信息安全等级保护及关键信息基础设施安全保护制度解读及工作实践

课程背景：

信息及重要数据是一个国家的新型基础性资源。近期，公安部制定出台了《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》，进一步健全完善国家网络安全综合防控体系，有效防范网络安全威胁，有力处置重大网络安全事件，切实保障关键信息基础设施、重要网络和数据安全。

课程时间：3 小时
授课讲师：马兆林

第一章 解析信息安全等级保护

一、 实施信息安全等级保护目的

1. 体现国家管理意志
2. 构建国家信息安全保障体系
3. 保障信息化发展和维护国家安全

二、 信息安全等级保护任务

1. 构建国家信息安全保障体系。
2. 推动信息应用发展
3. 实现很强技术性的国家风险控制行为

三、 如何开展信息安全等级保护工作

1. 管理办法
2. 实施指南
3. 定级指南
4. 基本要求

5．测评要求

第二章 解读关键信息基础设施安全保护制度及工作实践

一、 确定关键信息基础设施的认定方法

1．关键信息基础设施的定义等。

2．认定主体

3．认定依据。

4．认定方式：单独认定

二、 明确关键信息基础设施的主管部门及各自职责

1．保护工作部门及具体职责

2．国务院电信主管部门（即国家工业和信息化部）

3．国家网信部门职责（即国家互联网信息办公室）

4．国务院公安部门（即公安部）

三、 明确运营者的三大特殊合规制度建设义务

1．建立健全网络安全保护制度

2．建立健全数据安全保护制度

3．建立健全个人信息保护制度

4．强化和落实关键信息基础设施运营者主体责任

5．对漏洞探测、渗透性测试等活动进行了特别规定

工作实践：从滴滴事件分析信息安全等级保护及关键信息基础设施安全保护制度解读。