信息安全保障人员认证

关于举办《CISAW 应急处理与服务专业级》认证培训班的通知

各相关单位：

为尽可能降低疫情对国家信息安全保障人才队伍建设的影响，信息安全保障人员认证（CISAW）“应急管理与服务”培训拟通过线上钉钉直播结合线下面授的方式开展。现将培训的具体模式通知如下：

一、 培训培训与考试模式

阶段	培训模式	课程内容	课时
第一阶段	在线直播与互动	理论讲解 + 云端环境实操	18 课时/3 天
第二阶段	现场面授	沙盘演练 + 实操	9 课时/1.5 天
考试阶段	现场	笔试 + 实操考试	3 小时

1）在线直播与互动通过“钉钉课堂”采取线上直播方式开展；

2）第一阶段 6 月 27-29 日；第二阶段：待定；考试阶段：现场培训后即组织考试；

线下地址：广州市环市东路 326 号广东亚洲国际大酒店 19 楼报告厅

二、 课程介绍

CISAW 应急管理与服务认证课程根据《信息安全保障人员认证考试大纲》的要求，融合当前国内外的网络安全态势、业内专家的应急响应实战经验，并借助包含网络安全最新攻防技术的“红黑演义应急响应演练云平台”，理论结合实践向学员授课。课程内容既包括应急管理体系规划与管理实践及案例分享的理论课程，又包括让每位学员

在云端实验环境中运用红方、黑方攻防对抗技术，从正反两方面开展实战演练的实操课程。让学员充分了解和掌握应急管理的知识体系和实战技术，切实提升学员网络安全应急管理和技术能力，成为国家信息安全保障人才队伍中的一员。具体课程内容可参照“附件 1”。

三、 培训对象

CISAW 应急管理与服务培训适合政府部门、企事业单位的信息技术领域从业人员，特别是与网络安全、信息安全密切相关的中高级管理人员、技术人员、专业运维人员和其他相关人员。

四、 培训费用

（1）培训费 6800 元/人，包含培训、培训教材、资料费、现场培训时午餐，现场培训时需要住宿的学员请提前通知班务组联系人，食宿协助安排，费用自理。

培训费交费方式：6 月 25 日前将培训费 6800 元/人汇至以下账户：

开户单位	**广东省网络空间安全协会**
开户银行	**中国工商银行广州吉祥支行**
开户账号	**3602072509200098077**

注：请提前通知培训机构联系人开具培训发票，并提供相关开票信息。

（2）考试认证费网上注册后在线缴纳，并在线申请发票（网址 http://ryrzcisaw.isccc.gov.cn），具体缴纳时间、金额请留意中心通知。

五、 联系方式

联系人：成珍苑 15360402627、陈菊珍 15989296453、陈美云 18688452239 。

附件 1：CISAW 应急管理与服务专业级培训课程表

广东省网络空间安全协会　　广州华南信息安全测评中心

2021 年 12 月 1 日

附件一：

CISAW 应急管理与服务专业级培训课程表

日期			课程名称	课程内容简介
第一天	上午	9:00-12:00	概述	介绍 CISAW 认证体系、培训体系、教学实践和应急响应基本概念。
			应急响应相关法律法规	介绍网络安全事件管理和应急响应法规政策依据，包括《关于加强信息安全保障工作的意见》、《网络安全法》、《党委（党组）网络安全工作责任制实施办法》、等保 2.0、《数据安全法》、《个人信息保护法》、《关键信息基础设施安全保护条例》、国家标准/行业规范。
			信息安全事件分类分级	介绍信息安全事件分类分级，包括《信息安全技术信息安全事件分类分级指南》（GB/Z 20986-2007）内容，恶意程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障事件、灾害性事件案例分析，安全事件定级要素等。
	下午	13:30-16:30	网络安全事件管理与应急响应组织	介绍《信息技术 安全技术信息安全事件管理指南(GB/Z 20985-2007)》内容，介绍应急响应组作用、国际信息安全应急响应相关组织、国内信息安全应急响应相关组织。
			应急响应案例分析研讨	介绍应急响应案例，分析其响应过程中的不足之处，包括勒索病毒应急案例、网上营业厅数据被盗案例、积分管理系统隐蔽盗取案例。
			典型网络安全入侵事件重现与分析	通过真实入侵场景案例汇总分析，介绍典型网络安全入侵事件中多次被突破原因和应急响应对抗细节，包括入侵踩点预警与对策、系统框架漏洞被利用原理与对策、软件代码漏洞与对策、社工利用分析与对策、单位内部人员风险分析与对策。
第二天	上午	9:00-12:00	主机漏洞利用分析实践	介绍主机漏洞利用过程，其中上机攻防实操内容包括：远程溢出漏洞利用分析实践、本地溢出漏洞利用分析实践、账号后门与提权分析实践、应用系统提权分析实践等。
			主机入侵溯源分析实践	介绍主机入侵溯源分析过程，其中上机攻防实操内容包括：木马检测过程分析实践、开放端口检测分析实践、口令破解过程分析实践、用户登录日志审计实践、用户操作痕迹审计实践等。
			主机入侵事件检测技术总结与工具包准备	分别针对 Windows 和 Linux 总结主机入侵事件检测技术，其中入侵排查技术包括：特权账号排查、后门账号排查、命令执行痕迹分析、异常端口和连接排查、异常进程排查、异常文件排查、异常服务排查、启动项异常排查、计划任务排查、日志异常排查等；应急响应工具包准备包括：Rootkit 查杀工具包、病毒查杀工具包、Webshell 查杀工具包等。

	下午	13:30-16:30	主机攻击特征之数据流分析实践	介绍主机攻击特征，包括开源数据包分析软件使用技巧、攻击数据包与数据流检测实践、黑客工具攻击特征抓包溯源案例分析等。
			网络层应急技术与实践	介绍网络层攻击特征分析与应急技术实践，包括网络协议安全漏洞原理、ARP 欺骗攻击分析与应急响应、拒绝服务攻击分析与应急响应、网络安全域划分原则、网络安全架构与拓扑隐患分析实践、票务系统爬虫应急案例分析与应急方案研讨等。
			数据库渗透与应急响应实践	介绍数据库渗透与应急响应实践，包括应用系统管理后台突破分析、SQL 注入点利用过程分析、数据库脱库过程分析、数据库常见漏洞利用分析、数据库常见安全配置项加固等。
第三天	上午	9:00-12:00	应急技术综合演练实践之 SQL 注入攻击分析实践与加固	介绍 SQL 注入攻击原理与应急实践,包括 SQL 注入产生原理、SQL 注入利用过程分析实践、网马上传分析实践、反向连接后门利用分析实践、入侵痕迹分析实践、SQL 注入代码漏洞修补、SQL 注入绕过分析实践等。
			应急技术综合演练实践之 XSS 攻击分析实践与加固	介绍 XSS 攻击原理与应急实践，包括 XSS 攻击原理和类型、利用 XSS 增加应用系统账号分析实践、利用 XSS 钓鱼攻击分析实践、XSS 漏洞代码修复实践等。
			应急技术综合演练实践之 CSRF 攻击分析实践与加固	介绍 CSRF 攻击原理与应急实践，包括 CSRF 攻击原理、CSRF 攻击过程分析实践、CSRF 漏洞代码修复分析、Webshell 特征检测、数据库查询权限降权加固、系统账号安全配置实践、中间件安全加固实践、日志自动获取与分析实践等。
	下午	13:30-16:30	应急安全技术保障实践之 PKI 应用	介绍加解密原理与应用实践，包括对称加密概念、非对称加密概念、哈希算法概念、CA 与数字证书概念、常见单向 Https 认证漏洞原理和利用分析、双向 Https 认证配置实践等。
			应急安全技术保障实践之日志分析概念与技术	介绍日志分析概念与技术，包括日志分析基础性知识、日志分析内容及日志分析的要求、日志来源分类及采集方式、日志分析技术简介、设备日志分析技术的选择等。
			应急安全技术保障实践之日志集中管理与审计系统	介绍日志集中管理与审计系统，包括日志集中管理和审计系统架构、日志分析系统全生命周期管理、日志分析系统的功能要求、日志分析系统与其它系统接口等。
第四天	上午	9:00-12:00	企事业单位网络安全工作现状与困惑分析	介绍企事业单位网络安全工作现状和困惑，包括每天忙于救火的原因分析、网络安全防御思路误区、应急体系建设成熟度、应急管理体系建设阶段等。
			应急管理体系化建设 I	介绍应急管理体系化建设，包括责任体系建立、业务风险评估、业务影响分析、确定应急响应恢复目标等环节如何开展工作。
			应急管理体系化建设 II	介绍应急管理体系化建设，包括预警体系建设、安全态势监控与事件检测等环节如何开展工作。

	下午	13:30-16:30	应急预案制定与管理	介绍应急预案制定与管理，包括应急预案制定、应急预案测试、应急预案培训与演练、应急预案维护等。
			网络安全事件应急处理流程 I	介绍应急 PDCERF 模型，包括准备阶段、检测阶段应该如何开展工作，常见工作缺失分析。
			网络安全事件应急处理流程 II	介绍应急 PDCERF 模型，包括抑制阶段、根除阶段、恢复阶段、跟进阶段每个阶段应该如何开展工作。
第五天	上午	9:00-12:00	业务系统流程分析与数据流风险点识别沙盘演练	介绍业务系统流程分析与数据流风险点识别要点，分组选定业务系统、开展业务系统流程分析、数据流风险点识别沙盘实践练习。
			应急响应流程梳理与预案编写沙盘演练	介绍应急响应流程梳理与预案编写要点，结合案例模板，分组开展沙盘演练实践练习。
			应急演练组织与开展沙盘演练	介绍应急演练组织与演练工作要点，结合演练视频案例，分组开展沙盘演练实践练习。
	下午	13:30-16:00	考试	