附件 1

中华预防医学会网络安全等级保护测评服务项目采购文件

一、项目背景

为创建安全健康的网络环境，保护公众利益，促进中华预防医学会业务的深入发展，切实保障网络安全稳定运行，需要引入专业安全服务商为中华预防医学会提供等级保护合规咨询服务，保障集信息系统合法合规，整体提高信息安全保障能力。同时结合国际、国内的政策标准和最佳实践，采用科学的信息安全方法，依照中华预防医学会自身的网络安全实际情况，逐步或周期性地完善和健全信息安全防护体系。

二、技术需求

（一）服务范围

对中华预防医学会的 8 个信息系统进行定级备案及等级保护测评工作，具体内容如下：

1.拟定为三级等保系统。

（1）中华预防医学会会员系统、会议系统；

（2）中华预防医学会继续医学教育管理系统；

（3）中华预防医学会科学技术奖评审系统；

（4）社会组织参与艾滋病防治基金网站；

（5）社会组织参与艾滋病防治基金 NGO Fund（APP）。

2.拟定为二级等保系统。

（1）中华预防医学会官网；

（2）中华预防医学会办公协同系统（OA）；

（3）中华预防医学会系列期刊网站。

（二）交付成果

结项后提供中华预防医学会的8个信息系统包含但不限于以下材料：

序号	服务阶段	交付物
1	定级备案	《备案表》 《定级报告》 《专家评审意见》 《其他备案材料》
2	差距分析	《信息系统差距分析报告》
3	整改协助	《信息系统整改建议》
4	等级保护测评	《网络安全等级保护测评报告》

（三）服务内容

1.定级备案。

依照《关于开展全国重要信息系统安全等级保护定级工作的通知（公信安〔2007〕861号）》《信息安全等级保护备案实施细则（公信安〔2007〕1360号）》《信息安全技术 网络安全等级定级指南》《安全等级保护划分准则》等国家政策标准，根据中华预防医学会信息系统的业务信息安全和系

统服务安全情况及与之相关的受侵害客体和对客体的侵害程度可能不同，确定中华预防医学会信息系统的安全等级；指导相关人员编制未备案系统的定级报告，聘请专家进行专家评审，定级备案材料的准备等。具体要求如下：

（1）审核中华预防医学会信息系统初步确定的安全等级，提出审核意见。

（2）针对已确定安全等级但尚未备案的信息系统，编写系统定级报告。

（3）聘请专家（专家组由一名高级测评师，两名安全专家组成）对系统定级进行评审，出具专家评审意见，并上报行业主管部门或上级主管部门审核后到公安机关备案。

（4）协助完成定级备案材料准备。

（5）协助完成信息系统备案工作。

（6）交付本服务阶段要求的交付物。

2.差距分析。

信息系统安全等级保护差距分析将根据《信息安全技术 网络安全等级保护测评要求》、《信息安全技术 网络安全等级保护测评过程指南》等标准文件的要求，对已定级信息系统，进行系统现状调研，逐项进行合规性检测。其实质是采用基线安全分析的方法，明确当前信息系统与等级保护要求的不符合项及差距。

（1）依据信息系统定级情况，对信息系统的各项安全指标进行符合性评估，标识信息系统的不符合项，明确信息系统与等级保护基本要求之间的差距。

（2）明确信息系统当前安全防护情况，了解系统的基本安全状况和防护能力，了解现有安全措施和设备发挥作用的情况，管理体系的健全程度。同时，针对所发现的不符合项提出安全整改建议，从而指导信息系统开展整改加固工作。

（3）交付本服务阶段要求的交付物。

3.整改协助。

根据信息系统的初测结果，对信息系统从安全管理规范和安全技术规范两个方面来进行等级保护整改方案设计，为协助和指导整改加固实施提供依据。

根据信息系统安全等级保护基本要求、安全需求分析报告、机构总体安全策略文件等，提出系统需要实现的安全技术措施，形成机构特定的系统安全技术体系结构，用以指导信息系统分等级保护的具体实现，具体活动内容包括：

（1）（网络）规定目标系统网络的安全保护技术措施：根据机构总体安全策略文件、等级保护基本要求和安全需求，提出网络的安全保护策略和安全技术措施。目标系统网络的安全保护策略和安全技术措施提出时应考虑网络线路和网络设备共享的情况，如果不同级别的子系统通过目标系统网络的同一线路和设备传输数据，线路和设备的安全保护策略和安全技术措施应满足最高级别子系统的等级保护基本要求。

（2）（系统互联）规定子系统之间互联的安全技术措施：根据用户总体安全策略文件、等级保护基本要求和安全需求，提出跨局域网互联的子系统之间的信息传输保护策略要求

和具体的安全技术措施，包括同级互联的策略、不同级别互联的策略等；提出局域网内部互联的子系统之间的信息传输保护策略要求和具体的安全技术措施，包括同级互联的策略、不同级别互联的策略等。

（3）（边界）规定不同级别子系统的边界保护技术措施：根据用户总体安全策略文件、等级保护基本要求和安全需求，提出不同级别子系统边界的安全保护策略和安全技术措施。子系统边界安全保护策略和安全技术措施提出时应考虑边界设备共享的情况，如果不同级别的子系统通过同一设备进行边界保护，这个边界设备的安全保护策略和安全技术措施应满足最高级别子系统的等级保护基本要求。

（4）（安全计算环境）规定不同级别子系统内部系统平台和业务应用的安全保护技术措施：根据用户总体安全策略文件、等级保护基本要求和安全需求，提出不同级别子系统内部网络平台、系统平台和业务应用的安全保护策略和安全技术措施。

（5）（基础环境）规定不同级别信息系统机房的安全保护技术措施：根据用户总体安全策略文件、等级保护基本要求和安全需求，提出不同级别信息系统机房的安全保护策略和安全技术措施。信息系统机房安全保护策略和安全技术措施提出时应考虑不同级别的信息系统共享机房的情况，如果不同级别的信息系统共享同一机房，机房的安全保护策略和安全技术措施应满足最高级别信息系统的等级保护基本要求。

（6）形成信息系统安全技术体系结构：将目标系统网络、通过目标系统网络的子系统互联、局域网内部的子系统互联、子系统的边界、子系统内部各类平台、机房以及其他方面的安全保护策略和安全技术措施进行整理、汇总，形成信息系统的安全技术体系结构。

（7）（管理体系）从安全管理制度、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方面设计整改方案。

（8）交付本服务阶段要求的交付物。

4.等级保护测评。

根据《信息安全技术 网络安全等级保护测评过程指南》GT/T 28449-2018，通过测评准备活动、方案编制活动、现场测评活动、报告编制活动4个阶段完成等级保护测评工作：

（1）测评准备活动：主要是准备个方面测评表单及工具，采集系统信息，客户主要提供系统基本信息配合测评人员完成前期系统调研工作。

（2）方案编制活动：主要是根据定级结果确定测评指标、测评对象、工具接入点等工作，客户只需对结果进行确定。

（3）现场测评活动：主要是根据选定指标和对象进行等级保护测评，主要从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全系统建设、安全系统运维等10个方面进行现场测，并对系统进行漏洞扫描，记录

结果，客户只需配合技术人员完成技术测评和提供所有相关制度。

（4）报告编制活动：根据测评现场测评结果从单项测评、单元测评、整体测评进行安全问题风险分析，形成最终测评结论，完成测评报告。

（5）交付本服务阶段要求的交付物。

三、供应商资格要求及其它

（一）基本情况

1.供应商简介。

2.提供供应商财务近三年状况和负债情况。

3.提供 2018 年 1 月之后的信息系统等级保护测评项目成功案例。

（二）资质条件

1.提供网络安全等级保护测评机构推荐证书（若无法提供，将作无效处理）；

2.提供 ISO9001 质量管理体系认证证书；

3.提供 ISO27001 信息安全管理体系认证证书；

4.提供 14001 环境管理体系认证证书；

5.提供 45001 职业健康安全管理体系认证证书；

6.提供信息安全风险评估二级及以上服务资质证书。

（三）服务人员要求

参与本项目实施必须配备项目经理和项目成员组成的专业队伍：

1.项目实施团队人员数量大于 7 人（含），全部具备等

级保护测评师资质。

2.拟派的项目经理需具备3年以上项目经验，同时具备中级以上测评师证书、CISP、公安部信息安全等级保护评估中心联合中关村信息安全测评联盟颁发的国家重要信息系统保护人员证书等证书。

3.上述项目经理和项目组成员需提供单位个人社保证明。

4.供应商认为其他需要提供的材料。