一、项目概况

为加强总队所使用与管理的信息系统网络安全管理，保障信息系统网络安全、计算机软硬件系统和网络安全设备稳定运行，特向专业信息安全服务公司采购安全运维服务。

二、项目服务内容及范围

1、信息系统安全运维服务：包含信息系统安全监测服务、渗透测试服务、漏洞跟踪服务、系统安全清查服务、安全通告服务、日志分析服务、安全加固服务、专项应急预案以及演练服务、安全培训服务、协助监督检查服务、机房设备电源安全保护服务。

2、等级保护差异化评估:提供专业的安全体系建设建议，制定等级保护安全整改与实施方案。

3、 计算机和网络安全软硬件维护服务：总队计算机和网络安全设备软硬件维护服务。

4、网络安全审计服务：对总队所有互联网办公电脑上网行为的日志进行记录服务。

5、视频会议系统维护服务：对总队所有视频会议系统进行现场维护服务。

4、项目服务期限：一年。

三、项目服务要求

（一）信息系统安全运维服务

1、信息系统安全监测服务

包含合同期内总队已有和新建软件系统的安全监测服务，服务内容：通过专业的网站安全监控平台以及人工监控和分析相结合的方式，对网站的安全状态、网络质量及网站安全事件进行7\*24小时全面的监测服务。针对网站的安全情况定期推送安全检测报告，让客户方能全面了解网站的运行状况，有效解决重要网站的安全防护问题。

（1）网页挂马监测

网站安全监控平台支持对多种挂马方式（如Iframe、CSS、JS、Body挂马）等进行检测，并进行告警；

（2）网页篡改监测

采用语义分析技术对网站进行敏感关键字监测，判断系统是否存在恶意发布的违法、反动、色情等敏感信息，并进行定位和告警；

（3）网站可用性监测

支持通过从域名可用性、网站服务可用性和网站程序可用性进行实时监测；

（4）网站漏洞检测

支持检测SQL注入、XSS跨站脚本、目录遍历、脚本源码泄露、目录浏览、可能的敏感文件等常见漏洞，检测内容覆盖WASC分类的多达25种Web应用漏洞和OWASP TOP10 网站漏洞；

服务周期：实时监测，每月提供一份《网站监控报告》服务要求：每月汇总一次系统安全监控情况，并提交详细监控报告。

2、渗透测试服务

 针对目标系统开展黑客模拟攻击渗透测试服务，全面检测被测系统安全性。针对应用系统进行渗透测试服务，全面检测Web应用程序的安全性，深度挖掘程序中存在的各种漏洞和所面临的威胁，漏洞测试覆盖OWASP十大漏洞，如命令执行漏洞、SQL注入漏洞、XSS跨站脚本攻击漏洞、XXE漏洞、恶意代码上传漏洞、Cookie注入漏洞及其它各种敏感信息的检查等。主要渗透测试的内容如下：

（1）信息收集：通过搜索引擎侦测、专业化工具检测分析对业务系统所开放的端口、SERVER、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，确定信息资产暴露面。

（2）配置管理测试：开展系统配置管理方面安全测试，主要内容包括敏感目录遍历、敏感接口测试、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方法测试、历史高危漏洞测试例如心脏滴血漏洞，MS17010漏洞等方面测试。

（3）认证测试：开展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。

（4）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。

（5）授权测试：开展系统授权方面安全测试，主要内容包括绕过授权模式测试、横向越权测试、纵向越权测试、管理后台对外开放测试、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。

（6）文件上传下载测试：开展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。

（7）信息泄露测试：开展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、客户端源代码敏感信息测试、客户端源代码注释测试、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。

（8）数据验证测试：开展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。

（9）框架安全测试：开展系统框架安全方面安全测试，主要内容包括业务系统所用框架及其中间件相关类型专项漏洞测试。

（10）业务逻辑测试：针对逻辑方面开展安全测试测试工作，如对用户行为顺序处理不当、业务处理流程逻辑不当等问题。

服务要求：每月汇总一次系统安全监控情况，并提交详细监控报告，服务完成后输出《渗透测试报告》。

3、漏洞跟踪服务

对总队的计算机主机、应用、数据库等资产，通过漏洞评估了解资产软件信息以及潜在的安全漏洞，对资产存在的漏洞进行综合评估，客观评估系统的风险等级，结合系统实际情况对漏洞的风险等级进行赋值，得出漏洞对系统稳定安全运行的危害程度，对所发现的漏洞进行跟踪，督促整改，从漏洞发现到修复完成的全生命周期的漏洞管理，特别针对高危漏洞的处置跟踪和督促整改。

服务要求：服务频率一年四次，服务完成后输出《漏洞跟踪报告》。

4、系统安全清查服务

定期开展桌面系统、服务器及网络设备的运行状况和安全状况检查，建立系统安全管理档案，从结构安全、安全配置、安全策略、日志审查等方面进行巡检。巡检完成后出具安全巡检报告，内容需包含整改建议。针对年度内的网络安全重大检查事项，如在常规检查中有相关专项的缺漏，需不计次数的补充检查完善。

服务要求：服务频率一年四次，服务完成后输出《系统安全清查服务》。

5、安全通告服务

为了更好地运行维护信息安全，通过电话、传真、邮件等方式将前沿的安全技术和安全信息及时传递给客户。最新的安全动态、安全技术的发展趋势，包括时效性很强的漏洞、攻击手法、病毒码的预先通知，帮助客户的安全管理员在最快的时间内了解重要的安全信息。通告内容包括但不限于以下内容：

国内外最新重大漏洞、病毒安全通告；

国家安全政策及法律法规；

同行业安全威胁事件通告；

国内外重大安全事件，新技术发展动态通告；

重大安全漏洞爆发时需结合总队资产情况，提出相应修复建议。

服务要求：在年终汇总全年的安全通告，提交成果《安全通告报告》。

6、日志分析服务

针对系统内现有的关键性网络设备和安全设备，以及主机上的日志信息，利用专业的分析手段，进行日志的汇总、过滤及关联分析，从日志信息上一方面跟踪福建省海洋与渔业执法总队的安全态势变化，对当前的安全策略合理性进行评判；另一方面分析并得出目前系统内在安全策略上尚存的薄弱环节，为合理和及时的采取适当的补救措施提供依据。

通过专业日志软件对相关服务器及应用系统进行日志存储，满足网络安全法日志保存180天的要求。通过日志审计发现安全事件、及时告警并在次月生成上月的日志分析报告。

服务要求：服务频率一年四次，服务完成后输出《安全事件日志分析报告》。

7、安全加固服务

安全加固是对信息系统中的网络设备、操作系统及应用软件的脆弱性进行分析和修补的过程。需提出系统的安全加固方案，在加固过程中可能产生对系统的不同程度、不同方面的影响，针对不同的风险选择不同的策略。安全加固服务的一般性内容如下：

服务器系统加固：通过对系统层漏洞检测结果的分析，对在检测中发现的系统安全问题进行安全加固，提高系统的整体安全性能。

数据库安全性加固：该服务针对数据库系统，主要内容为修复数据库系统本身的漏洞及加强数据库系统账号、密钥、权限等带有安全风险的配置，从而从整体上提升数据库系统的安全性。

服务要求：服务频率一年四次，服务完成后输出《安全加固报告》。

8、专项应急预案以及演练服务

在系统遇到网络入侵、拒绝服务攻击、大规模病毒爆发、主机或网络异常事件等安全事故时提供7\*24小时应急响应安全技术支持，当远程支持无法解决时，要求2小时内到达现场，实施最有效的紧急救援及恢复补救方案。应急处理包括且不限于以下工作：事件范围损失控制，取证，事件处理，外部攻击源追溯，内部脆弱性分析；并提供相关文档详实记录分析判断过程及结果。

针对自身的网络实际情况，并结合网络安全应急处置相关的政策要求，设计出符合福建省海洋与渔业执法总队要求的网络安全应急预案。

服务要求：每年1次组织技术力量配合单位共同完成网络安全应急演练，演练完成后提交《应急演练报告》和相关应急演练记录。

9、安全培训服务

为了提高总队工作人员的安全意识和技术水平，每年按总队需要，开展安全意识培训，比如：政策法规解读，信息安全意识、安全常识、常见漏洞、热点0day事件等安全意识的培训。从个人电脑安全、邮件安全、移动安全、日常工作生活等维度进行强化参训人员的安全意识培训。服务完成后输出《安全培训材料》，一年1份。

10、协助监督检查服务

上级主管部门下发相关安全检查通知后，协助进行解读和消化，在上级主管部门检查过程中，全力配合进行人员访谈、资料准备，对被上级主管部门检查出的问题协助进行整改加固。

11、机房设备电源安全保护服务

为防止发生人员安全隐患和降低设备故障率。对机房内部相关网络，设备网络防雷、电源安全的状态、寿命、失效数据，通讯信号值、流量值、项目名称等数据进行统计分析；通过PC\手机微信功能查询告警；对设备网络防雷、电源防雷的状态、寿命、失效数据，通讯信号值、流量值、项目名称等数据进行云端存储，解决相关网络，服务器，pc设备的电源和网络线路安全保护。

PC\手机微信功能查询、告警功能支持：防雷功能寿命预警、防雷失效告警，设备GIS集中展现管理，每个设备的项目名称查询展示；设备PC\手机在线故障报修。（提供第三方检测机构的CMA检测报告佐证，原件备查）。

支持数据统计分析功能：网络防雷、电源防雷的寿命、失效，通讯信号值、流量值等的数据统计分析。（提供第三方检测机构的CMA检测报告佐证，原件备查）。

（二）等保差异化评估服务

等保差异化评估服务：提供专业的安全体系建设，制定等级保护安全整改与实施方案。 服务频率一年一次，提供《等级保护安全建议与建设方案》。

（三）计算机软硬件和网络安全设备维护服务

对总队计算机和网络安全设备进行软硬件维护服务。软硬件运维服务是针对计算机、网络安全设备和相关应用的维护和管理服务，旨在确保计算机和网络安全设备的正常运行和数据的可靠性。具体包括定期检查计算机网络安全设备的软硬件运行状态等情况，如发生故障情况及时通知用户，并在网络安全设备损坏时，提供临时备用设备。

（四）网络安全审计服务

 对总队互联网办公电脑提供全年网络安全审计服务，通过专业的服务工具对所有互联网办公电脑上网行为的日志进行记录，日志记录满足《中华人民共和国网络安全法》对日志须存满180天要求，每月日志冗余备份一次，总体日志数据保留不短于1年。

（五）视频会议系统维护服务

针对总队视频会议系统提供5\*8小时视频会议系统维护服务，包括视频会议的开机调试，使用问题的处理，日常故障的解决。

三、技术要求

1.投标人在计算机与网络安全运维服务过程中，所采用的安全服务工具可以实现用户在任意时刻只能访问一个网络，切换网络需要用户点击切换按钮，无需管理员干预，在不影响多网络使用的同时，实现网络逻辑隔离，加强网络访问安全。可支持自定义大于等于4个网络区域。（提供具备CNAS或CMA资质的第三方测试机构测试报告证明材料，至少包含报告首页，对应功能测试页和测试结果页，原件备查）

2.投标人在计算机与网络安全运维服务过程中，所采用的服务工具支持移动端通过生物特征识别用户身份，并对用户做网络控制，同时支持阻拦终端用户的相关弹窗，包括但不限于WinRAR、快压、360安全卫士、360画报、金山毒霸、热点资讯、今日热点等广告弹窗。（提供具备CNAS或CMA资质的第三方测试机构测试报告证明材料，至少包含报告首页，对应功能测试页和测试结果页，原件备查）

3.投标人在计算机与网络安全运维服务过程中，所采用的服务工具支持数据统计分析功能：网络防雷、电源防雷的寿命、失效，通讯信号值、流量值等的数据统计分析。（提供第三方检测机构的CMA检测报告）