政府采购项目
采 购 需 求

项目名称：长岛综合试验区信息系统安全防护等级保护测评

采购单位：长岛海洋生态文明综合试验区大数据服务中心

编制单位：长岛海洋生态文明综合试验区大数据服务中心

编制时间：2024 年 9 月 20 日

一、项目概况

本次采购为长岛综合试验区信息系统安全防护等级保护测评，本项目共包含22个系统，其中三级系统5个，二级系统17个。供应商须对采购内容全部响应，报价若有遗漏，视为对本项目让利，应免费提供。

二、采购项目预算

总 预 算：69万元。

三、采购标的汇总表

包号	序号	标的名称	品目 分类编码	计量 单位	数量	是否进口
A	1	长岛综合试验区信息系统安全防护等级保护测评	C16060000	宗	1	否

四、技术商务要求

采购内容及要求

1、测评依据

公安部、国家保密局、国家密码管理局、国务院信息化工作办公室联合转发的《关于信息安全等级保护工作的实施意见》(公通字[2004]66号)

公安部、国家保密局、国家密码管理局、国务院信息化工作办公室制定的《信息安全等级保护管理办法》(公通字[2007]143号)

《信息安全技术网络安全等级保护基本要求》(GB/T22239-2019)

《信息安全技术网络安全等级保护测评要求》(GB/T28448-2019)

《信息安全技术网络安全等级保护安全设计技术要求》(GB/T25070-2019)

《信息安全技术网络安全等级保护测评过程指南》(GB/T28449-2018)

2、具体服务内容

测评的内容包括但不限于以下内容：

安全技术测评：包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心等五个方面的安全测评。

安全管理测评：安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等五个方面的安全测评。

（1）安全物理环境

根据现场安全测评记录，针对信息系统机房和现场在“物理位置选择”“物理访问控制”“防盗窃和防破坏”“防雷击”“防火”“防水和防潮”“防静电”“温湿度控制”“电力供应”和“电磁防护”等安全物理环境方面所采取的措施进行，判断出与其相对应的各测评项的测评结果。

（2）安全通信网络

根据现场安全测评记录，针对信息系统通信网络方面在“网络架构”“通信传输”“可信验证”等方面所采取的措施进行检查，判断出与其相对应的各测评项的测评结果。

（3）安全区域边界

根据现场安全测评记录，针对信息系统安全区域边界现场测评包括“边界防护”“访问控制”“入侵防范”“恶意代码和垃圾邮件防范”“安全审计”“可信验证”等边界区域防范措施进行检查。

（4）安全计算环境

根据现场安全测评记录，针对信息系统安全计算环境现场测评包括“身份鉴别”“访问控制”“安全审计”“入侵防范”“恶意代码防范”“可信验证”“数据完整性”“数据保密性”“数据备份恢复”“剩余信息保护”“个人信息保护”等几个方面的测评。

（5）安全管理中心

根据现场安全测评记录，针对信息系统安全管理中心现场测评包括“系统管理”“审计管理”“安全管理”“集中控制”等方面。

（6）安全管理制度

根据现场安全测评记录，针对信息系统在安全管理制度方面的“安全策略”“管

理制度”“制定和发布”以及“评审和修订”等测评指标，判断出与其相对应的各测评项的测评结果。

（7）安全管理机构

根据现场安全测评记录，针对信息系统在安全管理机构方面的“岗位设置”“人员配备”“授权和审批”“沟通和合作”以及“审核和检查”等测评指标，判断出与其相对应的各测评项的测评结果。

（8）安全管理人员

根据现场安全测评记录，针对信息系统在安全管理人员方面的“人员录用”“人员离岗”“安全意识教育和培训”以及“外部人员访问管理”等测评指标，判断出与其相对应的各测评项的测评结果。

（9）安全建设管理

根据现场安全测评记录，针对信息系统在安全建设管理方面的“定级和备案”“安全方案设计”“产品采购和使用”“自行软件开发”“外包软件开发”“工程实施”“测试验收”“系统交付”“等级测评”以及“服务供应商选择”等测评指标，判断出与其相对应的各测评项的测评结果。

（10）安全运维管理

根据现场安全测评记录，针对信息系统在安全运维管理方面的“环境管理”“资产管理”“介质管理”“设备维护管理”“漏洞和风险管理”“网络和系统安全管理”“恶意代码防范管理”“配置管理”“密码管理”“变更管理”“备份与恢复管理”“安全事件处置”“应急预案管理”以及“外包运维管理”等测评指标，判断出与其相对应的各测评项的测评结果。

通过现场测评，逐项找出系统现状与国家相关标准要求之间的差距，进行逐项分析、整体分析，给出差距分析报告，并给出整改建议方案。待整改完毕后，进行结果确认，完成网络安全等级保护测评，出具测评报告，并将测评报告报当地公安机关备案。

3、交付成果

项目实施完成后，要求提供包括但不限于交付物如下：

《网络安全等级保护测评报告》

其他服务要求

1、项目后续服务期限内，针对系统存在的不符合等保测评规范要求的问题整改情况，进行免费的复测、复查。

2、供应商应提供相关系统商用密码应用安全性评估、信息安全咨询和技术支持服务。

3、项目后续服务期限内，当相关法律法规和标准规范发生变化时，应对信息系统按要求进行补充或重新测试，并重新出具符合规范要求的测评报告作为补充。

4、项目后续服务期限内，应为采购人提供相关系统定级、备案、制度完善等服务，同时按采购人要求提供师资力量和场地，组织不少于 2 次网络安全培训。

5、项目后续服务期限内，如被测系统发生重大信息安全事件，需协助采购人妥善处置安全事件，并提供技术咨询服务，抵达现场时间不超过 4 小时（遇到天气原因等不可抗力原因除外），同时应针对发生重大信息安全事件的系统提供免费的重新测评。

6、攻防演练响应服务：根据应急预案和当年业界发生大重大安全事件，提供整套的网络安全应急演练服务，包括快速分析与侦查、快速取证与隔离等；为了提高采购人管理人员的安全能力和意识，根据采购人要求，供应商的应急响应服务人员在服务期内针对热点问题组织网络安全演练并提供相应报告。

7、网络安全巡检服务：根据采购人要求，能够提供不少于 2 名 技术支持人员对被测系统进行每半年至少一次安全巡检服务。

8、保障服务：在重要保障时期，能够提供技术人员现场支持。

9、按照采购人要求，完成其他相关安全技术服务。

10、供应商需投入种类齐全、数量充足的测评设备、设施，确保项目梳理实施。

11、供应商应对项目进行重点、难点分析并配备相应解决措施，制定完善的质量控制措施、进度控制措施，确保项目顺利实施。

12、供应商可根据自身情况及项目实际提出切实可行、具有针对性的增值服务，符合有利于项目实施的原则。