部及相关驻市站的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、服务内容

（一）省中心本部网络安全运营服务

主要内容包括：安全风险评估、漏洞扫描、应用安全渗透测试、应用安全监测、云防护、第三方安全审计、日志审计服务、网络安全事故处置、数据安全与备份、蜜罐、安全基线核查、特殊时期安全保障、安全应急演练支撑、协助完善和落实安全制度、安全培训与安全宣传、人员安全运维、内部红蓝队攻击推演、国家护网和粤盾攻防演练值守等 18 项服务。具体服务要求见附件 1。

（二）驻市站网络安全运营服务

包括珠海、佛山、韶关、河源、梅州、惠州、中山、江门、阳江、茂名、潮州 11 个驻市站共 81 项服务。具体服务要求见附件 2。

珠海站：漏洞扫描、网络安全事故处置、重大节日（活动）时期安全保障、国家护网和粤盾攻防演练值守、网络安全态势评估等 5 项服务。

佛山站：漏洞扫描、网络安全事故处置、安全应急演练支撑、安全制度完善、终端防病毒、上网行为规范和效率分析、网络边界访问控制、网络安全态势评估、国产操作系统及国产应用软件安全评估、

驻场等 10 项服务。

韶关站：网络安全事故处置、安全应急演练支撑、安全制度完善、终端防病毒、上网行为规范和效率分析、网络边界访问控制、网络安全态势评估等 7 项服务。

河源站：漏洞扫描、网络安全事故处置、安全应急演练支撑、安全制度完善、终端防病毒、安全加固、驻场等 7 项服务。

梅州站：漏洞扫描、网络安全事故处置、重大节日（活动）时期安全保障、安全应急演练支撑、安全制度完善、国家护网和粤盾攻防演练值守、服务器安全性维护、专项安全预警加固整改、安全加固等 9 项服务。

惠州站：漏洞扫描、网络安全事故处置、安全应急演练支撑、安全制度完善、终端防病毒、上网行为规范和效率分析、网络边界访问控制、驻场等 8 项服务。

中山站：漏洞扫描、网络安全事故处置、安全应急演练支撑、安全制度完善、终端防病毒、上网行为规范和效率分析、网络边界访问控制、网络安全态势评估、驻场等 9 项服务。

江门站：网络安全事故处置、安全应急演练支撑、安全制度完善、终端防病毒、上网行为规范和效率分析、网络边界访问控制、网络安全态势评估、驻场等 8 项服务。

阳江站：漏洞扫描、网络安全事故处置、安全应急演练支撑、安全制度完善、终端防病毒、驻场等 6 项服务。

茂名站：漏洞扫描、网络安全事故处置、安全应急演练支撑、安全制度完善、终端防病毒、网络边界访问控制、网络安全态势评估、驻场等 8 项服务。

潮州站：网络安全事故处置、重大节日（活动）时期安全保障、

安全应急演练支撑、安全制度完善等 4 项服务。

三、项目实施要求

（一）项目组织管理

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。在机制保障方面，成立组织实施小组和项目专家组的双轨制的组织模式。在项目日常管理和条件保障方面，从行政组织、后勤保障和支撑条件各方面创造良好的服务环境，确保项目的顺利实施。

（二）服务人员

投标人须书面承诺，如在项目实际执行过程中，项目经理、驻场服务工程师及二线技术支持工程等任意一类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相关人员，投标人需在两周内调整符合采购文件要求且能胜任相关工作的项目人员到位开展工作，否则采购人有权终止合同并追究投标人相关责任。

中标人在项目实施过程中如出现资源、进度、质量协调控制不力的情况，采购人有权要求更换相关项目人员，中标人必须予以配合，并确保不影响项目建设的进度和质量。

投标人必须向采购人保证项目人员的稳定性，在本项目结束前，项目人员的变动必须取得采购人同意。

投标人承诺的项目经理和开发实施的主要人员未经用户同意不得调整；投标人如中途更换项目经理和主要开发技术人员，应征得用

户同意，否则采购人有权终止合同。

服务商应指派专业团队为本项目提供专业服务，服务团队成员不得少于15人。项目经理应具备5年以上项目管理经验。

如需调整服务团队成员，须书面向采购人提出申请，说明申请理由，经采购人书面同意后方可调整团队人员，调入人员的资历和从业经验不低于调出人员，否则视为违约行为，采购人有权终止服务合同。

应提供以上人员相关证明资料复印件并加盖公章，并提供以上人员在本公司任职的有效外部证明材料（如加盖政府有关部门印章的《投保单》或《社会保险参保人员证明》，或单位代缴个人所得税税单等，事业法人的相关人员应提供该单位的相关证明）复印件。

（三）项目进度要求

1. 项目交接：中标人需与现服务单位做好项目交接工作，保证项目连续不中断，有序开展新项目实施。

2. 工期要求：中标人必须在合同约定的12个月服务期内完成所有服务内容，服务到期前2个月按照广东省政务服务和数据管理局（以下称省政数局）要求提交《项目验收前符合性自查表》及相关材料，通过符合性审查后，采购人组织专家开展项目终验。

3. 工作方式：投标人需明确招标项目工作的方式、方法、过程步骤、按阶段分解的详细计划、对应计划应提交的工作成果、需要采购人协调与配合的事项，并经采购人审核、批准。

4. 监督管理：采购人有权监督和管理项目的服务进度、质量、验收等各项工作，中标人必须接受并服从采购人的监督、管理要求，无

条件提供中间过程工作成果。

（四）质量要求

1．在本项目服务期限内，中标人负责采购人本地私有云设备、网络基础设备、系统平台的安全保障，并协助采购人保障政务云系统平台的网络安全。

2．中标人要求根据 ISO9000、CMMI 及项目管理成熟度模型，结合本项目的实际情况，编制详细的质量控制计划。

3．中标人必须接受采购人的质量监督检查，提供真实有效的相关质量活动记录、证据，无条件接受采购人提出的质量问题整改要求，承担质量责任及因质量问题导致的进度延迟责任。

4．投标人必须在投标文件中提出质量控制和保证机制。

（五）文档管理

1．文档管理依据省政数局发布的《政务信息化验收规范》等要求提交相应的过程及成果文档。

2．本项目所有的技术文件必须用中文书写或有完整的中文翻译。中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。验收后，中标人按国家、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。

（六）服务成果要求

1．项目成果的内容应符合本项目的有关要求，并按程序完成相关工作。采购人按省政数局及采购人内部的项目验收管理办法进行验收，必要时邀请相关的专业人员或机构参与验收;

2. 满足《广东省省级政务信息化项目验收前符合性审核细则》要求，通过采购人组织的验收，质量达到合格标准。

（七）验收要求

项目验收需符合《广东省省级政务信息化项目管理办法》《政务信息化验收规范》的要求，同时需符合下列要求:

1. 满足合同和招标文件中列举的全部要求。

2. 实现合同和招标文件中列举的全部功能和非功能要求。

3. 达到合同和招标文件中列举的全部指标。

4. 文档齐全，符合合同和招标文件及相关标准要求，包括但不限于下列文档: 项目实施方案、服务计划、质量管理计划、周报（如有）、月报、阶段性总结报告、年度总结报告、项目各类会议纪要、项目各项服务成果物及省政数局项目验收管理办法所要求的全部文档。

（八）服务时间要求

1. 人员考核: 按采购人《信息化服务外包人员管理规定》《考勤管理制度》等规定，项目驻场人员与采购人工作时间保持一致，日常上班时间为每周一至周五，上午 8:30-12:00，下午 2:00-5:30，遇法定节假日的按国家规定执行。其余参与人员按实际情况进行考核。

2. 应急工作时间: 在重大节日（活动）或其他应急值班节点期间，项目人员应按采购人实际要求，开展应急值班值守服务，通过线上和线下相结合的方式，实行 7×12 小时或 7×24 小时工作制，具体以实际工作为准。

四、知识产权要求

1. 本项目涉及的所有资料(包括但不限于采购人的需求资料和中标人递交的技术要求、设计、图纸等所有资料）及建设完成品均被视为依照采购人的委托要求而创作，并均于其完成时视同自动使采购人拥有服务内容的全部知识产权、商业秘密和其他相关权利，中标人或任何第三方不得对此主张任何权利或提出赔偿要求。

2. 本项目所涉及的数据所有权归采购人所有。中标人只能用于履行本合同之义务。

3. 中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、安全等保等方面的有关规定和要求。

4. 中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。如因中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，中标人应负责解决并赔偿因此给采购人造成的全部损失。

5. 项目完成终验后，中标人在 20 个工作日内向采购人移交所有约定项目服务材料。

五、违约责任与赔偿损失

1. 中标人提供的服务不符合本合同规定的，采购人有权要求中标人在合同规定期限内交付满足合同要求的服务。

2. 中标人提供的服务不符合招标文件、响应文件或本合同规定的，中标人应进行整改，整改两次后仍不合格的，采购人有权拒收，并且中标人须向采购人支付本合同总价 5%的违约金。采购人无正当

理由拒绝接受服务，到期拒付服务款项的，采购人向中标人偿付本合同总价的 5%的违约金。

3. 如中标人未能按本合同规定的时间履行义务，包括但不限于逾期提供服务或服务成果（无论是阶段性服务成果还是最终服务成果）等，从逾期之日起，每日应按本合同总价万分之四的数额向采购人支付违约金。逾期半个月以上的（含本数），采购人有权单方解除本合同，余款不再支付，已经支付的相应款项中标人应当在收到解除通知之日起三日内予以退还，且采购人有权要求中标人按本合同总价的 20%支付违约金。

4. 中标人违反本合同约定的保密义务的，采购人有权单方解除本合同，中标人因此获得的利益应当全部归采购人所有，并且中标人还应向采购人支付本合同总价的 20%的违约金、赔偿采购人因此产生的损失（包括但不限于：采购人的经济损失；采购人因此支付的赔偿金、补偿金、罚金；采购人因维权、制止或减少损失所支付的律师费、诉讼费、调查取证费等费用）。

5. 其他违约责任按《中华人民共和国民法典》处理。

六、保密要求

1. 中标人和采购人在签订合同时应签订保密协议，对中标人的相关人员因身份、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。

2. 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。

3. 项目实施过程中至中标人正式向采购人交付技术文档资料时止，中标人必须采取措施对本项目实施过程中的数据、源代码、技术文档等资料保密，否则，由于中标人过错导致的上述资料泄密的，中标人必须承担一切责任。

4. 中标人需对在项目过程中所获取的采购人信息、文件、资料及考生、考试信息（如有）承担保密责任。

5. 合同终止后，中标人应将保密信息退还采购人或根据采购人要求予以删除或销毁，不得擅自留存。中标人或中标人人员违反保密义务的，中标人应妥善处理纠纷并承担赔偿责任（包括但不限于赔偿采购人因此支出的赔偿金/和解款、诉讼费、律师费等）。

本条约定的保密条款单独有效，不因本合同其他条款的到期或失效而无效；保密义务为长期，直至相关技术、信息或文件被依法公开为止。

七、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。

八、付款方式

采购人按以下程序，分 3 期支付服务费:

1. 首付款：支付比例 60%，项目合同签订后 15 个工作日内，中标人书面提出支付申请，并提供相应支付金额发票（符合采购人财务管理要求）及其他申请资料，采购人确认后 15 个工作日内支付合同总金额的 60%。

2. 进度款：支付比例 30%，服务满 6 个月后，监理方对中标人提交的相应进度服务报告进行审核，审核结果经采购人确认后，中标人书面提出支付申请，并提供相应支付金额发票（符合采购人财务管理要求）及其他申请资料，采购人确认后 15 个工作日内支付合同总金额的 30%。

3. 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，并提供相应支付金额发票（符合采购人财务管理要求）及其他申请资料，采购人确认后 15 个工作日内支付合同总金额的 10%。

4. 关于付款的特别约定: 中标人逾期交付付款申请资料或所交付的付款申请资料不符合约定的，采购人有权延期支付相应费用并不视为违约。采购人在约定的付款时间内办理支付手续即视为采购人办理完毕付款。如因政府财政部门审查、财政支付管理流程及预算下达等原因导致支付延期的，支付期限自动顺延，不视为采购人违约，采购人不承担责任，中标人不得以此为由迟延履行或不履行合同义务。

九、采购方式

拟采用公开招标采购方式。

十、附件

1. 省中心本部网络安全运营服务要求

2. 驻市站网络安全运营服务要求

附件 1

省中心本部网络安全运营服务要求

序号	服务内容	服务要求	服务频率
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;	1 次/半年
		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。	
		服务成果：《信息安全综合评估报告》《信息资产清单》	
2	漏洞扫描服务	针对服务对象定期（每个月一次）进行全面漏洞扫描（包括主机、操作系统、应用、设备等），并提供漏洞扫描报告。	1 次/月
		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、远程登录和远程服务等。	
		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。	
		服务成果：《漏洞扫描报告》	
3	应用安全渗透测试服务	对服务对象进行 1 次/2 个月的安全渗透测试，并形成系统渗透测试报告。	1 次/2 个月
		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) 增强安全意识: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。	
		服务成果：应用安全渗透测试报告	
4	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。	1 次/季度

序号	服务内容	服务要求	服务频率
		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。	
		服务成果：应用安全监测报告	
5	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。	2 个域名/1 年
		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。	
		云防护产品提供 6 个域名，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。	
		服务成果：云防护报告	
6	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。	1 次/半年
		服务成果：网络安全第三方审计报告	
7	日志审计服务	本次日志审计服务针对省监测中心的所有应用系统进行日志收集审计工作。	1 次/半年
		通过日志采集、日志分析、告警展示、日志检索、日志数据	

序号	服务内容	服务要求	服务频率
		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发生原因的定位。	
		服务成果：日志审计报告	
8	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。	6 次/年
		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的识别、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。	
		服务成果：网络安全处置预案、网络安全总结报告、异常检测工作总结报告、网络安全事故处置培训报告	
9	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。	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	
10	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，能够使省监测中心各系统了解目前所面对的安全威胁，帮助省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。	1 次/季度
		服务成果：蜜罐服务报告（每季度 1 份）	
11	安全基线核查服务	依据安全基线合规配置要求，对水务局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	1 次/季度

序号	服务内容	服务要求	服务频率
		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。	
		服务时间：服务期内每半年提供一次安全配置核查服务；	
		服务成果：向用户提交《安全配置核查报告》。	
12	特殊时期安全保障	提供在特殊时期内的网站安全保障服务，特殊时期指国家重大事件发生时期，如两会、国庆等重要时期。特殊时期提供监控服务，频度为每天 3 次，安全状况报告为每天 1 次。	1 次/季度
		服务成果：《重保时期安全服务报告》	
13	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，进行一年一次的不超过 4 个场景（不同地方对应不同的场景）的安全应急演练支撑服务，形成安全应急预案、应急演练脚本、应急演练报告，并进行安全意识培训。	1 次/年
		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，确保在网络安全事件发生时，省监测中心的应急工作能快速、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，主要包括：	
		1）应急体系建立：构建应急组织机构，完善应急制度；	
		2）应急预案完善：梳理应急机制和监测预警系统，完善应急方案；	
		3）应急实战演练：编制应急演练方案，开展演练活动，检测校验应急体系。	
		服务范围：为省生态环境监测中心的信息系统，通过不同地方的不同安全应急演练场景提供安全应急演练支撑服务。	
		服务成果：《安全应急预案》《应急演练脚本》《应急演练工作报告》《安全意识培训》	
14	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。	1 年
		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	

序号	服务内容	服务要求	服务频率
		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》	
15	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。	3 次/年
		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》	
16	人员安全运维服务	主要涉及两方面，对内部人员的安全管理和对外部人员的安全管理。具体包括其他运维人员离岗、安全意识教育和外部人员访问管理以及相应人员的授权管理。 频率：项目每天一次，伴随整个项目周期。 服务成果：《人员情况登记表和运维账号管理情况表》。	1 次/周
17	内部红蓝队攻击推演服务	提供红队攻击，蓝队防守服务，其中红队信息收集需 8 人天，纵向攻击建立据点需 10 人天，横向拓展需 10 人天，拿下目标 5 人天。蓝队安全加固 10 人天，安全设备有效性校验 5 人天，攻击发现 5 人天，策略优化 5 人天，输出报告 2 人天，共计 60 人天。约 3 人月（60/21.75）。	3 人月
18	国家护网和粤盾攻防演练值守服务	国家护网和粤盾攻防演练周期一般为 15 天，需提供 7*24 小时服务（24 小时为 3 人天），因此监控值守服务 45 人天（3 人天*15 天），分析研判 30 人天（2 人天*15 天），应急溯源 30 人天（2 人天*15 天），共计 105 人天。约 6 人月（135/21.75）。	4.8 人月

附件 2

驻市站网络安全运营服务要求

序号	驻市站	服务内容	服务要求	服务频率
1	潮州	网络安全事故处置	对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，立即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。	2 次/年
2		重大节日(活动)时期安全保障	提供在特殊时期内的网站安全保障服务，特殊时期指国家重大事件发生时期，如两会、国庆等重要时期。特殊时期提供监控服务，频度为每天 3 次，安全状况报告为每天 1 次。	1 次/季度
3		安全应急演练支撑服务	按照网络安全监管需求，进行一年一次的不超过 4 个场景（不同地方对应不同的场景）的安全应急演练支撑服务，形成安全应急预案、应急演练脚本、应急演练报告，并进行安全意识培训。	1 次/半年
4		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制度。	1 次/年
5	佛山	漏洞扫描服务	针对服务对象定期进行全面漏洞扫描（包括主机、操作系统、应用、设备等），并提供漏洞扫描报告。	1 次/月
6		网络安全事故处置	对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，立即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。	1 次/年
7		安全应急演练支撑服务	按照网络安全监管需求，进行一年一次的不超过 4 个场景（不同地方对应不同的场景）的安全应急演练支撑服务，形成安全应急预案、应急演练脚本、应急演练报告，并进行安全意识培训。	1 次/半年
8		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制度。	1 次/年
9		驻场服务	服务期限内应安排人员进行驻场服务。通过驻场人员，提供设备巡检、资产管理服务。	1 人/年
10		终端防病毒服务	对终端提供防病毒软件和病毒库更新服务，导出防病毒安全检查报告、对有风险和中毒的文件与数据进行检查；定期检测病毒，防止病毒对系统的影响。	120 台计算机
11		上网行为规范和效率分析服务	通过专业设备，对局单位网络使用情况输出相关成果，并能对上班时间视频、游戏、购物、股票等影响工作效率的业务进行限制，并按月提供网络运行情报报表，规范内网用户行为。	1 次/月
12		网络边界访问控制服务	通过专业设备，对网络出口进行访问控制，并记录相关访问日志不少于 180 天要求，实现对网络出口的管控，并按月生成网络使用日志报表。	1 次/月
13		网络安全态势评估服务	通过专业设备，对单位网络安全态势输出相关成果，包含流量态势、僵木蠕态势、网站安全态势、入侵态势。	1 次/月
14		国产操作系统及国产应用软件安全	对非 windows 的国产操作系统以及应用软件进行安全评估，提出风险预警、加固的可行性方法	1 次/月

序号	驻市站	服务内容	服务要求	服务频率
		评估		
15	河源	漏洞扫描服务	针对服务对象定期进行全面漏洞扫描（包括主机、操作系统、应用、设备等），并提供漏洞扫描报告。	1 次/月
16		网络安全事故处置	对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，立即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。	1 次/半年
17		安全应急演练支撑服务	按照网络安全监管需求，进行一年一次的不超过 4 个场景（不同地方对应不同的场景）的安全应急演练支撑服务，形成安全应急预案、应急演练脚本、应急演练报告，并进行安全意识培训。	1 次/半年
18		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制度。	1 次/年
19		驻场服务	服务期限内应安排人员进行驻场服务。通过驻场人员，提供设备巡检、资产管理服务。	1 人/年
20		终端防病毒服务	对终端提供防病毒软件和病毒库更新服务，导出防病毒安全检查报告、对有风险和中毒的文件与数据进行检查；定期检测病毒，防止病毒对系统的影响。	40 台内网电脑
21		安全加固服务	每次扫描检查及本地检查后，对项目范围的服务器、终端、网络设备、安全设备、常用业务系统等重要系统进行安全加固和优化。	1 次/月
22	惠州	漏洞扫描服务	针对服务对象定期进行全面漏洞扫描（包括主机、操作系统、应用、设备等），并提供漏洞扫描报告。	1 次/季度
23		网络安全事故处置	对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，立即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。	1 次/年
24		安全应急演练支撑服务	按照网络安全监管需求，进行一年一次的不超过 4 个场景（不同地方对应不同的场景）的安全应急演练支撑服务，形成安全应急预案、应急演练脚本、应急演练报告，并进行安全意识培训。	1 次/半年
25		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制度。	1 次/年
26		驻场服务	服务期限内应安排人员进行驻场服务。通过驻场人员，提供设备巡检、资产管理服务。	1 人/年
27		终端防病毒服务	对终端提供防病毒软件和病毒库更新服务，导出防病毒安全检查报告、对有风险和中毒的文件与数据进行检查；定期检测病毒，防止病毒对系统的影响。	150 台内网电脑
28		上网行为规范和效率分析服务	通过专业设备，对局单位网络使用情况输出相关成果，并能对上班时间视频、游戏、购物、股票等影响工作效率的业务进行限制，并按月提供网络运行情报报表，规范内网用户行为。	1 次/年
29		网络边界访问控制服务	通过专业设备，对网络出口进行访问控制，并记录相关访问日志不少于 180 天要求，实现对网络出口的管控，并按月生成网络使用日志报表。	1 次/年
30	江门	网络安全事故处置	对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，立即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。	1 次/年

序号	驻市站	服务内容	服务要求	服务频率
31		安全应急演练支撑服务	按照网络安全监管需求，进行一年一次的不超过 4 个场景（不同地方对应不同的场景）的安全应急演练支撑服务，形成安全应急预案、应急演练脚本、应急演练报告，并进行安全意识培训。	1 次/半年
32		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制度。	1 次/年
33		驻场服务	服务期限内应安排人员进行驻场服务。通过驻场人员，提供设备巡检、资产管理服务。	1 人/年
34		终端防病毒服务	对终端提供防病毒软件和病毒库更新服务，导出防病毒安全检查报告、对有风险和中毒的文件与数据进行检查；定期检测病毒，防止病毒对系统的影响。	80 台
35		上网行为规范和效率分析服务	通过专业设备，对局单位网络使用情况输出相关成果，并能对上班时间视频、游戏、购物、股票等影响工作效率的业务进行限制，并按月提供网络运行情报报表，规范内网用户行为。	1 次/年
36		网络边界访问控制服务	通过专业设备，对网络出口进行访问控制，并记录相关访问日志不少于 180 天要求，实现对网络出口的管控，并按月生成网络使用日志报表。	1 次/年
37		网络安全态势评估服务	通过专业设备，对单位网络安全态势输出相关成果，包含流量态势、僵木蠕态势、网站安全态势、入侵态势。	1 次/年
38	茂名	漏洞扫描服务	针对服务对象定期进行全面漏洞扫描（包括主机、操作系统、应用、设备等），并提供漏洞扫描报告。	1 次/季度
39		网络安全事故处置	对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，立即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。	1 次/年
40		安全应急演练支撑服务	按照网络安全监管需求，进行一年一次的不超过 4 个场景（不同地方对应不同的场景）的安全应急演练支撑服务，形成安全应急预案、应急演练脚本、应急演练报告，并进行安全意识培训。	1 次/半年
41		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制度。	1 次/年
42		驻场服务	服务期限内应安排人员进行驻场服务。通过驻场人员，提供设备巡检、资产管理服务。	1 人/年
43		终端防病毒服务	对终端提供防病毒软件和病毒库更新服务，导出防病毒安全检查报告、对有风险和中毒的文件与数据进行检查；定期检测病毒，防止病毒对系统的影响。	1 次/月
44		网络边界访问控制服务	通过专业设备，对网络出口进行访问控制，并记录相关访问日志不少于 180 天要求，实现对网络出口的管控，并按月生成网络使用日志报表。	1 次/月
45		网络安全态势评估服务	通过专业设备，对单位网络安全态势输出相关成果，包含流量态势、僵木蠕态势、网站安全态势、入侵态势。	1 次/月
46	韶关	网络安全事故处置	对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，立即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。	1 次/年
47		安全应急演	按照网络安全监管需求，进行一年一次的不超过 4 个场景（不同	1 次/半年

序号	驻市站	服务内容	服务要求	服务频率
		练支撑服务	地方对应不同的场景）的安全应急演练支撑服务，形成安全应急预案、应急演练脚本、应急演练报告，并进行安全意识培训。	
48		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制度。	1 次/年
49		终端防病毒服务	对终端提供防病毒软件和病毒库更新服务，导出防病毒安全检查报告、对有风险和中毒的文件与数据进行检查；定期检测病毒，防止病毒对系统的影响。	100 台内网电脑
50		上网行为规范和效率分析服务	通过专业设备，对局单位网络使用情况输出相关成果，并能对上班时间视频、游戏、购物、股票等影响工作效率的业务进行限制，并按月提供网络运行情报报表，规范内网用户行为。	1 次/月
51		网络边界访问控制服务	通过专业设备，对网络出口进行访问控制，并记录相关访问日志不少于 180 天要求，实现对网络出口的管控，并按月生成网络使用日志报表。	1 次/月
52		网络安全态势评估服务	通过专业设备，对单位网络安全态势输出相关成果，包含流量态势、僵木蠕态势、网站安全态势、入侵态势。	1 次/月
53	阳江	漏洞扫描服务	针对服务对象定期进行全面漏洞扫描（包括主机、操作系统、应用、设备等），并提供漏洞扫描报告。	1 次/季度
54		网络安全事故处置	对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，立即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。	1 次/年
55		安全应急演练支撑服务	按照网络安全监管需求，进行一年一次的不超过 4 个场景（不同地方对应不同的场景）的安全应急演练支撑服务，形成安全应急预案、应急演练脚本、应急演练报告，并进行安全意识培训。	1 次/半年
56		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制度。	1 次/年
57		驻场服务	服务期限内应安排人员进行驻场服务。通过驻场人员，提供设备巡检、资产管理服务。	1 人/年
58		终端防病毒服务	对终端提供防病毒软件和病毒库更新服务，导出防病毒安全检查报告、对有风险和中毒的文件与数据进行检查；定期检测病毒，防止病毒对系统的影响。	51 台
59	中山	漏洞扫描服务	针对服务对象定期进行全面漏洞扫描（包括主机、操作系统、应用、设备等），并提供漏洞扫描报告。	1 次/半年
60		网络安全事故处置	对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，立即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。	按需服务 1 次/年
61		安全应急演练支撑服务	按照网络安全监管需求，进行一年一次的不超过 4 个场景（不同地方对应不同的场景）的安全应急演练支撑服务，形成安全应急预案、应急演练脚本、应急演练报告，并进行安全意识培训。	1 次/半年
62		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制度。	1 次/年
63		驻场服务	服务期限内应安排人员进行驻场服务。通过驻场人员，提供设备巡检、资产管理服务。	1 人/年

序号	驻市站	服务内容	服务要求	服务频率
64		终端防病毒服务	对终端提供防病毒软件和病毒库更新服务，导出防病毒安全检查报告、对有风险和中毒的文件与数据进行检查；定期检测病毒，防止病毒对系统的影响。	252 台办公电脑
65		上网行为规范和效率分析服务	通过专业设备，对局单位网络使用情况输出相关成果，并能对上班时间视频、游戏、购物、股票等影响工作效率的业务进行限制，并按月提供网络运行情报报表，规范内网用户行为。	1 次/月
66		网络边界访问控制服务	通过专业设备，对网络出口进行访问控制，并记录相关访问日志不少于 180 天要求，实现对网络出口的管控，并按月生成网络使用日志报表。	1 次/月
67		网络安全态势评估服务	通过专业设备，对单位网络安全态势输出相关成果，包含流量态势、僵木蠕态势、网站安全态势、入侵态势。	1 次/月
68	珠海	漏洞扫描服务	针对服务对象定期进行全面漏洞扫描（包括主机、操作系统、应用、设备等），并提供漏洞扫描报告。	1 次/季度
69		网络安全事故处置	对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，立即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。	1 次/年
70		重大节日(活动)时期安全保障	提供在特殊时期内的网站安全保障服务，特殊时期指国家重大事件发生时期，如两会、国庆等重要时期。特殊时期提供监控服务，频度为每天 3 次，安全状况报告为每天 1 次。	1 次/季度
71		国家护网和粤盾攻防演练值守服务	国家护网和粤盾攻防演练周期一般为 15 天，提供安全值守服务。	1 次/年
72		网络安全态势评估服务	通过专业设备，对单位网络安全态势输出相关成果，包含流量态势、僵木蠕态势、网站安全态势、入侵态势。	1 次/月
73	梅州	漏洞扫描服务	针对服务对象定期进行全面漏洞扫描（包括主机、操作系统、应用、设备等），并提供漏洞扫描报告。	1 次/季度
74		网络安全事故处置	对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，立即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。	根据实际事故时间确定
75		重大节日(活动)时期安全保障	提供在特殊时期内的网站安全保障服务，特殊时期指国家重大事件发生时期，如两会、国庆等重要时期。特殊时期提供监控服务，频度为每天 3 次，安全状况报告为每天 1 次。	1 次/年
76		安全应急演练支撑服务	按照网络安全监管需求，进行一年一次的不超过 4 个场景（不同地方对应不同的场景）的安全应急演练支撑服务，形成安全应急预案、应急演练脚本、应急演练报告，并进行安全意识培训。	1 次/半年
77		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制度。	1 次/年
78		国家护网和粤盾攻防演练值守服务	国家护网和粤盾攻防演练周期一般为 15 天，提供安全值守服务。	1 次/年
79		服务器安全性维护	检查加固服务器设置，审核升级补丁，修复漏洞。	1 次/每月

序号	驻市站	服务内容	服务要求	服务频率
80		专项安全预警加固整改服务	安全主管部门通报处置：各级信息安全测评中心安全预警和漏洞通报的自查、修复工作，每月按相关通报文件对单位资产开展对应全面检查，含技术自查、技术整改、文档编制等，并协助与检查方的技术沟通工作。并提交相关报告。	根据实际通报情况确定
81		安全加固服务	每次扫描检查及本地检查后，对项目范围的服务器、终端、网络设备、安全设备、常用业务系统等重要系统进行安全加固和优化。	1 次/季度