采购需求

一、项目名称

项目名称：2021 年临高县网络安全等级保护测评及安全服务项目

二、项目背景

通过委托专业的网络安全等级保护测评服务机构，对用户方的信息系统安全保护等级进行需求分析，并协助用户方完成等保备案相关事宜。依据《信息安全技术 网络安全等级保护基本要求》（GBT2223902019），对信息系统的物理机房、网络结构、应用系统、主机、网络及安全设备等进行合规性检查，分析信息系统与安全保护等级要求之间的差距，出具《网络安全等级保护测评报告》，并对相关单位提供应急响应、内网威胁分析、应急演练服务。

三、项目工期和地点

合同履行期限：自用户通知进场起 60 个工作日内

交付内容：交付《网络安全测评报告》、《内网威胁分析报告》、《信息安全事件应急预案》和《信息安全事件应急演练总结评估报告》。

地点：临高县。

四、项目需求

4.1 网络等级保护测评服务内容

4.1.1 服务范围

序号	单位名称	信息系统名称	级别
1	县公安局	视频督查系统	二级
2		三台合一接处警系统	二级
3		视频图像信息共享平台	二级

4		DSS-智能交通系统	二级
5		执法记录仪信息综合管理系统（交警）	二级
6		执法记录仪信息综合管理系统（公安局）	二级
7		SIS 信息系统	二级
8		临高县看守所视频监控管理系统	二级
9		临高县强制戒毒所视频监控管理系统	二级
10	县政法委	临高县社会治理综合信息平台	三级
11	县人民法院	法院办公专网	三级
12	县水务局	山洪灾害监测预警系统	二级
13	县旅游和文化广电体育局	应急广播系统	二级
14	县融媒体中心	融媒体平台	三级
15	县财政局	财政专网	二级
16	临高县生态环境局	尾气遥感监测系统	二级
17	临高县环境监测站	环境空气质量自动检测系统	二级
18	县自来水公司	水费收费系统	二级

4.1.2 服务内容

依据《信息安全等级保护管理办法》（公通字[2007]43 号）规定，以及根据公安部和海南省公安厅网络监察职能部门的建议和要求，第二级信息系统应当每两年至少进行一次等级测评，第三级信息系统应当每年至少进行一次等级测评，第四级信息系统应当每半年至少进行一次等级测评，第五级信息系统应当

依据特殊安全需求进行等级测评。

单位将聘请具有公安部认可的信息安全等级保护测评资质的测评机构对临高县 10 家单位，其中三级系统 3 个，二级系统 15 个开展测评工作，具体工作内容如下：

1、对被测的信息系统进行摸底、分析和梳理，提出详细的测评方案及完成系统备案工作。

2、逐一对信息系统进行安全等级保护测评，测评的内容包括但不限于以下内容：

（1）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；

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

4.1.3 结果输出

出具《网络安全保护等级测评报告》。

4.2 应急响应服务内容

4.2.1 服务范围

应急响应服务：全县	
单位	服务次数
全县	提供 2021 年 10 次应急响应服务

4.2.2 服务内容

根据等级保护《基本要求》的“安全事件处置”的要求，当信息系统安全事件发生时，指导全县进行信息安全事件应急响应服务（提供总数为 10 次应急响应服务），同时，将针对内网监测发现的问题，提供应急响应服务，及时解决

内网存在的安全问题，及时排除安全隐患通过应急响应对安全事件发生的信息系统进行安全事故分析，以及时解决安全故障、修复系统，最大限度的保护服务器和数据，最快的速度恢复访问和网络畅通，使信息系统恢复正常工作，尽可能挽回或减少损失。

紧急事件响应服务主要对如下安全事件做出响应：

- 计算机病毒事件
- 蠕虫病毒事件
- 特洛伊木马事件
- 网页内嵌恶意代码事件
- 拒绝服务攻击事件
- 后门攻击事件
- 漏洞攻击事件
- 网络扫描窃听事件
- 信息篡改事件

具体内容详见下表：

序号	服务项目	服务内容	服务说明	服务对象	主要成果文档	服务类型
1	应急响应	应急响应	在信息系统安全事件发生时，对安全事件发生的信息系统进行安全事故分析，并协助及时解决安全故障、修复系统，最大限度的保护服务器和数据，最快的速度恢复访问和网络畅通，使信息系统恢复正常工作，尽可能挽回或减少损失。	安全事件	《应急响应处理报告》	远程服务现场服务

4.2.3 结果输出

一旦全县某单位发生安全事件，做好有力的技术扩充与支持保障，帮助及时控制安全事件造成的恶劣影响，帮助找到问题的根源，防止后续同类事件的发生。出具《应急响应处理报告》。

4.3 内网威胁分析服务内容

4.3.1 服务范围

内网威胁分析服务：针对业务比较重要 6 家单位开展内网威胁分析服务	
序号	单位
1	县公安局
2	县政法委
3	县人民法院
4	县党政信息中心
5	县人民医院
6	县医院

4.3.2 服务内容

内网是一个部署有服务器、网络设备、PC 终端、移动终端等多元化信息系统架构的区域，是距离用户核心信息资产最接近的地方，加上内网的使用人员众多、计算机管理水平良莠不齐，因而内网也是面临安全威胁最大的区域。

对于多数信息安全管理者而言，现有的网络安全防护手段大多强调对来自外部的主动攻击进行预防、检测以及处理，而授予了内部主机及用户更多的信任和权限。然而堡垒最容易从内部突破，近些年统计的数据表明，相当多的安全事件是从内网而产生的；这通常是由于内网用户有意或无意的违规操作，使得某台服务器或终端设备被黑客、病毒渗透入侵，黑客利用一台设备作为跳板对整个内网进行漫游渗透，进而发生数据泄露、设备窃听、病毒传播、服务器宕机、网络瘫痪等等恶性事件的发生。

为保护内网的安全，一些单位将内网与外网物理隔离，或者将内部通过统一的网关接入外网，并在网关处架设防火墙、IPS、IDS 等安全监控设备，尽管各单位都加强了对内网的安全管理，可内网安全事件仍时有发生，这充分说明

了内网安全监测的复杂性以及内网安全分析的重要性。

针对业务比较重要内网威胁服务的实施。

4.3.3 结果输出

输出《内网威胁分析报告》

4.4 应急演练服务内容

4.4.1 服务范围

应急演练服务：对县 12 家单位开展应急演练服务	
序号	单位
1	临高县公安局
2	县政法委
3	县人民法院
4	县水务局
5	县旅游和文化广电体育局
6	县融媒体中心
7	县财政局
8	临高县生态环境局
9	县气象局
10	县党政信息中心
11	县中医院
12	县人民医院

4.4.2 服务内容

应急演练(应急预案+演练)服务将根据《中华人民共和国突发事件应对法》、《突发事件应急预案管理办法》、GB／T 22239-2019《信息安全技术网络安全等级保护基本要求》、GB／T 38645-2020《信息安全技术 网络安全事件应急演练指南》、《中华人民共和国网络安全法》、《海南省信息化条例》和《关于印发海南省党政机关、事业单位和国有企业互联网网站安全专项整治行动方案的通知》等文件对“信息安全事件应急响应、应急预案和应急演练”的相关规定，结合信息系统的实际情况，指导建立健全信息与网络安全事件应急响应工作机制，完成编制《信息安全事件应急预案》，并对信息系统相关人员进行应急预案、应急技巧及对典型的信息安全事件进行预防等方面的培训，并针对《信息安全事件应急预案》开展相应的应急演练工作。

信息安全事件应急预案演练主要对运行环境安全、网络结构安全、设备运行安全、系统可用性、外界风险因素等各方面进行全面演练，主要覆盖重要信息系统、数据中心、灾备中心等重要基础设施，重要服务商应急保障能力，外部应急协调机制等。

做到全面演练和专项演练相结合。应急演练应贴合信息系统的实际情况，主要的演练方式为模拟演练及桌面演练。

演练场景以可能出现的通讯故障、系统故障、系统安全等为重点，结合实际情况和关键风险点，设计以下应急场景进行演练:

- **通讯故障：**演练在流量激增、网络设备故障、通信线路被破坏、网络受到攻击等原因导致通讯中断和拥塞时的应急预案以及与公安、电信部门的应急协调与保障机制。
- **系统安全：**演练因病毒爆发、网络入侵攻击、篡改网站等情形下的系统应急预案以及与公安、电信部门的应急协调机制。
- **系统故障：**主要演练主要信息系统出现应用故障、数据库故障、存储设备故障、主机硬件故障等的应急预案以及外联单位、系统重要服务商的应急协调与保障能力；检验外联单位相关系统的应急保障能力。

4.4.3 结果输出

输出《信息安全事件应急预案》、《信息安全事件应急演练总结报告》

五、项目服务要求

5.1. 项目实施要求

项目实施过程中，供应商应遵循国家标准、行业标准。

在项目实施中供应商须做到：

1. 本项目的项目经理必须具有 2 年以上的等保测评服务项目管理经验；其中，本项目成员中至少有 1 人具备信息安全等级保护中级测评师资格；

2. 提供完整的系统实施方案和项目实施管理办法；

3. 提供详细的项目实施方案和计划进度说明书；

4. 提供详细、全面的人员培训计划和实施方案；

5. 项目实施完成后提供可靠的后期技术服务工作；

6. 严格按照双方确定的计划进度保质保量完成工作；

7. 规范项目实施过程中的文档管理；

5.2 项目验收要求

中标人必须提供给业主详细的项目验收方案。

中标人必须书面通知业主所完成的工作和准备进行验收的项目种类及验收开始时间，此通知书需经业主认定后方可执行。

5.3 验收交付物

1）提交《网络安全等级保护测评报告》，每个被测系统一份；

2）提交《内网威胁分析报告》，业务比较重要 6 家单位各一份；

3）提交《信息安全事件应预案》和《信息安全事件应急演练总结报告》12 家单位各一份。

5.4 售后服务要求

对于评估中发现的应用系统、主机和网络设备漏洞，投标方应提供项目验收后一年内的跟踪服务，对本次评估范围内的问题提供远程或现场技术咨询，对于漏洞的修补、问题的排除给出建议和指导。

六、项目服务明细表

序号	服务内容	系统级别	数量	单位	备注
1	**等保测评服务**	二级	15	个	测评内容包括：物理安全、网络安全、主机安全、应用安全、数据安全与备份恢复、安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理测评内容
		三级	3	个	
2	**应急响应服务**		10	次	提供总数为 10 次应急响应服务。在被测单位信息系统安全事件发生时，对安全事件发生的信息系统进行安全事故分析，并协助及时解决安全故障、修复系统，最大限度的保护服务器和数据，最快的速度恢复访问和网络畅通，使信息系统恢复正常工作，尽可能挽回或减少损失
3	**内网威胁分析服务**		6	家	内部的主机、应用系统及终端进行漏洞扫描、APT 分析、数据分析、木马分析、蠕虫分析等，检测内网中是否存有 APT 攻击、木马蠕虫、恶意文件、后门等相关

					安全威胁
4	**应急演练服务**		12	家	编制《信息安全事件应急预案》，并对信息系统相关人员进行应急预案、应急技巧及对典型的信息安全事件进行预防等方面的培训，并针对《信息安全事件应急预案》开展相应的应急演练工作