合同编号：JSGXS2500010CGN00

江苏省水利互联网安全保障服务（2025 年）合同

委托方（甲方）：江苏省水利厅

住　所　地：江苏省南京市鼓楼区上海路 5 号水利大厦

委托代拟人：

项目联系人：陆明

联系方式

通 讯 地 址：江苏省南京市鼓楼区上海路 5 号水利大厦

电　　话：025-86338123　　传　真：

电 子 信 箱：jsslwxb@163.com

受托方（乙方）：江苏省公用信息有限公司

住　所　地：南京市建邺区江东中路 49 号河西电信大厦

法定代表人：许敏

项目联系人：王默润

联系方式

通 讯 地 址：南京市建邺区江东中路 49 号河西电信大厦

电　　话：18051998858　　传　真：025-86788158

电 子 信 箱：wangmr@chinatelecom.cn

本合同甲方委托乙方 江苏省公用信息有限公司 提供专项技术服务，并支付相应的技术服务报酬。双方经过平等协商，在真实、充分地表达各自意愿的基础上，根据《中华人民共和国合同法》的规定，达成如下协议，并由双方共同恪守。

第一条　甲方委托乙方进行技术服务的内容如下：

1．技术服务的目标和内容：详见附件 1。

2．技术服务的方式：详见附件 1。

第二条　乙方应按下列要求完成技术服务工作：

1．技术服务地点：江苏省南京市鼓楼区上海路 5 号江苏省水利厅。

王默润

2．技术服务期限：合同签订之日起至 2025 年 12 月 31 日。

3．技术服务进度：详见附件 1。

4．技术服务质量要求：详见附件1。

5．技术服务质量期限要求：详见附件 1。

第三条　为保证乙方有效进行技术服务工作，甲方应向乙方提供下列工作条件和协作事项：

1．提供技术资料：

（1）详见附件 1；

（2）详见附件 1；

（3）详见附件 1。

2．提供工作条件：

（1）必要的工作衔接。

3．其他：无。

4．甲方提供上述工作条件和协作事项的时间及方式：必要时。

第四条　甲方向乙方支付技术服务报酬及支付方式为：

1．技术服务费总额为：（大写）壹佰叁拾贰万贰仟伍佰圆（1322500 元）人民币（包干使用）；

2．技术服务费由甲方分期支付乙方。具体支付方式和时间如下：

合同生效后 7 天内，甲方向乙方支付合同额的 30%；开展攻防演练并提供合格成果后 10 日内，经甲方审核后向乙方支付合同额的 50%；合同履行完成并通过甲方验收后 10 日内，甲方向乙方支付合同额的 20%。

乙方开户银行名称、地址和账号为：

开户银行：中国工商银行南京察哈尔路支行

地　　址：江苏省南京市鼓楼区铁路北街 128 号财大科技园 B 座

帐　　号：4301011209100132640

第五条　双方确定因履行本合同应遵守的保密义务如下：

甲方：

1．保密内容（包括技术信息和经营信息）：详见附件 2。

2．涉密人员范围：详见附件 2。

3．保密期限：详见附件 2。

4．泄密责任：详见附件 2。

乙方：

1．保密内容（包括技术信息和经营信息）：详见附件 2。

2．涉密人员范围：详见附件 2。

3．保密期限：详见附件 2。

4．泄密责任：详见附件 2。

第六条　本合同的变更必须由双方协商一致，并以书面形式确定。但有下列情形之一的，一方可以向另一方提出变更合同权利与义务的请求，另一方应当在 30 日内予以答复；逾期未予答复的，视为同意。

第七条　双方确定以下标准及方法对乙方的技术服务工作成果进行验收：

1．乙方完成技术服务工作的形式：详见附件 1。

2．技术服务工作成果的验收标准：详见附件 1。

3．技术服务工作成果的验收方法：详见附件 1。

4．项目科技成果的验收方法：详见附件 1。

5．验收的时间和地点：根据工作进度安排。

第八条　双方确定：

1．在本合同有效期内，甲方利用乙方提交的技术服务工作成果所完成的新的技术成果，归 甲 方所有。

2．在本合同有效期内，乙方利用甲方提供的技术资料和工作条件所完成的新的技术成果，归 甲 方所有。

第九条　双方确定，按以下约定承担各自的违约责任：

1．乙 方违反本合同第 二 条约定，应当 视情况支付合同总价的 30%以上至 100%的违约金 (支付违约金或损失赔偿额的计算方法)。**(因甲方原因除外)**

2．甲 方违反本合同第 三 条约定，应当 视情况支付合同总价的 10%以上至 50%的违约金 (支付违约金或损失赔偿额的计算方法)。

第十条　双方确定，在本合同有效期内，甲方指定 陆明 为甲方项目联系人，乙方指定 王默润 为乙方项目联系人。项目联系人承担以下责任：

1．日常联络。

一方变更项目联系人的，应当及时以书面形式通知另一方。未及时通知并影响本合同履行或造成损失的，应承担相应的责任。

第十一条　双方确定，出现下列情形，致使本合同的履行成为不必要或不可能的，可以解除本合同；

王默润

1．因发生不可抗力或技术风险。

第十二条　双方因履行本合同而发生的争议，应协商、调解解决。协商、调解不成的，确定按以下第 1 种方式处理：

1．提交南京仲裁委员会仲裁；

2．依法向人民法院起诉。

第十三条　双方确定：本合同及相关附件中涉及的有关名词和技术术语，其定义和解释如下：

1．/

第十四条　与履行本合同有关的下列技术文件，经双方以 书面 方式确认后，为本合同的组成部分：

1．技术背景资料：/

2．可行性论证报告：/

3．技术评价报告：/

4．技术标准和规范：/

5．原始设计和工艺文件：/

6．其他：乙方投标/参选/应答文件

第十五条　双方约定本合同其他相关事项为：乙方与甲方签订《网络安全服务人员保密协议和安全承诺》（详见附件 2），并向甲方提供所有参与合同人员无犯罪记录证明、背景调查证明材料及《保密承诺书》（详见附件 3，一人一份）。

第十六条　本合同一式 陆 份，具有同等法律效力。

第十七条　本合同经双方签字盖章后生效。

甲方：江苏省水利厅　（盖章）

委托代理人：　（签名）

年　月　日

乙方：江苏省公用信息有限公司　（盖章）

法定代表人／委托代理人：　（签名）

年　月　日

王默涧

合同编号：JSGXS2500010CGN00

附件 1：

江苏省水利互联网安全保障服务（2025 年）要求

1. 项目名称及范围

项目名称：江苏省水利互联网安全保障服务（2025 年）。

项目范围：江苏省水利厅、厅直各单位、市县水利局互联网应用资产。

2. 服务内容

2.1 安全运营服务方案

投标人提供互联网重点互联应用资产网络安全实时监测服务功能。监测信息应全面、准确，实时性应满足采购人对网络安全监测需求。投标人提供实时监测服务功能要求如下：

2.1.1 运营技术方案

投标人依据本项目要求编写运营技术方案，做到运营内容全面、实时，方案合理可行。对省水利厅、厅直各单位、地市及县属水利局的互联网重点应用资产进行实时监测，发现互联网重点应用资产存在的各类网络与信息安全事件，提升空间威胁监测能力，特别是上级单位开展攻击演练时应具备安全监测、应急处置能力。

2.1.2 安全数据汇聚存储技术方案

投标人依据本项目要求编写安全数据汇聚存储技术方案，包括数据汇聚技术路线等方面，方案合理可行。提供网络安全数据汇聚存储服务功能，包括威胁情报库、资产信息库、安全事件库，实现网络环境安全类、管理类数据以及网络资源的采集和集中存储，并将网络监测系统发现的应用资产、安全事件、流量日志、安全告警、威胁情报等多方面信息汇聚存储。

2.1.3 应用服务功能技术方案

投标人依据本项目应用服务功能技术方案。提供资产管理、网络安全分析、事件应急处置、统一指挥展示等应用服务功能技术方案，思路清晰、合理可行，架构完整、符合实际需求。

（1） 网络资产管理

提供入网水利资产的信息收集管理，建立资产信息管理台账，对网络资产进行常态化管理服务。将资产上报、各次扫描、复扫结果进行关联存储、分析、统计、汇总等，报备确认后形成资产清单库、历史资产信息快照、当前最新资产信

王默润

息。建立资产信息管理与资产安全管理的风险评估、漏洞情况、检查核查、事件处置、等级保护、维护管理等关联机制。

（2） 网络安全分析

提供水利互联网安全分析服务功能，具备海量、多源、异构数据存储、分析和建模能力，支撑网络安全监测与追踪溯源分析业务。通过建立离线分析模型（基于专家经验或机器学习），挖掘更深层次的安全事件，从而建立实时监测和离线发现结合，可整体感知网络的安全威胁态势。实现攻击态势、网络异常行为、威胁预警、安全态势报表等服务功能。

（3） 网络安全事件应急处置

提供网络安全事件及处置子系统服务功能，对于互联网中重点水利信息化系统可能发生的各种网络安全事件，在第一时间做出快速反应并采取应对措施，及时恢复信息网络和业务系统正常运行，最大程度控制和降低事件造成的负面影响及损失，确保信息系统运行的连续性、有效性。主要包括安全事件主动防御、事件闭环管理等。

（4） 网络安全统一指挥展示

提供网络安全统一指挥展示服务功能。依托各类网络安全数据，按照水利信息系统特点进行态势感知和联动分析，通过多维数据关联分析，提供网络安全态势、安全预警分析、资产分布管理、安全事件分布、安全事件闭环管理等可视化展示手段，通过大屏显示系统展示。具有为网络安全业务工作提供统一指挥和调度支撑等功能。

2.2 服务要求

（1） 网络安全运营服务要求

①网络安全运营服务工具

提供一套网络安全运营服务工具，满足如下功能要求：

功能指标	技术要求
资产管理	能够自动发现在网设备开放的端口及服务，为后续威胁分析及处置提供便利。
	支持按照资产名称进行查询，高级查询支持基于 IP 地址，资产价值，资产责任人，所属区域进行检索查询。
日志采集	支持对注册的 Agent 进行管理，包括对 Agent 进行启动、停止操作，以及支持以列表形式展示管理的 Agent。
	支持通过离线导入方式导入日志，导入历时日志时，可以根据日志信息进行设备厂商、对应设备型号、文件编码、日志类型进行范式化匹配。

功能指标	技术要求
安全事件分析	支持展示对应安全事件能够导致的风险危害，并支持对风险危害自定义内容修改，便于同样安全事件周期性处置确认。
	支持对安全事件中的灰色事件自动化处置，误报事件会自动处置为自动忽略；非误报事件基于判定模型会进行状态重新判别。
威胁处置	支持 NAT 溯源功能，查找内网资产，并能够查看相对应的安全风险，并在此基础上支持查找相似行为主机，提前规避风险。
	发现安全事件后，可以支持同品牌路由器、交换机、防火墙、入侵防御、终端安全管理软件联动处置。
安全管理	为保障信息安全，防止通过平台产生敏感信息泄露事件，弱口令功能模块支持隐藏采集到的弱口令账号和密码信息，如需查看，通过提供管理员密码进行控制。
	支持按照硬盘空间阈值百分比和时间阈值保存天数自动进行数据清理。
综合展示	支持自定义展示图表设置，根据用户需求选择可展示内容，包括可选资产安全信息、用户安全信息、安全事件信息、端口分布信息和综合报告展示模块设置。

②网络安全入侵防御服务工具

提供一套网络安全入侵防御工具，具备入侵防御功能、URL 过滤功能、行为审计功能、数据安全功能、加密流量检测功能、DDoS 防护功能，诊断功能。

功能指标	技术要求
产品架构	采用多核多线程并行操作系统架构
部署模式	支持路由模式、透明模式、混合模式部署
路由功能	支持静态路由、策略路由、RIP、OSPF、等价路由等路由协议
接口要求	提供不少于 2 个万兆接口，不少于 10 个千兆光口，不少于 16 个千兆电口，具备独立管理接口。（提供证明材料）
入侵防御功能	集成入侵防御与检测、病毒防护、带宽管理和 URL 过滤等功能，所有特性全面支持 IPv6 ，支持 WEB 攻击特征库
URL 过滤功能	提供预分类的 URL 地址库，支持 URL 黑白名单，支持联动云端 URL 地址库进行全面实施核查
行为审计功能	可基于用户名或 IP 地址实现统一分析界面，包括应用流量、网站访问集中分析，基于时间轴的访问行为轨迹，关联账号等相关用户行为审计内容
数据安全功能	支持数据防泄露，对传输的文件和内容进行识别过滤。
加密流量检测功能	支持 HTTPS 加密流量的安全检测。支持 TCP 代理和 SSL 代理

王默润

功能指标	技术要求
DDoS 防护功能	支持流量自学习功能，自动生成 DDoS 防范策略
诊断功能	支持报文示踪功能，可对原始报文进行回放，网页诊断、报文捕获、一键诊断收集
可靠性	提供双电源冗余能力，不断电配置回滚能力
配置要求	配置主机，双电源，不少于 1T 硬盘空间，满足接口要求（提供证明材料）

③重点网站安全监测服务

提供不少于 50 个主 URL 的重点应用网站安全监测,提供资产 Web 漏洞检测，网站资产核查，可用性监控，网页黑链挂马监测，敏感词监测，敏感文件监测，域名解析监测，系统漏洞检测，实时监控以及报表功能;

功能指标	技术要求
网站资产识别	支持自动识别网站资产信息，包括："中间件、JS 库$框架、后台数量、网站状态码、系统名称、ICP 备案编号、网站响应信息等属性。
二级域名扫描	支持二级域名扫描功能，输入一级域名进行一键扫描，自动获取到该域名的二级域名、网站标题、IP 等信息。（提供证明材料）
IP 反查域名监测	输入 IP 或者网段，自动获取到 IP 对应的域名、url、网站标题、返回状态码。（提供证明材料）
网站资产台账	系统应具备网站资产台账功能。 包括：支持导入，添加网站资产的资产属性，比如子域名、系统名称、负责人、负责人联系方式、价值等。（提供证明材料）
web 漏洞监测	支持网站漏洞扫描，如"跨站脚本攻击、FCKeditor 任意文件上传、cookie SQL 注入漏洞、ASP 代码注入、SQL 注入、SQL 盲注"等网站脆弱性漏洞。
web 漏洞跟踪管理	支持对漏洞进行处置，并记录漏洞误报处置历史
可用性异常事件监测	模拟浏览器访问，监测站点的可用性情况，监测频率低至 5 分钟/次
域名劫持事件监测	监测域名截止异常 IP，监测频率低至 5 分钟/次
全站敏感词事件监测	用户可对不同网站自定义不同的敏感词库,并显示站点名称、网站地址、敏感词、敏感链接数量等。
敏感文件事件泄露监测	可监测发布到网上的文件中是否包含"身份证号、邮箱、手机号码、页面敏感字"等敏感信息，可在系统上查看敏感链接及敏感词。（提供证明材料）

王默润

功能指标	技术要求
报表管理	支持生成各个网站监测综合报表、网站监测站点报表、html_漏洞综合报表。报表可自定义时间，选择生成的报表包含的模块：可用性、域名劫持、篡改、高风险漏洞、中风险漏洞、敏感词、敏感文件等。
监测中心	展示整体安全监测概况，呈现主机监测雷达图、漏洞分类图、web 监测雷达图、风险主机、风险站点、事件趋势包含："可用性、篡改、敏感词、敏感文件、黑链/挂马"等。
邮件告警	支持邮件告警，告警发件邮箱配置。

④威胁诱捕服务

提供一套威胁诱捕服务工具，满足如下功能要求

功能指标	技术要求
沙箱仿真模块	组合服务构建沙箱：创建沙箱时，支持选择多个服务进行自由组合，保障沙箱最大程度的灵活性；关联同网段空闲 IP，可绑定当前沙箱的所有服务。（提供证明材料）
	应用服务：支持 wiki、bbs、discuz、ecshop、espcms、websphere、phpmyadmin、confluence、hadoop、crm、oa、tomcat、mailbox、jboss、zabbix、struts2.jenkins、weblogic、vpn、joomla 等不少于 20 种高交互应用服务类模板。（提供证明材料）
	数据仿真：新建沙箱时，向沙箱中注入脱敏数据，随机替换 web 服务的模板，增加沙箱的真实性。（提供证明材料）
诱饵感知模块	平台反制：支持制作 Windows、Mac、Android 反制木马，支持一键免杀（提供证明材料）
智能蜜网模块	一键探测：支持一键探测所在网络的资产信息：发起探测 IP、Vlan ID、未存活 IP 数、操作。（提供证明材料）
溯源反制模块	支持对黑客溯源功能，形成黑客溯源，对溯源结果按照国内、国外、内网分类并展示，可提供对黑客备注功能。（提供证明材料）
	支持黑客画像分析、设备指纹功能，黑客画像分析包括攻击源 IP、操作系统、浏览器信息等。设备指纹包括操作系统、设备类型、CPU 核数、语言、显卡设置、音频设备、浏览器等信息（提供证明材料）
	具备 Macos 攻击反制功能，支持获取系统版本、内核版本、计算机名称、用户名、设备序列号、应用名称、应用版本、浏览器 URL 地址和用户名、微信账号、手机号、钉钉手机号、邮箱等关键信息。（提供证明材料）
	支持攻击事件回放，支持从攻击时间、攻击资产、攻击手法、事件类型等进行筛选。（提供证明材料）
	支持记录攻击者上传的恶意文件，并分析其文件类型、文件 MD5 等，支持 VirusTotal 鉴定、AntiVirus 恶意文件鉴定、webshell 鉴定等。（提供证明材料）
	支持记录攻击者所有行为，并能识别真人与扫描工具，至少能识别 AWVS、Sqlmap 、WebReaver 、WebInspect、NSFOCUS RSAS 等扫描

王默润

	工具。（提供证明材料）

⑤上网行为管理工具

指标项	描述
硬件和性能	设备实配≥12 个千兆电口，8 个千兆光口, 4 个万兆光口
	硬盘≥2T，实配双电源
部署适应性	支持路由模式、透明（网桥）模式、旁路模式、混合模式
	支持 VRF，可以将接口添加到 VRF 内
行为审计	支持 http、邮件、即时通讯、基础协议、娱乐股票、网络应用六个大类维度的用户应用审计。
	支持 IM 聊天行为审计、网页版微信审计、移动飞信审计、其他即时通讯类软件审计等细粒度的审计。
SSL 加密内容审计	支持 HTTPS 解密功能，支持管理界面及命令行配置解密策略，包括入接口、源地址对象、目的地址对象、https 对象、域名排除等。
流量管理	支持高性能的限制通道，限制通道支持基于接口、地址、用户、用户组、应用、服务、时间维护的条件匹配，支持每 IP 和每用户限速配置。
	支持惩罚通道建立、支持惩罚通道内限制每 IP 和每用户限速。
资产管理	支持主动扫描发现内网资产、被动从网络流量中识别资产，获取资产基本信息。
	支持用户手动新建、导入、导出资产信息。
综合展示	支持小时/天/周/自定义时间为单位的用户流量、应用流量、设备流量趋势图、列表 TOP 统计展示

（2） 攻防演练服务要求

采购人根据工作安排提前 10 天通知投标人开展漏扫工作时间；采购人根据水利互联网安全检查需要，提前 30 天通知投标人开展渗透工作时间。

为有序开展江苏水利互联网安全检查服务工作，投标人应根据采购人要求编制服务方案，内容包括组演练队伍、签订保密协议、攻击工具、展示环境、演练规则、配套软件、账号及使用说明、应急措施等。

投标人应投入充足的专业技术人员，且具有较强的后端服务支撑能力，能够及时响应服务期间采购人的紧急性、突发性服务支持需求。后端支撑团队服务支撑内容包括提供日常安全咨询、疑难安全事件分析研判、安全情报分析、突发性事件处置，必要时能够通过后备人员及时补充服务力量。

投标人应根据采购人授权内容完成工作任务，深度渗透以取得证据、点到为

王默润

止，不得对应用资产造成破坏，演练过程录屏、录像做到有据可查。

投标人应保障所有攻防检查工具的相关信息得到有效清除，且无法通过已知技术手段还原，如收集报告、清除后门、回收账户及权限、设备回收、网络恢复等工作。当次服务结束后应及时清理现场，采购人将组织查验清理痕迹和结果。

投标人负责对参与重要环节的人员进行背景审查，投标人需与参与服务人员提前签署保密协议，不得泄漏目标单位任何信息。

投标人应对项目需求内容理解透彻，提出的攻防演练方案可执行性强，攻防演练方案的场景涵盖范围广、针对性强。

①攻防演练总体要求

提供至少两支攻击队参与攻防演练服务，各攻击队应充分发挥各自的优势和特点，运用各种攻击手段和战术策略，对目标系统进行全面、深入的攻击测试，旨在发现潜在的安全漏洞和风险，为提升目标系统的安全性提供有价值的参考和建议，同时也为参演各方提供一次实战经验交流机会，共同推动网络安全防护水平的提升。*（本项为实质性要求，供应商提供承诺书，否则视为未实质性响应采购文件）*

②攻防演练平台功能要求

投标人需提供可投放到大屏幕的网络安全攻防工作动态可视化界面，提供网络安全攻防演练实况展示。在攻防演练期间，针对攻击队伍获取到的成果，提供攻击数据成果展示功能。

功能指标	技术要求
演练平台功能	账号管理、组织管理、策略管理、成绩管理、攻击分析、公告管理、数据大屏、系统设置、队伍成绩、举报管理、公告信息、成绩评审、违规处理等；
演练场景	支持攻防演练实战、安全培训演练等多种场景
多维度演练	支持攻击流量监控、攻击操作监控等，对演练过程和结果进行数据分析和展示
可视化展示	支持多个展示模块包含攻击队状态、防守队状态、演练动态
自定义功能	支持用户自定义演练场景和任务，以满足不同组织的特定需求和培训目标

③攻防演练具体内容

资产探测

授权投标人组建的队伍对互联网以广谱扫描方式查找与江苏水利有关的 Web

王默润

和 APP 应用、小程序等未申报的互联网资产，发现易被攻陷的高危主机，发现存在恶意行为的主机，经采购人核实后列入渗透测试对象。

漏洞扫描

利用专业工具对掌握的互联网资产进行全覆盖全漏洞扫描，挖掘系统的弱口令、XSS、文件上传、服务器提权、远程命令执行等潜在风险漏洞，自动生成漏洞扫描报告，提出整改建议措施。

渗透测试

对互联网资产模拟黑客渗透攻击，挖掘系统的弱口令、XSS、文件上传、服务器提权、远程命令执行等漏洞，并展示漏洞利用的过程。测试各单位部门的网络安全感知、应急防护能力，查找风险漏洞，提出整改措施。

漏洞复测

对上级单位攻防演练发现和采购人委托检查发现的网络安全漏洞进行复测，检验漏洞整改情况，以及查找是否存在新的风险漏洞。

安全整改服务

在水利厅攻防演练期间，需针对发现的网络安全漏洞编写网络安全整改通知，配合局点完成网络安全整改，整改后提供复查等服务。

攻防演练技术材料输出

攻防演练完成后服务商须提供下列文件，包含但不仅限于：攻防演练服务实施方案，攻防演练服务报告（含整改建议），攻防演练服务总结报告，攻防演练资产成果、监测成果等。

（3） 其它服务要求

①不定期防守保障服务

做好中央网信办、公安部、水利部、省委网信办等单位开展的网络安全攻防演练活动时的防守工作，包含但不限于以下工作：

每次防守工作开展前，需制定保障工作整体方案及工作计划；

对单位内网络、资产进行梳理，在已有梳理结果上进行补充完善；

开展漏洞扫描、渗透测试、入侵排查，对漏洞尤其是中高危漏洞，必须进行整改或采取严格的缓释措施，进行防护能力评估和安全加固开展，安全设备和防护系统部署；

建立演练攻防团队、制定攻防实战演练预演习方案、沟通预演习工作基本信息，并制定应急预案以及应急预案演练；

王默润

建立协同防守团队，在演练开展期间，提供 7×24H 现场人员安全值守、入侵攻击监测，做到多家防守单位情报共享、攻击研判，开展入侵事件应急处置，并按应急预案开展应急处置；

通过本次保障实战，总结攻击方式方法，分析安全防护缺陷，指导安全建设和安全防护能力提升。

②法定节假日现场值守服务

做好国家法定节假日期间的现场值守工作，要求如下：

每次防守工作开展前，需制定保障工作整体方案及工作计划；

对单位内网络、资产进行梳理，在已有梳理结果上进行补充完善；

开展漏洞扫描、渗透测试、入侵排查，对漏洞尤其是中高危漏洞，必须进行整改或采取严格的缓释措施，进行防护能力评估和安全加固开展，安全设备和防护系统部署；

建立协同防守团队，在保障开展期间，提供 7×24H 现场人员安全值守、入侵攻击监测，做到多家防守单位情报共享、攻击研判，开展入侵事件应急处置，并按应急预案开展应急处置。

③新系统上线安全检测服务

提供新业务上线时的系统安全检测服务，包含渗透测试，漏洞扫描，漏洞复测等服务，人员需具备以下能力要求：

需配备至少 6 人的安全测试服务团队。精通安全测试技术手段，并可独立开展安全测试工作，所有成员都具备 2 年以上的渗透性测试服务经验；

测试团队应在管理团队的统一协调下，按需提供及时的服务响应，储备每日不低于 6 人的安全测试服务团队人员，保障在提出安全测试服务需求的 1 日内到达现场提供服务，包括护网，重点节日，重大活动等特殊时期。

④应急响应处置服务

提供中央网信办，公安部、水利部、省委网信办等单位给予安全风险或安全事件通报后的应急响应处置服务，相关人员需具备以下要求：

需配备至少 6 人的安全应急响应服务团队。精通安全响应，溯源等技术手段，并可独立开展安全响应工作，所有成员都具备 2 年以上的应急响应服务经验；

应急响应团队将在管理团队的统一协调下，按需提供及时的服务响应，储备每日不低于 6 人的应急响应服务团队人员，保障在提出安全应急响应服务需求的 1 日内到达现场提供服务，包括护网，重点节日，重大活动等特殊时期；

王默润

攻防演练服务期间一旦出现意外事件，应安排专业人员立即进行远程处置，无法远程处置的应在 6 小时内到现场检查处置。

⑤定期扫描与检查服务

提供每月 1 次日常网络安全漏洞扫描和漏洞复测服务，编写网络安全整改通知，输出月度报告、季度报告和年度报告。

⑥现场驻场服务

投标人应安排网络安全技术人员驻水利厅提供网络安全保障服务，人员需具备以下要求：

人员数量配备：日常需配备 2 名信息安全工程师（中级）以上网络安全技术人员，其中 1 人常驻水利厅开展网络安全服务，另 1 人现场攻防演练服务技术经理负责处理协调水利厅发生的突发安全事件以及对接水利厅的安全需求。重要时期提供 7×24 小时技术人员值班服务保障网络安全。

驻场时间：自合同签订日起至 2025 年 12 月 31 日，需接受值夜班工作安排。

工作时间：日常工作时间，驻场人员与省水利厅作息时间同步，发现问题 2 小时内处置。重要时期保障工作时间按需调整。

工作职责：信息安全事件处置管理，信息安全产品运维，IT 风险管理与漏洞修复，协助灾难恢复相关工作，信息安全日志监控，安全渗透测试结果复查，漏洞复现工作。

⑦网络安全技术培训服务

投标人应安排网络安全技术专家，对水利厅信息化管理，根据水利厅的实际需求，开展信息化技术能力培训，例如 WEB 安全基础、渗透测试介绍、信息收集技术介绍、渗透测试工具介绍、漏洞实操演练（暴力破解、SQL 注入、命令执行、文件上传、文件包含等）。

⑧厅直单位网络安全检查

投标人应在汛前等重要时期配合省水利厅开展厅直单位网络安全检查工作，提交网络安全检查报告。

附：投标人如为满足本项目服务内容需提供软硬件设备，自行负责设备安装和移除，所有成果以 Word 或 Excel 文档格式移交采购人。

王默润

（4） 服务清单

江苏省水利互联网安全保障服务（2025 年）清单

序号	项　　目	单 位	数 量
一	网络安全运营服务		
1	网络安全实时监测	项	1
2	网络安全数据汇聚存储	项	1
3	网络安全应用	项	1
4	网络安全运营服务工具	项	1
5	网络安全入侵防御服务工具	项	1
6	上网行为管理工具	项	1
二	攻防演练服务		
1	资产探测	项	1
2	漏洞扫描	项	1
3	渗透测试	项	1
4	漏洞复测	项	1
5	安全整改服务	项	1
6	攻防演练平台	项	1
三	其它服务		
1	重点网站安全监测服务	个	50
2	威胁诱捕服务	项	1
3	不定期防守保障服务	项	1
4	法定节假日现场值守服务	项	1
5	新系统上线安全检测服务	项	1
6	应急响应处置服务	项	1
7	定期扫描与检查服务	项	1

王默润

8	人员驻场服务	人	2
9	网络安全技术培训服务	项	1
10	厅直单位网络安全检查	项	1

2.3　攻防演练总结报告编制

网络安全攻防演练报告编制技术要求：应体现攻防演练科学性分析，攻防演练实战过程分析（科学、合规、可回溯），多维度演练成果数据分析，体现演练价值，提供安全整改建议，提出符合江苏水利系统实际的网络安全建设近期规划任务。

王默润

合同编号：JSGXS2500010CGN00

附件 2：

网络安全服务人员保密协议和安全承诺

乙方仔细阅读本文件，知悉并理解本文件的所有规定和要求，并承诺在江苏省水利互联网安全保障服务（2025 年）合同实施过程中严格遵守执行。

一、保密协议

（一）本协议所称“保密信息”是指：系统账号（系统管理员账号、普通账号）和用以上账号可以获取有关系统、业务、用户的数据和信息，IP 地址、网络拓扑、业务流程、规章制度、资产重要性信息、项目输出等。包括但不限于：任何甲方不欲公开的观点、发现、发明、公式、程序、计划、图表、模型、参数、数据、标准和专有技术秘密，或其中的任何知识产权。

（二）甲方向乙方提供保密信息的行为不构成向乙方授予任何与保密信息相关的专利权、专利申请权、商标权、著作权、商业秘密或其它的知识产权。

（三）乙方承诺为甲方 提供网络安全服务 目的使用保密信息。

（四）未经甲方的事先书面批准，乙方不得以任何形式或任何方式将保密信息或其中的任何部分，披露或透露给任何第三方。乙方有义务妥善保管保密信息，不得复制、泄漏或遗失。乙方亦不得依据保密信息，就任何问题，向任何第三方做出任何建议。

（五）乙方违背保密承诺，未按照本协议的规定使用保密信息或向第三方披露保密信息，或依据该保密信息向第三方做出任何建议，都被视为乙方违反本协议。

（六）如任何一方违反本协议，违约方应按照《中华人民共和国合同法》的相关规定承担违约责任。

（七）甲方保留在甲方认为必要的情况下收回所提供的保密信息及其使用权的权利。

（八）凡因执行本协议所发生的或与本协议有关的一切争议，双方应通过友好协商解决。如果协商不能解决时，申请 南京市 仲裁委员会依其仲裁时现行有效的仲裁规则进行。

（九）本协议须经乙方签字后方能生效。

（十）本协议规定的保密责任的期限为自本协议生效之日起 3 年内有效。

二、安全承诺

乙方承诺严格遵守国家和各级监管部门在信息安全方面的法律法规、严格遵守甲方已实施和即将实施的信息安全方面的不违反国家法律法规的各项管理制度和要求，包括但不限于以下方面：

（一）自觉遵守职业道德，有高度的责任心并自觉维护甲方的利益，不得以任何理由利用甲方信息资源从事危害国家利益、甲方利益及其它组织或个人利益的活动，不得从事危害信息系统安全的活动；不利用获得的资源从事国家法律法规或公共道德所禁止或不受欢迎的活动，因上述活动而产生的问题，乙方承担相关责任。

（二）乙方不得向任何个人或单位提供项目实施中所获取的信息，包括但不限于账户信息、信息系统和信息设备配置信息、源代码等；

（三）乙方在项目实施过程中应尽量避免影响甲方业务的正常运转，若出现意外操作而导致异常则应立刻通知甲方并积极配合协商解决；

（四）在项目实施完成后，乙方承诺即时销毁在项目实施过程中获取的甲方项目实施信息，清理恢复实施现场为实施前状态，不对外泄露甲方项目实施信息；

三、本协议壹式 贰 份，甲乙双方各执 壹 份，具有同等法律效力。

甲方：江苏省水利厅（盖章）　　乙方：江苏省公用信息有限公司（盖章）

日期：　　日期：