《信息安全监管》知识点串讲

一、网络安全政策

1. 网络空间安全战略：五项目标，和平、安全、开放、合作、有序。
2. 回顾中央办公厅 2003 的 27 号文件

1）方针：积极防御、综合防范

2）原则：立足国情、以我为主、技管并重；正确处理安全和发展的关系；统筹规划、突出重点、强化基础工作；发挥国家、企业和个人的作用。

3）9 项工作内容：不包括**国产化、自主创新、知识产权和隐私保护**。

二、网络安全法律法规

1. 计算机犯罪：狭义（信息系统为目标）和广义（包括狭义和其他目标）之分。
   计算机犯罪特点：多样性、复杂化、国际化、不对称性。
2. 我国的多级立法机制（总分结构）及法律体系的构成。
3. 网络安全法（见如下介绍）：总则、网络安全支持与促进、网络运行安全、网络信息安全、网络安全监测预警与应急处置、法律责任、附则。
4. 网络安全法总则：

1）网络空间主权的原则

2）国家网信部门统筹协调（中国共产党中央网络安全和信息化委员会）

3）域外适用效力的理解

5. 网络安全支持与促进

1）网络安全建设和发展的法律支持

2）网络安全建设和发展政策制定的依据

6. 网络运行安全

6.1 一般规定（等级保护）

1）网络运营者义务：管理制度及责任；技术防护与日志 6 个月；数据保护；实名制；应急预案；安全协助和支持。

2）产品和服务提供者义务：强制标准；告知补救；安全维护；个人信息保护。

3）一般性义务：信息发布的安全；禁止的危害行为；信息使用规则。

6.2 关键信息基础设施的保护（强调一下：在一般规定基础上进一步的要求）

1）人员安全审查、培训教育和考核；

2）数据出境的国家安全评估；

3）产品和服务采购的国家安全评估；

4）一年一次的风险检测评估；

5）应急预案的制定和定期演练。

7. 网络信息安全

1）个人信息的保护

2）从主体及行为的角度规范信息管理。

3）各主体的职责

8. 监测预警与应急处置

1）网信部门统筹该工作。

2）其他部门各司其职。

9. 法律责任

1）民事责任

2）行政责任

3）刑事责任
10.附则（术语的解释等）
其他与网络安全有关的法律（参考教材）
三、**道德准则**
1、理解道德是法律的基础。
2、掌握 cisp 道德规范的四个部分。
四、标准
1. 标准化基础（国际）
1）标准化概念：动态、相对、应用效益，简化、统一、协调、优化。
2）标准化国家组织：ISO\IEC**IETF**\ITU 等。
3）ISO/IEC JTC1 SC27 的工作组（5 个），WG1 是信息安全管理体系的标准制定的,iso/iec 27001-27005；WG3 是安全评估标准的制定，iso/iec 15408。
2. 我国的标准化
1）标准化组织：TC260
2）标准组织的分工：TC260 有 8 个工作组，其中 WG2 是涉密信息系统安全标准的制定；WG5 是评估标准；WG7 是管理标准的制定；SWG-BDS 大数据安全标准。
3. 等级保护标准
3.1 流程：定级备案、建设整改、测评。
3.2 定级标准：GB **原理（122-234-345）**、业务信息和系统服务的等级。
3.3 基本要求：
1）2019 年 12 月 1 日生效的通用要求：
—技术要求包括：安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心。
—管理要求包括：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 。
2）各类要求：1-4 级（云计算、工控安全、物联网、移动互联网安全）。
3.4 测评标准
1）测评指南、测评过程要求。
2）三级系统一年测评一次；四级系统每半年测评一次。
3）测评结论：符合、**基本符合**和不符合。
4）测评人员：初级、中级和高级测评师，其中高级测评师需要签字。

温馨提示：为了减少学习的负担和聚焦核心，知识点总结写的是关键的精要的要点，并非是知识点的全文，请一定进一步结合官方的教材进行理解和掌握全面，以免产生以偏概全的问题。

因为需要兼顾到大纲、教材、过去的考题，以及现在的发展，如下强调一下：
1）第一个强调的：网络安全法中关键信息基础设施保护的要求是建立在一般要求的基础上的，先满足一般要求，然后满足关键信息基础设施要求，比如一般要求中要求制定应急响应预案，而关键信息基础设施中进一步要求周期演练。但实际工作要注意，都是需要演练，演练是判断预案是否可行的一个方式。
2）第二个强调的：等级保护基本要求的考试可能性，如果出题考的是通用要求中的技术和管理各 4 个子类,那么按照各四类解答。如果涉及到各为 5 个子类的，请按照我给大家补充的最新知识点中的 5 个子类解答。

（END）