第二章、采购需求

F 包-海口市自然灾害综合监测预警指挥平台项目网络安全服务

一、商务要求

1、交付时间：自合同签订生效之日起 1 年内，完成采购需求项下所有安全服务内容并提交服务成果，若因平台建设时间延误导致安全服务无法正常开展，则按照平台延误时间对安全服务周期进行顺延。

2、交付地点：用户指定地点。

3、交付方式：免费送至用户指定地点。

4、采购资金的支付方式、时间、条件：

4.1 合同签订完成后 15 个工作日内，支付至合同金额 50%；

4.2 服务完成交付项目成果经采购人确认后，支付至合同金额 80%。

4.3 项目通过海口市财政局结算审核后，按实际结算金额支付项目尾款。

5、验收要求：按标书服务要求和国家行业标准进行验收。

二、技术要求

1、标包名称

海口市自然灾害综合监测预警指挥平台项目（F 包二次招标）

2、服务内容及要求

网络安全服务矩阵表

编号	项目	系统名称	安全服务内容
1	海口市自然灾害综合监测预警指挥平台项目	综合监测预警与联动处置可视化系统	1、安全风险评估服务 2、安全代码审计服务 3、渗透测试服务 4、安全管理制度编制服务 5、计算环境安全加固服务 6、安全培训服务
2		城市内涝综合风险监测预警系统	1、安全风险评估服务 2、安全代码审计服务 3、渗透测试服务 4、安全管理制度编制服务 5、计算环境安全加固服务

编号	项目	系统名称	安全服务内容
			6、安全培训服务
3		涉自然灾害桥梁临灾安全监测预警系统	1、安全风险评估服务 2、安全代码审计服务 3、渗透测试服务 4、安全管理制度编制服务 5、计算环境安全加固服务 6、安全培训服务
4		涉自然灾害燃气临灾安全监测预警系统	1、安全风险评估服务 2、安全代码审计服务 3、渗透测试服务 4、安全管理制度编制服务 5、计算环境安全加固服务 6、安全培训服务
5		涉自然灾害供水临灾安全监测预警系统	1、安全风险评估服务 2、安全代码审计服务 3、渗透测试服务 4、安全管理制度编制服务 5、计算环境安全加固服务 6、安全培训服务
6		城市气象防灾减灾保障系统	1、安全风险评估服务 2、安全代码审计服务 3、渗透测试服务 4、安全管理制度编制服务 5、计算环境安全加固服务 6、安全培训服务
7		市区厂站网河监控	1、安全风险评估服务 2、安全代码审计服务 3、渗透测试服务 4、安全管理制度编制服务 5、计算环境安全加固服务 6、安全培训服务

安全服务频次及方式表

编号	安全服务名称	服务频次	服务方式
1	安全风险评估服务	每个系统半年 1 次，共计 2 次	现场
2	安全代码审计服务	每个系统每年 4 次	现场
3	渗透测试服务	每个系统每年 1 次	现场
4	安全管理制度编制服务	/	现场

5	计算环境安全加固服务	每个系统每年 1 次	现场
6	安全培训服务	每个系统半年 1 次，共计 2 次	现场
7	攻防演练和网络安全重大保障服务	根据业主要求，每年每系统提供不少于 2 次攻防演练和重大活动服务保障	现场

2.1 安全风险评估服务

项目组依据《信息安全技术 信息安全风险评估规范》（GB/T 20984-2007）、《信息安全技术 信息系统安全保障评估框架》（GB/T 20274-2008）等国家风险评估工作相关规范和标准，对云公司云平台或资源池进行风险评估工作。风险评估流程具体包括风险评估准备、资产识别、威胁识别、脆弱性识别、风险分析以及风险评估文件记录。

2.1.1 风险评估准备

组织实施风险评估是一种战略性的考虑，其结果将受到组织业务战略、业务流程、安全需求、系统规模和结构等方面的影响。因此在风险评估实施前，应：

（1）确定风险评估的目标。

（2）确定风险评估的范围。

（3）组建适当的评估管理与实施团队。

（4）进行系统调研。

（5）确定评估依据和方法。

（6）获得最高管理者对风险评估工作的支持。

2.1.2 资产识别

（1）资产分类

机密性、完整性和可用性是评价资产的三个安全属性。风险评估中资产的价值不是以资产的经济价值来衡量，而是由资产在这三个安全属性上的达成程度或者其安全属性未达成时所造成的影响程度来决定的。

在一个组织中，资产有多种表现形式；同样的两个资产也因属于不同的信息系统而重要性不同，而且对于提供多种业务的组织，其支持业务持续运行的系统数量可能更多。这时首先需要将信息系统及相关的资产进行恰当的分类，以此为基础进行下一步的风险评估。在实际工作中，具体的资产分类方法可以根据具体的评估对象和要求，由评估者灵活把握。根据资产的表现形式，可将资产分为数据、软件、硬件、服务、人员等类型。

（2）资产赋值

1）保密性赋值

根据资产在保密性上的不同要求，将其分为五个不同的等级，分别对应资产在保密性上应达成的不同程度或者保密性缺失时对整个组织的影响。

2）完整性赋值

根据资产在完整性上的不同要求，将其分为五个不同的等级，分别对应资产在完整性上缺失时对整个组织的影响。

3）可用性赋值

根据资产在可用性上的不同要求，将其分为五个不同的等级，分别对应资产在可用性上应达成的不同程度。

4）资产重要性等级

资产价值应依据资产在机密性、完整性和可用性上的赋值等级，经过综合评定得出。综合评定方法可以根据自身的特点，选择对资产机密性、完整性和可用性最为重要的一个属性的赋值等级作为资产的最终赋值结果；也可以根据资产机密性、完整性和可用性的不同等级对其赋值进行加权计算得到资产的最终赋值结果。加权方法可根据组织的业务特点确定。

2.1.3 威胁识别

（1）威胁识别

威胁可以通过威胁主体、资源、动机、途径等多种属性来描述。造成威胁的因素可分为人为因素和环境因素。根据威胁的动机，人为因素又可分为恶意和非恶意两种。环境因素包括自然界不可抗的因素和其它物理因素。威胁作用形式可以是对信息系统直接或间接的攻击，在机密性、完整性或可用性等方面造成损害；

也可能是偶发的、或蓄意的事件。

（2）威胁赋值

判断威胁出现的频率是威胁赋值的重要内容，评估者应根据经验和（或）有关的统计数据来进行判断。在评估中，需要综合考虑以下三个方面，以形成在某种评估环境中各种威胁出现的频率：

1）以往安全事件报告中出现过的威胁及其频率的统计；

2）实际环境中通过检测工具以及各种日志发现的威胁及其频率的统计；

3）近一两年来国际组织发布的对于整个社会或特定行业的威胁及其频率统计，以及发布的威胁预警。

可以对威胁出现的频率进行等级化处理，不同等级分别代表威胁出现的频率的高低。等级数值越大，威胁出现的频率越高。

2.1.4 脆弱性识别

（1）脆弱性识别

脆弱性识别是风险评估中最重要的一个环节。脆弱性识别可以以资产为核心，针对每一项需要保护的资产，识别可能被威胁利用的弱点，并对脆弱性的严重程度进行评估；也可以从物理、网络、系统、应用等层次进行识别，然后与资产、威胁对应起来。脆弱性识别的依据可以是国际或国家安全标准，也可以是行业规范、应用流程的安全要求。对应用在不同环境中的相同的弱点，其脆弱性严重程度是不同的，评估者应从组织安全策略的角度考虑、判断资产的脆弱性及其严重程度。信息系统所采用的协议、应用流程的完备与否、与其他网络的互联等也应考虑在内。

脆弱性识别时的数据应来自于资产的所有者、使用者，以及相关业务领域和软硬件方面的专业人员等。脆弱性识别所采用的方法主要有：问卷调查、工具检测、人工核查、文档查阅、渗透性测试等。

（2）脆弱性赋值

可以根据对资产的损害程度、技术实现的难易程度、弱点的流行程度，采用等级方式对已识别的脆弱性的严重程度进行赋值。由于很多弱点反映的是同一方面的问题，或可能造成相似的后果，赋值时应综合考虑这些弱点，以确定这一方

面脆弱性的严重程度。

对某个资产，其技术脆弱性的严重程度还受到组织管理脆弱性的影响。因此，资产的脆弱性赋值还应参考技术管理和组织管理脆弱性的严重程度。

脆弱性严重程度可以进行等级化处理，不同的等级分别代表资产脆弱性严重程度的高低。等级数值越大，脆弱性严重程度越高。

2.1.5 已有安全措施确认

在识别脆弱性的同时，评估人员应对已采取的安全措施的有效性进行确认。安全措施的确认应评估其有效性，即是否真正地降低了系统的脆弱性，抵御了威胁。对有效的安全措施继续保持，以避免不必要的工作和费用，防止安全措施的重复实施。对确认为不适当的安全措施应核实是否应被取消或对其进行修正，或用更合适的安全措施替代。

2.1.6 风险分析

（1）风险计算原理

在完成了资产识别、威胁识别、脆弱性识别，以及对已有安全措施确认后，将采用适当的方法与工具确定威胁利用脆弱性导致安全事件发生的可能性。综合安全事件所作用的资产价值及脆弱性的严重程度，判断安全事件造成的损失对组织的影响，即安全风险。

（2）风险结果判定

为实现对风险的控制与管理，可以对风险评估的结果进行等级化处理。可以将风险划分为五级，等级越高，风险越高。应根据所采用的风险计算方法，计算每种资产面临的风险值，根据风险值的分布状况，为每个等级设定风险值范围，并对所有风险计算结果进行等级处理。每个等级代表了相应风险的严重程度。

（3）风险处理计划

对不可接受的风险应根据导致该风险的脆弱性制定风险处理计划。风险处理计划中明确应采取的弥补弱点的安全措施、预期效果、实施条件、进度安排、责任部门等。安全措施的选择应从管理与技术两个方面考虑。安全措施的选择与实

施应参照信息安全的相关标准进行。

（4）残余风险评估

在对于不可接受的风险选择适当安全措施后，为确保安全措施的有效性，可进行再评估，以判断实施安全措施后的残余风险是否已经降低到可接受的水平。残余风险的评估可以依据本标准提出的风险评估流程实施，也可做适当裁减。一般来说，安全措施的实施是以减少脆弱性或降低安全事件发生可能性为目标的，因此，残余风险的评估可以从脆弱性评估开始，在对照安全措施实施前后的脆弱性状况后，再次计算风险值的大小。

2.1.7 风险评估文档记录

风险评估文档是指在整个风险评估过程中产生的评估过程文档和评估结果文档。

2.2 安全代码审计服务

源代码安全审计是依据 CVE（Common Vulnerabilities&Exposures）公共漏洞字典表、OWASP 十大 Web 漏洞（Open Web Application Security Project），以及设备、软件厂商公布的漏洞库，结合专业源代码扫描工具对各种程序语言编写的源代码进行安全审计。能够为客户提供包括安全编码规范咨询、源代码安全现状测评、定位源代码中存在的安全漏洞、分析漏洞风险、给出修改建议等一系列服务。

2.2.1 服务内容

针对系统开发过程中的编码阶段、测试阶段、交付验收阶段、对各阶段系统源代码进行安全审计检测，利用数据流分析引擎、语义分析引擎、控制流分析引擎等技术，采用专业的源代码安全审计工具对源代码安全问题进行分析和检测并验证，从而对源代码安全漏洞进行定级，给出安全漏洞分析报告等，帮助开发软件人员统计和分析当前阶段软件安全的风险、趋势，跟踪和定位软件安全漏洞，提供软件安全质量方面的真实状态信息。

2.2.2 服务报告

《系统源代码代码审计报告》

2.3 渗透测试服务

在大数据办允许下和可控的范围内，采取可控的，不造成不可弥补损失的黑客入侵手法，对城市网络和系统发起模拟攻击。目的是侵入系统并获取机密信息，并入侵的过程和细节产生报告给大数据办。渗透测试是一种从攻击者的角度来对信息系统的安全程度进行安全评估的手段，在对现有信息系统不造成任何损害的前提下，模拟入侵者对指定系统进行攻击测试。渗透测试通常能以非常明显，直观的结果来反映出系统存在的脆弱点。

通过定期对网信办信息系统进行渗透性测试，以便找出漏洞并加以改进。渗透性测试服务一般包括三类：

应用程序渗透：对渗透目标提供的各种应用，如 ASP、CGI、JSP、PHP 等组成的 WWW 应用进行渗透测试。

设备漏洞扫描及渗透测试：包括网络、主机、网络设备端和安全设备的端口、漏洞扫描，对各种安全设备、网络设备、主机等进行渗透测试。

系统渗透测试：包括操作系统、数据库系统的渗透测试。根据被测应用系统部署的服务器操作系统，包括 Windows、Solaris、AIX、Linux 等。数据库包括 MS-SQL、MySQL、Informix、Sybase、DB2 等。

为保证渗透测试服务质量，服务机构应具备一定的项目经历，如曾参与公安、网信等部门组织的网络攻防、护网行动等。

2.4 安全管理制度编制服务

依据《网络安全等级保护基本要求》及组织网络安全管理工作的特点从安全策略、管理制度、制定和发布以及评审和修订等方面进行安全管理制度设计。

制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。

对安全管理活动中的各类管理内容建立安全管理制度，对管理人员或操作人员执行的日常管理操作建立操作规程，形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系，从而指导并有效地规范各级部门的信息安全管理工作。

由海口市应急管理局领导层指定或授权专门的部门或人员负责安全管理制度的制定，安全管理制度通过正式、有效的方式发布，并进行版本控制。

安全策略系列文档制定后，必须有效发布和执行。发布和执行过程中除了要得到管理层的大力支持和推动外，还必须有合适的、可行的发布和推动手段，同时在发布和执行前对每个人员都要做与其相关部分的充分培训，保证每个人员都知道和了解与其相关部分的内容。

信息安全领导小组应组织相关人员对信息安全策略体系文件进行评审，并确定其有效执行期限。同时应指定信息安全职能部门每年审视安全策略系列文档。

2.5 计算环境安全加固服务

根据网络安全基础设施建设需求和网络安全等级保护工作需求，在客户允许的前提下，为客户完全、彻底地堵住这些安全缺陷和漏洞、去除这些薄弱环节。包括打补丁、停止不必要的服务、升级或更换程序、除去特洛伊后门程序、网络安全设备的安全配置，网络安全设备的安全加固，网络安全设备的优化配置、修改配置及权限以及针对复杂问题的专门解决方案。

评估加固的范围主要是系统中的主机系统和网络设备，以及相关的数据库系统等。安全加固服务主要以人工的方式实现。主要有：

基于网络层的加固。主要包括传输链路安全加固和网络拓扑结构的合理性检查。

服务器加固。主要包括对 Windows 服务器和 Unix 服务器的评估加固，其中还包括对服务器操作系统层面的评估和数据库层面的评估加固。

网络设备加固。主要包括对路由器，交换机的评估加固。

安全防护系统加固。主要包括防火墙系统、入侵检测系统、防病毒系统等的加固。

应用系统开发优化。主要包括应用系统的开发优化、应用服务加固及数据系

统加固。

其他需要安全加固的系统等。

消除等级保护测评中以下网络安全、主机安全问题。

2.6 安全培训服务

包含安全意识培训、安全技术培训、安全管理培训等，针对海口市应急管理局中不同的受众（包括单位领导、各业务处室、信息系统主管领导、工作人员等），提供不同层面的培训课程集中培训。

3、成果交付

3.1《安全风险评估报告》

3.2《系统源代码代码审计报告》

3.3《渗透测试服务报告》

3.4《信息安全工作总体方针》

3.5《信息安全管理机构职责》

3.6《安全管理制度制定和发布》

3.7《信息安全管理体系评审与修订》》

3.8《计算环境安全加固服务报告》

3.9《培训计划》、《培训资料》