**福建省水利厅软件源代码及供应链安全检测服务要求**

# 服务内容

建设支撑福建省水利厅对当前存量业务系统及待上线业务系统进行软件源代码及供应链安全风险检测的服务体系，健全软件源代码及供应链的安全风险评估机制，建立软件供应链安全检查措施，引导规范软件开发安全流程，持续提升存量业务系统的安全健壮性，保障福建省水利厅业务系统的安全稳定运行。

具体服务内容如下：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务名称** | **服务内容** | **服务成果** | **服务对象** | **服务频率** |
| **1** | 已建系统软件供应链安全检测服务 | 通过在水利专网部署的代码安全检测系统，定期对水利厅业务系统进行安全风险监测。利用代码安全检测系统的软件成分分析套件和静态应用安全测试套件对业务系统的组件安全和编码风险进行全面分析。同时，结合安全服务专家的专业知识和经验，对分析结果进行二次审核，确保真实、准确地识别出业务系统中存在的安全风险，并协助指导相关部门采取有效的整改措施。 | 《业务系统软件成分分析报告》  《业务系统源码安全检测报告》 | 15个业务系统 | 4次/年 |
| **2** | 在建系统上线前扫描 | 通过在水利专网部署的代码安全检测系统，对水利厅在建系统上线前进行安全风险监测，对在建系统的组件安全和编码风险进行全面分析，同时，结合安全服务专家的专业知识和经验，对分析结果进行二次审核，确保真实、准确地识别出在建系统中存在的安全风险，并协助指导相关部门采取有效的整改措施。 | 《业务系统软件成分分析报告》  《业务系统源码安全检测报告》 | 在建业务系统 | 按需（不超过3次/1年） |
| **3** | 网安检查等特殊时期扫描对所有业务系统进行扫描 | 网安检查等特殊时期，通过在水利专网部署的代码安全检测系统，对水利厅所有业务系统进行安全风险监测，对业务系统的组件安全和编码风险进行全面分析，同时，结合安全服务专家的专业知识和经验，对分析结果进行二次审核，确保真实、准确地识别出业务系统中存在的安全风险，并协助指导相关部门采取有效的整改措施。 | 《业务系统软件成分分析报告》  《业务系统源码安全检测报告》 | 15个业务系统 | 按需（不超过2次/1年） |

# 服务工具要求

1. 所使用的服务工具须为供应商自主研发的与代码安全或WEB漏洞挖掘或软件成分分析相关的系统。**（需提供相关系统的计算机软件著作权登记证书）**
2. 所使用服务工具支持C/C++、C#、Java、Python、PHP、Swift、Go、Rust、Objective-C、Node.js、Kotlin、SQL（Oracle 、SQL Server、MySQL、HiveQL等类型）、Ruby、Scala、XML、JSP、Javascript等主流编程语言开发的软件源代码的缺陷检测。
3. 所使用服务工具支持代码注入、跨站脚本、输入验证、危险函数、代码质量、API误用、密码管理、异常处理等常见安全缺陷问题的检测。并且支持自定义污点规则能力，可以根据实际开发环境导入规则。支持代码规范审计，覆盖GJB-5369-2005、GB/T-34943-2017、GJB-8114-2013编码规范。
4. 所使用服务工具支持OWASP、CERT、CVE漏洞库中严重等级较高的安全漏洞的检测，支持国际、国内相关安全编码标准的检测。
5. 所使用服务工具支持提供缺陷知识库在线查看功能，能够根据缺陷类型、关键词、威胁等级等条件进行全局搜索，分语言和类型显示该缺陷的等级、详细信息、修复建议和参考信息内容。
6. 所使用的服务工具可支持生成软件系统的物料清单，包含组件名称、版本、所属语言、作用域、风险等级、漏洞分布、修复建议、许可ID等信息。**（需提供服务工具功能截图）**
7. 所使用的服务工具可支持对查看软件系统的相关组件详情信息，包括来源、依赖类型、依赖关系、组件引入结构、组件存在的漏洞名称，CNNVD编号，CVSS编号，危险等级，升级后状态等信息。**（需提供服务工具功能截图）**
8. 所使用的服务工具可支持对代码的存在的漏洞进行检测，检测结果包含风险类型、风险代码位置、风险代码行号、风险等级、代码块等信息，能够查看与漏洞相关的污点源、摘要、详情、建议、提示、引用等信息。**（需提供服务工具功能截图）**
9. 服务采购单位有权要求供应商在签约合同前针对供应商提供的服务工具功能进行现场验证，如现场验证无法符合服务工具要求的，则中标资格无效。
10. 为保障软件系统的代码等敏感数据不泄露，供应商需书面承诺所提供的服务工具需本地部署在服务采购单位指定的网络环境中，直至服务期结束为止。**（需提供书面承诺函）**
11. 服务期为合同签订后一年。

# 人员要求

1. 供应商所提供的服务人员应具备专业的网络安全技术能力，需具备CISP及PMP相关的资质证书。**（提供人员资质证书及近六个月任意一个月的社保缴纳证明材料）**

# 其他要求

1. 为保障服务工具的稳定运行，供应商需提供每月1次的现场设备巡检服务。
2. 为保障突发重大漏洞的安全支撑，供应商需承诺根据服务采购单位实际需求提供应急响应服务。

# 保密要求

1. 供应商在提供服务期间，必须遵守国家保密相关的法律法规以及我单位保密相关的规章制度，与我单位签订保密协议，履行保密相关职责。