附件1

**网络与信息系统等级保护**

**第三方运维(2024年）**

**（二）服务内容及要求**

1.服务内容：包含安全评估服务、安全巡检与通告服务、安全加固服务、应急演练服务、应急响应服务、安全培训服务、重要时期安全保障服务、攻防演练防守保障服务、等保咨询服务以及其他相关网络与信息安全服务和保障工作。

2．服务要求

2.1安全评估服务

通过安全评估来识别的安全现状，全面了解和掌握系统面临的安全威胁和风险，为安全需求和解决方案的提出提供原始依据，为信息系统的使用、管理部门开展网络安全等级保护提供依据，为确立安全策略、制定安全规划、开展安全建设提供决策支持，保障信息系统安全运行。

2.1.1网络架构安全评估服务

分析自建机房整体的网络拓扑结构安全隐患，分析网络内部网络面临的外部和内部威胁，面向数据中心机房网络。

2.1.2网络设备安全评估服务

评估自建机房现有网络设备的配置、使用状况、漏洞情况，考察网络设备的有效性、安全性，面向交换、路由设备。

2.1.3安全设备安全评估服务

评估现有安全设备的配置、使用状况、漏洞情况，考察安全设备的有效性、安全性，面向防火墙、上网行为管理、日志审计、堡垒机等相关安全设备。

2.1.4主机服务器系统安全评估服务

利用扫描工具及相关人工测试等方式检查整个网络内部网络的主机系统与数据库系统的漏洞情况，评估主系统与数据库本身存在的安全漏洞，面向数据中心机房网络。

2.2安全巡检服务

2.2.1安全扫描服务

通过使用自动化安全漏洞挖掘工具和在线检测平台，以基于互联网远程检测的方式，来测试和识别当前的安全漏洞和存在的安全脆弱性，从而帮助招标方全面了解和掌控其应用系统的安全状况。

2.2.2渗透测试服务

对业务系统进行人工渗透测试。直观体现安全风险现状，针对渗透成果获得有效处理方案；防止系统入侵安全隐患再次被黑客利用；帮助建立一体化信息系统隐患检测机制，渗透成果作为信息系统信息安全建设参考依据。

信息收集

通过搜索引擎侦测、专业化工具检测结合人工分析，对业务应用系统、中间件、操作系统等类型指纹收集分析、端口扫描和目标系统提供的服务识别等，确定信息资产互联网暴露面。

配置管理测试

开展业务系统配置管理方面安全测试，主要内容包括敏感目录遍历、 Robots方式的敏感接口查找、 Web服务器的控制台、文件备份测试、 HTTP开启方法测试等方面测试。

认证测试

开展业务系统认证方面安全测试，主要内容包括登录验证码、认证错误提示、锁定策略、认证绕过、找回密码、修改密码、安全的数据传输、强口令策略、手机验证码、撞库、接口滥用等方面测试。

会话管理测试

开展业务系统会话管理方面安全测试，主要内容包括会话变量泄露、 Cookie属性测试、 Cookie存储方式测试、用户注销登陆的方式、注销时会话信息测试、会话超时时间测试、会话固定测试等方面测试。

授权测试

开展业务系统授权方面安全测试，主要内容包括绕过授权模式测试、横向提权测试、纵向越权测试、后台页面未授权访问测试、中间件未授权访问测试等方面测试。

文件上传下载测试

开展业务系统文件上传下载方面安全测试，主要内容包括 HTTP PUT/MOVE上传文件测试、页面上传测试、文件下载测试等方面测试。

信息泄露测试

开展业务系统信息泄露方面安全测试，主要内容包括连接数据库的帐号密码加密测试、源代码敏感信息测试、源代码注释测试、不安全的存储、注册手机号批量获取、 Json敏感信息测试等方面测试。

数据验证测试

开展业务系统数据验证方面安全测试，主要内容包括跨站脚本类测试、SQL注入类测试、命令执行测试等方面测试。

2.2.3配置核查服务

对服务器开展合规性配置检查，采用基线核查工具和专家手工方法对实施范围内的主机系统、应用系统、数据库系统等对象逐个进行检查分析，输出详细的基线核查情况，详细说明各类资源节点运行情况及调优建议。

2.2.4网络巡检服务

为了确保核心信息系统安全稳定的工作，最大限度的降低系统的运行故障，提供安全设备、服务器系统、网络设备等周期性巡检服务。巡检采用网络运维工具进行自动化定期巡检，网络运维工具应具备如下功能：

（1）支持业务拓扑，以拓扑形式展示每个业务流程中的每台相关设备，展示业务流程中涉及到的所有的设备之间的链路关系，流程方向。

（2）支持网络设备监控管理，网络设备管理包括路由器、交换机、安全设备等的监测。需支持业界主流厂商网络设备的自动发现和性能采集。支持主机设备监控管理，支持对Linux、Windows、AIX、Unix、Solaris等主流操作系统的监控，Windows支持SNMP协议和WMI协议，Linux、AIX、Unix、Solaris操作系统支持SNMP、SSH、Telnet协议。支持数据库监控管理，支持对主流数据库的监控。系统能够对数据库Instance（实例基本信息）、Session（会话）、PGA、SGA、Background process、Disk storage等关键指标进行实时监控，并通过图表进行可视化显示。支持中间件监控管理，支持市场上各类主流中间件的信息监测，包括有J2EE（WebSphere、Weblogic、TOMCAT）、Apache、Nginx、TLQ、NodeJS、IBMMQ、ActiveMQ、IIS、ElasticSearch等中间件。支持存储监控管理，支持实时监控核心存储设备，分析存储设备的状态和可用性。

（3）支持资产管理，包括物理资产及软件资产，通过资产管理建立了资产数据库。支持统一告警管理，支持经过告警风暴抑制，归一化处理，告警过滤等步骤转换成无冗余的，统一格式的告警消息；对于重复告警信息可进行计数、指定时间间隔再次发送或指定间隔数量后再次发送。提供链路、端口瞬断过滤机制。支持IP地址管理，包括子网容量、使用情况、在线情况、基准IP、可用IP、非法IP。

（4）支持故障自愈，匹配告警设置的执行策略，并执行实现告警自动化处理，实现自动恢复故障。支持根源分析，能够自动将衍生故障归并到根源故障中，使运维人员可快速定位和解决核心问题，提升运维效率。

（5）网络运维工具所使用数据库为国产数据库，且为厂商自研，符合国家对软件自主可控的要求。

（6）采购人有权对网络运维工具是否满足标书要求进行测试验证，恶意应答将会视为失信行为，采购人保留追责的权利。

2.3安全加固服务

根据安全评估、基线核查服务的结果，提供每年4次的应用安全加固辅导、服务器安全加固、Web服务器（中间件）加固辅导、数据库安全加固建议，提升系统整体安全性，并提交报告。

2.3.1主机系统配置加固服务

通过对系统层安全检测结果的分析，对在检测中发现的系统的安全问题进行提交加固措施和建议，针对系统层的安全策略的不足进行加固，以提高系统的整体安全性能。

安全加固服务采用“人工+工具”加固方式，即通过安全基线检查和安全策略修复，并结合第三方安全加固工具实现对操作系统的全面安全增强

（1）提供的安全加固工具支持内核级的强制访问控制功能，支持基于敏感标记(安全等级)控制文件读写权限**（提供对应工具功能截图）**

（2）提供的安全加固工具支持白名单功能，只有属于白名单的进程可以运行，可以有效禁止病毒或木马的执行。**（提供对应工具功能截图）**

（3）提供的安全加固工具支持基于MD5的识别技术的文件完整性检查功能，可对文件进行资源完整性监控。**（提供对应工具功能截图）**

（4）提供的安全加固工具支持基线检查功能，能对常见的系统脆弱性进行一键扫描和加固修复。**（提供对应工具功能截图）**

（5）本次提供的安全加固工具具有IT产品信息安全认证证书，满足“ISCCC-TR-001-2017《操作系统安全加固产品安全技术要求》（增强级）”及以上相关产品标准及技术要求，**提供证书复印件证明**。

（6）采购人有权对安全加固有效性进行测试验证，恶意应答将会视为失信行为，采购人保留追责的权利。

2.3.2主机中间件配置加固建议

针对Apache/IIS/Tomcat/Weblogic等Web应用服务器（中间件），从协议安全等方面进行识别，并提供配置加固与优化建议。

2.3.3数据库安全配置加固建议

提供数据库安全加固建议，包括最大程度降低数据库系统（SQL Server，Oracle等）本身的漏洞风险、纠正数据库系统使用中构成安全威胁的错误策略、加强数据库系统账号、密钥、权限等带有安全风险的配置，从整体上提升数据库系统的安全性。

2.3.4应用安全加固建议

对信息系统提供通过对源代码层级的加固建议，可有效防范危险字符提交、权限绕过、允许上传、远程包含等漏洞，并可以有效修复如SQL注入漏洞、XSS跨站漏洞、恶意代码上传漏洞、Cookie注入漏洞及网页Webshell等类型漏洞。

2.4应急演练服务

根据《网络安全法》等国家、各行业相关文件精神，应妥善处理应对和处置信息系统突发事件，确保信息系统的安全、稳定、持续运行，防止造成重大的损失和影响；增强用户人员的安全意识。根据突发网络安全事件的性质,深度切合本单位所面临的实际网络安全问题，为本单位提供全方位,分门别类的演练方案。

通过定期对信息网开展安全应急演练，检验网络与信息安全综合应急预案和业务技术专项应急预案的有效性，保证各项应急指挥调度工作迅速、高效、有序地进行，给用户进行体验式的安全意识教育。同时通过演练，不断提高各部门开展应急工作的水平和效率，发现预案的不足，进一步完善应急预案。

编制应急预案服务

编制1个预案场景的《安全应急预案》。建立应急预案框架，框架应包括事件分级方法、各级事件启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容。

安全应急演练服务

为信息系统安全，预防和遏制突发安全事件的发生，减轻和消除突发事件造成的危害和影响，进行应急演练，确保能够应对各类安全事件的发生。

根据拟定的安全预案模拟1个预案场景进行应急演练，并提交《安全应急演练报告》。

2.5应急响应服务

投标人向招标人派驻金鸡山环保大楼机房现场维护人员1名，投标人需开设专用的电话维护热线及监督电话，在维护时间内向招标人提供全天候电话呼叫维护服务。节假日按招标人实际要求执行，应有24\*7\*365服务热线，备应急服务之用。招标人因紧急工作任务需要加班的，投标人同样需安排人员加班。

提供全年的远程及现场的安全应急响应服务以及安全检查技术支持服务，当安全事件发生后，向提供发现问题、解决问题的快速、有效的响应，为快速恢复系统的保密性、完整性和可用性，阻止和减小安全事件带来的影响，提高用户网络故障排查效率。

远程应急响应服务

提供7×24小时应急响应服务，1小时内电话或QQ远程支持和响应。

现场应急响应服务

远程应急响应无法解决问题时，2小时内现场响应。

2.6安全培训服务

基于对网络安全产品和丰富的安全运维服务经验，提供全面深入的信息安全知识方面培训，面向网络管理员、信息技术人员或者全体员工的定制化安全培训服务。

开展网络安全意识培训(一节课45分钟)，面向员工讲座，培训内容包含不限于以下方面：安全标准、政策法规解读，信息安全意识、信息安全发展方向，周期性安全服务报告解读，可定制培训内容。

2.7重要时期安全保障服务

上级部门安全检查配合服务

针对上级主管部门下发的安全检查通知，配合用户进行相关政策的解读和消化，根据检查指标和要求等准备相关资料并先进行自查，不足之处立即进行整改，在上级主管部门检查过程中，我们将全力配合进行人员访谈、资料准备、将上级主管部门领导的意见和建议进行记录和反馈等工作，完成整改之后，记录已完成整改的内容及下一步调整、优化思路。

特殊时点安全检查配合服务

在特殊时期，包括在重大会议前夕、国内重大节日、重大历史事件纪念日或者国家局领导检查时期，国内发生特殊敏感事件时期、有新的病毒或漏洞出现、重大安全事件发生等特殊时期，可进行远程守护服务，检查网络门户网站的首页是否被篡改，监控网络和互联网统一出口流量情况，提供全面的评估、应急响应等服务。

区县网络与信息安全监督检查服务

配合业主单位，摸底福州市各县市区生态环境部门网络和信息化工作开展情况。了解各地信息化安全管理机构建设、日常管理、安全防护、应急管理以及安全教育培训等工作开展情况，对发现的问题提出相应的整改意见并提供技术支持。

2.8攻防实战演练防守保障服务

在采购人作为攻防演练的防守单位时，组织围绕相关的信息资产开展的网络攻防实战活动，将通过网络安全攻防演练，进一步检验网络安全防护能力、监测发现能力、应急处置能力，在实战中有效提升网络安全保障能力。针对攻防实战演练期间需辅导相关负责人完成以下工作内容：

制定攻防演练保障方案

制定攻防演练工作方案，包含组织架构、工作分工、实施计划与方案，准备工作、演练期间风险排查、正式演练监测保障、总结等阶段工作内容。

演练期间风险排查工作

对本单位的参演系统进行：资产分析及梳理、网络架构评估服务、安全策略有效性评估服务、服务器入侵检查服务、漏洞扫描；

攻防演练安全整改加固

整体加固：强口令、外部访问权限、内部访问IP；

访问控制策略优化、设备部署和调试；

安全风险较高、业务连续性较低的系统，下线或临时关停；

安全监测服务

安全专家团队在本单位现场，提供安全监测分析，对网络中异常流量进行检测分析，及时发现可疑的执行文件和网络流量，针对潜在的未知攻击进行预警。

溯源分析服务

现场保障值守人员对监测发现的网络风险、主机风险、网站风险进行溯源分析，其中对流量日志、主机日志、应用日志进行分析、审计、溯源等操作，找出事件根源所在。编写和提交《防守报告》。

汇报总结服务

对防守过程事宜进行各方协调、汇报工作；撰写总结报告；整改问题和复查漏洞；完善制度：在护网行动中暴露出来的组织管理、处置流程等方面的问题进行修正完善。

2.9等保咨询服务

结合“等级保护 2.0”，对本单位内信息系统提供等保咨询服务，包括但不限于定级、备案、差距分析、整改以及管理制度梳理等服务。

2.10其他临时性相关服务和保障工作