《网络安全法》解读报告

何治乐 公安部第三研究所

个人简介

2013年毕业于西安交通大学，硕士研究生，信息安全法学。

中国网络空间安全协会网络空间安全法律与公共政策专业委员会委员

西安交通大学信息安全法律研究中心兼职研究员

翻译多部国外信息安全法律法规；作为主要参与人参加上海市科委、中国工程院、公安部等省部级课题6项；发表论文20余篇；参与编写著作教材6本；参与编写5部研究报告并向社会公开发布，向公安部网络安全保卫局提交法律研究报告超过20个。

公安三所网络安全法律研究中心

- 致力于服务网络安全中心工作需要，跟踪研判国内外网络安全事件，深度分析国外网络安全战略、政策和立法动向，动态关注新技术新应用给网络管理带来的热点难点问题，为政府机构提供高质量的法律研究支撑。


这是最好的时代
也是最坏的时代

目录

一、网络安全法的背景、定位和制度设计

一、网络安全法的背景、定位和制度设计

- 网络主权等国际斗争愈发尖锐；
- 信息化衍生的负面效应影响广泛；
- 网络安全立法的国际较量日趋激烈；
- 党中央决策部署的重要内容。

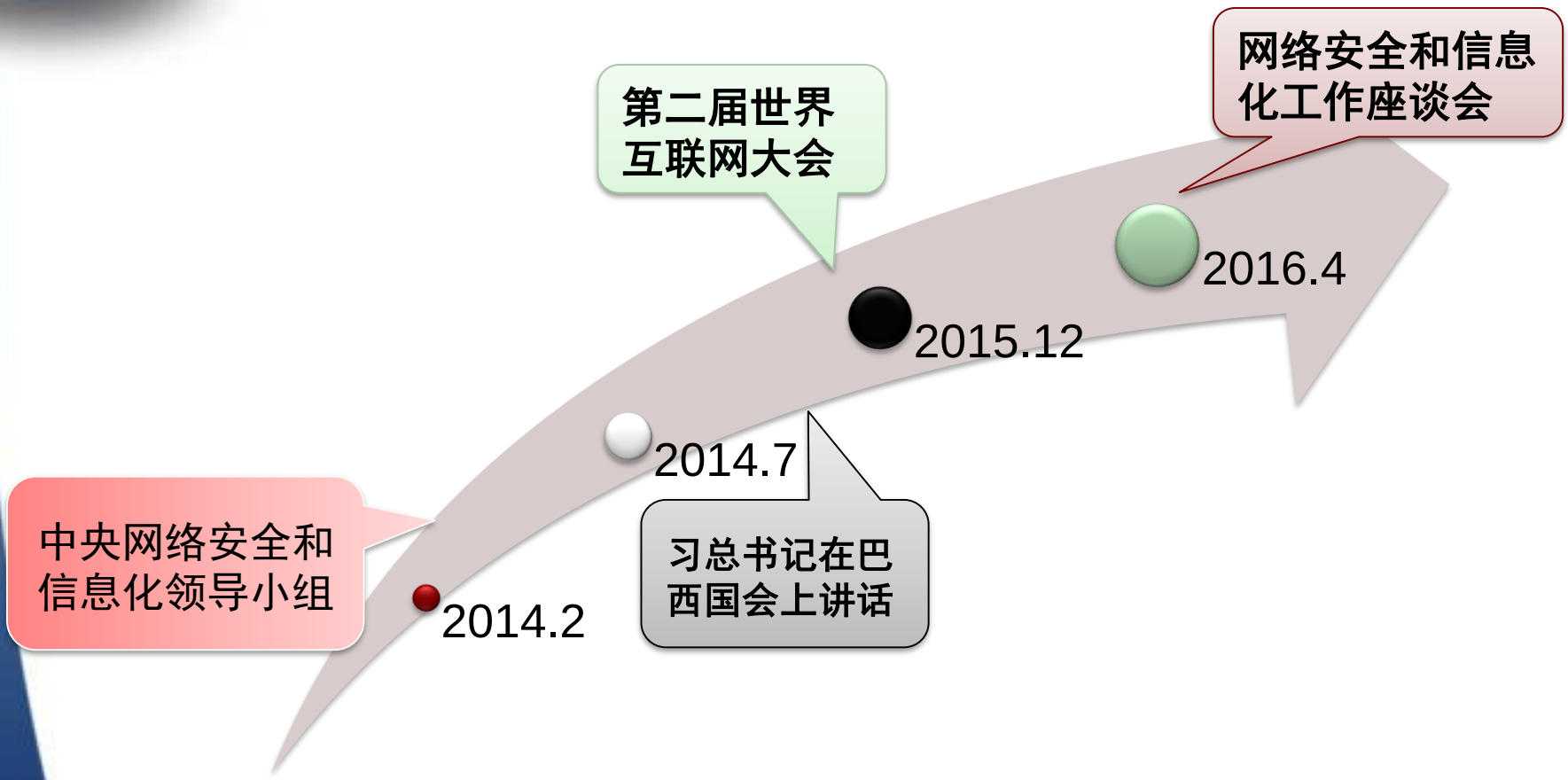
国际网络安全法治环境重大变革

- 美国《联邦信息安全现代化法》《国家网络安全保护法》《网络安全人员评估法案》《网络安全增强法》（2014.12）
- 美国CISA法案（2015.11）
- 2016信息自由法案促进法（2016.6）
- 国防部发布“漏洞披露政策”（2016.11）
- 关于收集、分析和储存美国公民资讯的行政命令12333号；国家网络事件响应计划（NCIRP）；（2017年1月）
- 电子邮件隐私法（2017.2）
- 《2017 NIST网络安全框架、评估和审查法案》，针对金融机构的网络安全规则；废除FCC网络用户隐私保护法案（2017.3）

国际网络安全法治环境重大变革

- 欧盟GDPR（2015.12.25）
- 以色列史上最严的新反恐法（2016.6）
- 俄罗斯反恐法（2016.7）
- 欧美安全港协议陨落到隐私盾生效（2016.7）
- 瑞士通过扩大监控权限的《新情报法》（2016.9）
- 英国《国家网络安全战略》（2016.11）
- 英国2016IPA赋予政府更充分的侦查权（2016.11）
- 俄罗斯新版《俄联邦信息安全学说》（2016.12）
- 2017英国数字化战略（2017.3）
- 新加坡《计算机滥用和网络安全法》引入新的刑事犯罪，马来西亚提议海外数据转移“白名单”草案（2017.4）

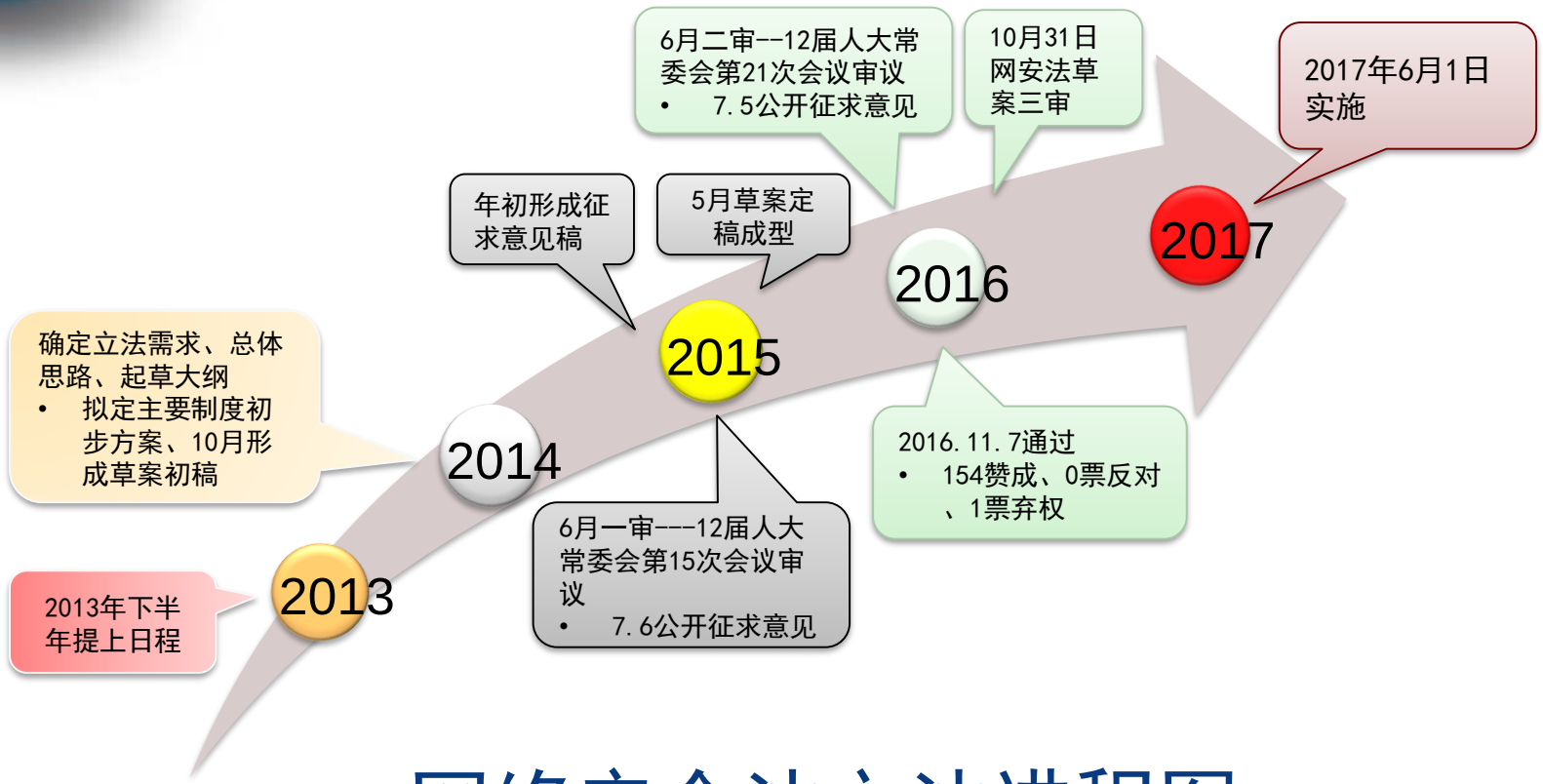
网络安全立法的顶层设计支持



网络安全立法的顶层设计支持

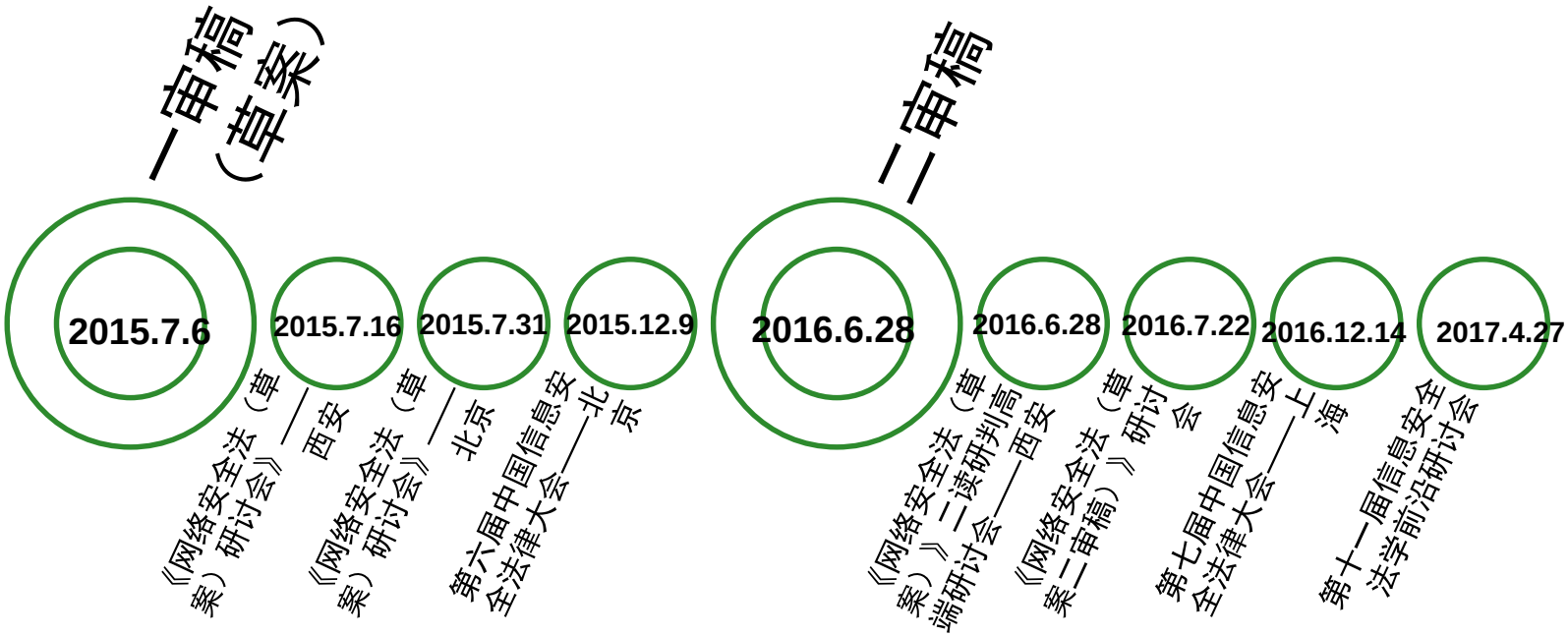
- 2014年11月1日，《反间谍法》通过；
- 2015年7月1日，《国家安全法》通过，1993年制定的《国家安全法》被取代；
- 2015年7月6日，《网络安全法》草案公开征求意见；
- 2015年12月27日，《反恐怖主义法》通过；
- 2016年7月5日，《网络安全法（草案二次审议稿）》公开征求意见；
- 2016年7月21日，《国家信息化发展战略纲要》正式出台；
- 三稿三审，2016年11月7日，《网络安全法》终获通过，2017年6月1日开始正式施行；

一、网络安全法的制定过程



网络安全法立法进程图

一、网络安全法的制定过程



全程参与


第七届中国信息安全法律大会
The 7th China Information Security Law Conference
主权·治理·密码·执法


《网络安全法(草案二次审议稿)》研讨会

一、网络安全法的制度设计

- **三大战略影响深远**

  网络安全战略、人才培养战略、可信身份战略

- **四大原则凝聚共识**

  和平、安全、开放、合作

- **八项制度规范行为**

  等级保护、CII保护、国家安全审查、数据离境存储、用户信息保护、安全认证和检测、监测预警和信息通报、应急处置

网络安全法的定位

以风险控制为主线，从网络的设备设施安全、运行安全及数据安全等方面入手；以维护网络空间主权和国家安全、社会公共利益和公民、法人及其他组织的合法权益，促进经济社会信息化健康发展为目的；重点确立网络安全保护制度和网络运营者的责任，网信部门、公安机关等的监管职权。

重视对信息社会整体的保护，将个人信息、CII及信息系统等都纳入保护范围，是一部保障我国网络安全的**综合性和基础性**立法。

二、网络安全法的体系架构与亮点

网络安全法的体系架构

1、总体框架。共7章79条。目录如下：

第一章 总 则

第二章 网络安全支持与促进

第三章 网络运行安全

第一节 一般规定

第二节 关键信息基础设施的运行安全

第四章 网络信息安全

第五章 监测预警与应急处置

第六章 法律责任

第七章 附 则

网络安全法的体系架构

2、规范和调整的范围：

- 网络空间主权(关于特定域外效力)
  - 国内管辖权、独立权、自卫权、依赖性主权
  - 对境外攻击破坏行为的管辖权
  - 监测
  - 防御
  - 惩治
  - 制裁

网络安全法的体系架构

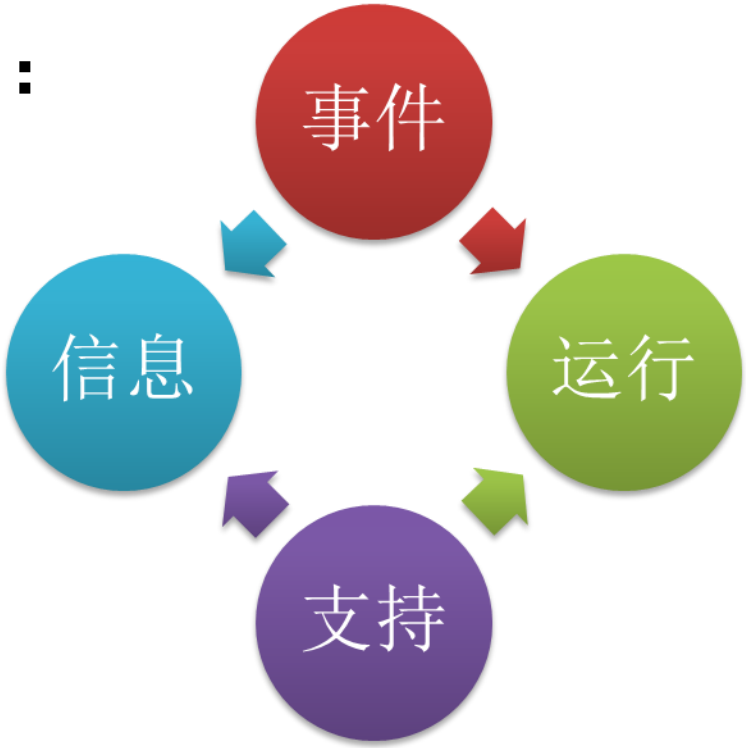
2、规范和调整的范围：

- 国家网络安全等级保护制度
- 关键信息基础设施保护
- 网络运营者义务
- 网络产品和服务提供者义务
- 保障网络信息安全，个人信息保护
- 关键信息基础设施重要数据跨境传输
- 监测预警与应急处置

网络安全法的体系架构

3、有机结合的架构：

- 网络安全支持
- 网络运行安全
- 网络信息安全
- 网络安全事件
- 几者之间关系



网络安全法的亮点

1、战略入法

- 战略入法，欧盟网络安全指令有先例
- 战略入法保障国家政策的顶层设计

2、关键信息基础设施概念首次立法明确

- 概念首次出现在习近平讲话

（二）网络安全法的亮点

3、综合安全范畴形成

- 网络安全包括内容安全
- 网络安全包括数据安全
- 网络运营安全融合供应链安全

4、制度机制衔接协同有力

- 网络安全监管统筹协调、分工负责明确
- 国家、地方、行业、军队

三、网络安全法的亮点

5、综合应对境外网络攻击

- 经济制裁（75）
- 过滤网站（50）

6、注重国家队与社会队的协同能力

- 国家采取措施（5）
- 安全社会化服务体现建设（17）

7、发展并重特色明显

- 鼓励开发、创新（16、18）
- 研究开发有利于未成年人（13）
- 认证、检测结果互认（23）

三、网络安全法的重点

关键信息基础设施保护（重中之重）

背景

从世界范围看，网络安全威胁和风险日益突出，并日益向政治、经济、文化、社会、生态、国防等领域传导渗透。特别是**国家关键信息基础设施**面临较大风险隐患，网络安全防控能力薄弱，难以有效应对国家级、有组织的高强度网络攻击。

金融、能源、电力、通信、交通等领域的关键信息基础设施是经济社会运行的神经中枢，是网络安全的重中之重，也是可能遭到重点攻击的目标。

——习近平总书记419讲话

背景

国家	时间	攻击对象	CII
美国	2012	华盛顿大学和费城大学网站	教育
日本	2012	财政部	政府
澳大利亚	2012	莫纳什大学官方网站	教育
中国	**2013**	**大批中国政府站点**	**政府**
印尼	2013	印尼第二步兵及陆军战略指挥部	国防
墨西哥	2013	墨西哥国防部网站	国防
美国	2013	麻省理工学院、斯坦福及哈佛大学	教育
土耳其	2013	总统和执政党网站	政府
美国	2013	美国空军文化&语言中心官方网站	国防
美国	2013	能源部（DOE）网站被黑	能源

背景

2016年4月，菲律宾，委员会选举网站，5500万，个人信息；

2016年6月，英国，格林威治大学，网络数据库，所有数据；

2016年7月， 美国，民主党全国委员会，大量内部邮件；

2017年3月，美国，Dun＆Bradstreet，数据库遭到泄露；

2017年3月，新加坡，国防部，国民服役人员和国防部职员；

2017年4月，美国，医疗机构，1800起重大数据泄露事件。

背景

- 2015年2月，汇丰银行大量秘密银行账户文件被曝光。这些文件覆盖的时间为2005-2007年，涉及约3万个账户，这些账户总计持有约1200亿美元资产，堪称史上最大规模银行泄密。
- 2015年6月，工行快捷支付被曝存在严重漏洞，多位北京地区的工行储户遭遇了存款被盗事件。
- 2016年10月，印度，ATM网络，国家银行60万张借记卡；
- 2016年11月，俄罗斯，五家主流大型银行，DDoS攻击；

网络安全等级保护制度

- 《中华人民共和国人民警察法》第十二条规定，公安机关负责监督管理计算机信息系统的安全工作。《中华人民共和国计算机信息系统安全保护条例》（国务院147号令）明确规定，计算机信息系统实施安全等级保护，由公安机关牵头会同有关部门制定。
- 2007年以来，公安部会同保密、密码、信息办等部门先后出台了《信息安全等级保护管理办法》及一系列安全保护标准，建立信息安全等级保护工作体系。
- 在试点的基础上，从2007年开始，公安部会同有关部门在全国范围内全面部署开展信息安全等级保护工作，大力推动信息系统运用使用单位按照等级保护要求，开展定级、备案、建设（整改）、测评工作。

网络安全等级保护制度的理解

《信息安全等级保护管理办法》[2007]43号文

网络安全等级保护制度

第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；（软硬件监测，留存日志）

（四）采取数据分类、重要数据备份和加密等措施；（数据安全）

（五）法律、行政法规规定的其他义务。

网络安全等级保护制度

第五十九条　网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。（法律责任）

关键信息基础设施保护制度

第三十一条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。（建立关键信息基础设施保护制度，在等级保护制度基础上突出保护重点）

国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

关键信息基础设施保护制度

《国家网络空间安全战略》

国家关键信息基础设施是指关系国家安全、国计民生，一旦数据泄露、遭到破坏或者丧失功能可能严重危害国家安全、公共利益的信息设施，包括但不限于提供公共通信、广播电视传输等服务的基础信息网络，能源、**金融**、交通、教育、科研、水利、工业制造、医疗卫生、社会保障、公用事业等领域和国家机关的**重要信息系统**，**重要互联网应用系统**等。

采取一切必要措施保护关键信息基础设施及其重要数据不受攻击破坏。

关键信息基础设施保护制度

第三十二条 按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门分别编制并组织实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工作。（职责规定：制定规划）

第三十三条 建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。（安全要求，“三同时”制度）

关键信息基础设施保护制度

第三十四条 除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：（重点措施）

（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；

（二）定期对从业人员进行网络安全教育、技术培训和技能考核；

（三）对重要系统和数据库进行容灾备份；

（四）制定网络安全事件应急预案，并定期进行演练；

（五）法律、行政法规规定的其他义务。

第三十五条 关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。（非常态的网络产品和服务的国家安全审查）

《国家安全法》第五十九条 国家建立国家安全审查和监管的制度和机制，对影响或者可能影响国家安全的外商投资、特定物项和关键技术、网络信息技术产品和服务、涉及国家安全事项的建设项目，以及其他重大事项和活动，进行国家安全审查，有效预防和化解国家安全风险。

- 网络产品和服务安全审查办法(试 行)
- 第十条 公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过网络安全审查。产品和服务是否影响国家安全由关键信息基础设施保护工作部门确定。

法律责任

第六十五条 关键信息基础设施的运营者违反本法第三十五条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款;对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。（使用未经安全审查或者安全审查未通过的网络产品或者服务行为的处罚规定）

第三十六条 关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。（产品和服务的供应链风险控制（资质资信审查+保密义务+监督过程留存相关记录）

第三十七条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。（数据境内存储和向境外提供）

4月11日，网信办发布《个人信息和重要数据出境安全评估办法（征求意见稿）》

法律责任

第六十六条 关键信息基础设施的运营者违反本法第三十七条规定，在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。（处罚数据境外存储、向境外提供）

第三十八条 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。（等级测评，风险评估，渗透测试）

- 第三十九条 国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：
- （一）对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估；
- （二）定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力；
- （三）促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享；
- （四）对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助。（统筹协作机制）

第五十一条 国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。（建立监测预警和信息通报制度，将信息通报制度上升为法律）

第五十二条 负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。（要求行业建立信息通报制度)

法律责任

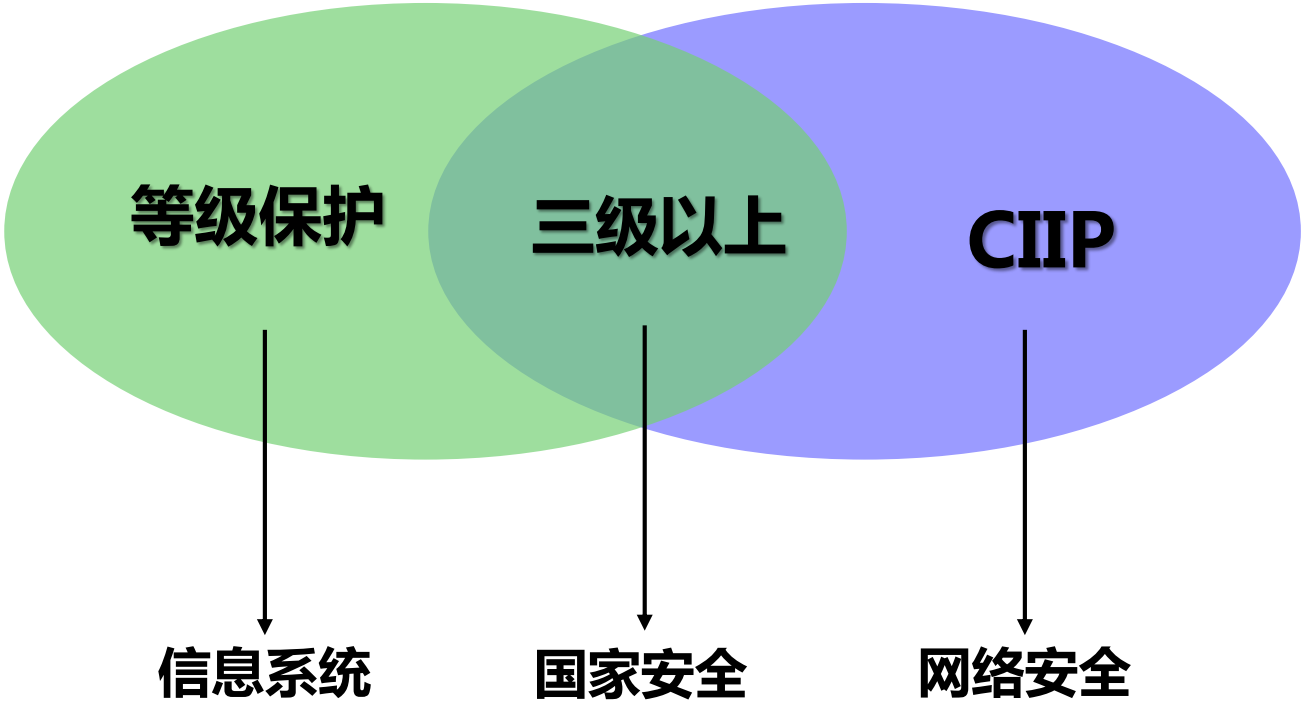
第五十九条 网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款；对直接负责的主管人员处五千元以上五万元以下罚款。关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款；对直接负责的主管人员处一万元以上十万元以下罚款。（网络运营者不履行网络安全保护义务应承担的法律责任）

三、网络安全法的重点

CIIP与等级保护

等级保护与CIIP的差异

等级保护与CIIP的协调



关键信息基础设施保护制度借鉴

2014年2月，美国国家标准技术研究院（NIST）发布《提升关键基础设施网络安全的框架》（Framework for Improving Critical Infrastructure Cybersecurity）；

2016年1月，欧盟网络和信息安全局发布的《CIIs保护的梳理、分析和建议》（Stocktaking, Analysis and Recommendations on the Protection of CIIs）报告。

等级保护与CIIP的协调

1.确定第三级以上的信息系统为关键信息基础设施；

2.协调公安部门、网信部门等机构之间的管理职责；

3.以等级保护为基础，确定CII保护的最佳实践；

4.重视公私部门之间的合作互助与信息共享；

5.增强法律的可操作性，做到执法必严，违法必究。

三、网络安全法的重点

个人信息保护

我国个人信息保护法律法规

- 刑法（253条之1、186条之1）
- 居民身份证法（6、15、16、17、18、19）
- 治安管理处罚法（42、48）
- 消费者权益保护法（14、29、50、56）
- 全国人大常委会关于加强网络信息保护的决定
- 国务院关于促进信息消费扩大内需的若干意见（6）
- 规范互联网信息服务市场秩序若干规定（11、12、13、16、18）
- 电信和互联网用户个人信息保护规定
- 即时通信工具公众信息服务发展管理暂行规定（5、6）
- 最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定（12、13、18）

个人信息概念

个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

第二十二条　网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

对网络运营者的规定

第四十条　网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。

第四十一条　网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。（**收集、使用个人信息**）

对网络运营者的规定

第四十二条　网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

第四十三条　个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

- 第四十四条　任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。
- 第四十五条　依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。
- 第四十六条　任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

第四十八条　任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。

电子信息发送服务提供者和应用软件下载服务提供者，应当履行安全管理义务，知道其用户有前款规定行为的，应当停止提供服务，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

第四十九条　网络运营者应当建立网络信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关网络信息安全的投诉和举报。

网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合。

金融机构个人信息保护制度调研

- 2012年12月《全国人大常委会关于加强网络信息保护的决定》《电信和互联网用户个人信息保护规定》
- 9大CII行业217家单位：互联网、教育、金融、医疗、航空、政府机构、电子商务、通信、电子设备提供行业
- 隐私政策中涉及保护范围、收集使用原则、限制利用原则、数据安全保护措施、删除权、未成年人的个人数据保护等内容以及企业超出现有立法规定的自我规定进行分析。

金融机构个人信息保护制度调研

- **金融行业（42）**
- （1）银行：中国人民银行，中国政策性银行（中国国家开发银行、中国农业发展银行、中国进出口银行），及十六家代表性的商业银行（中国民生银行、华夏银行、中国光大银行、中信实业银行、中国银行、中国建设银行、恒丰银行、上海浦东发展银行、交通银行、浙商银行、兴业银行、深圳发展银行、招商银行、广东发展银行、中国工商银行、中国农业银行）。
- （2）证券公司：上海证券交易所、深圳证券交易所、国泰君安、银河证券、申银万国、国信证券、海通证券、广发证券、招商证券、中信建投、中信证券、华泰证券。
- （3）保险公司：中国人寿、中国平安、太平洋保险、中国人保、中国太平、友邦保险、新华保险、泰康保险、阳光保险、大地保险。

金融机构个人信息保护制度调研

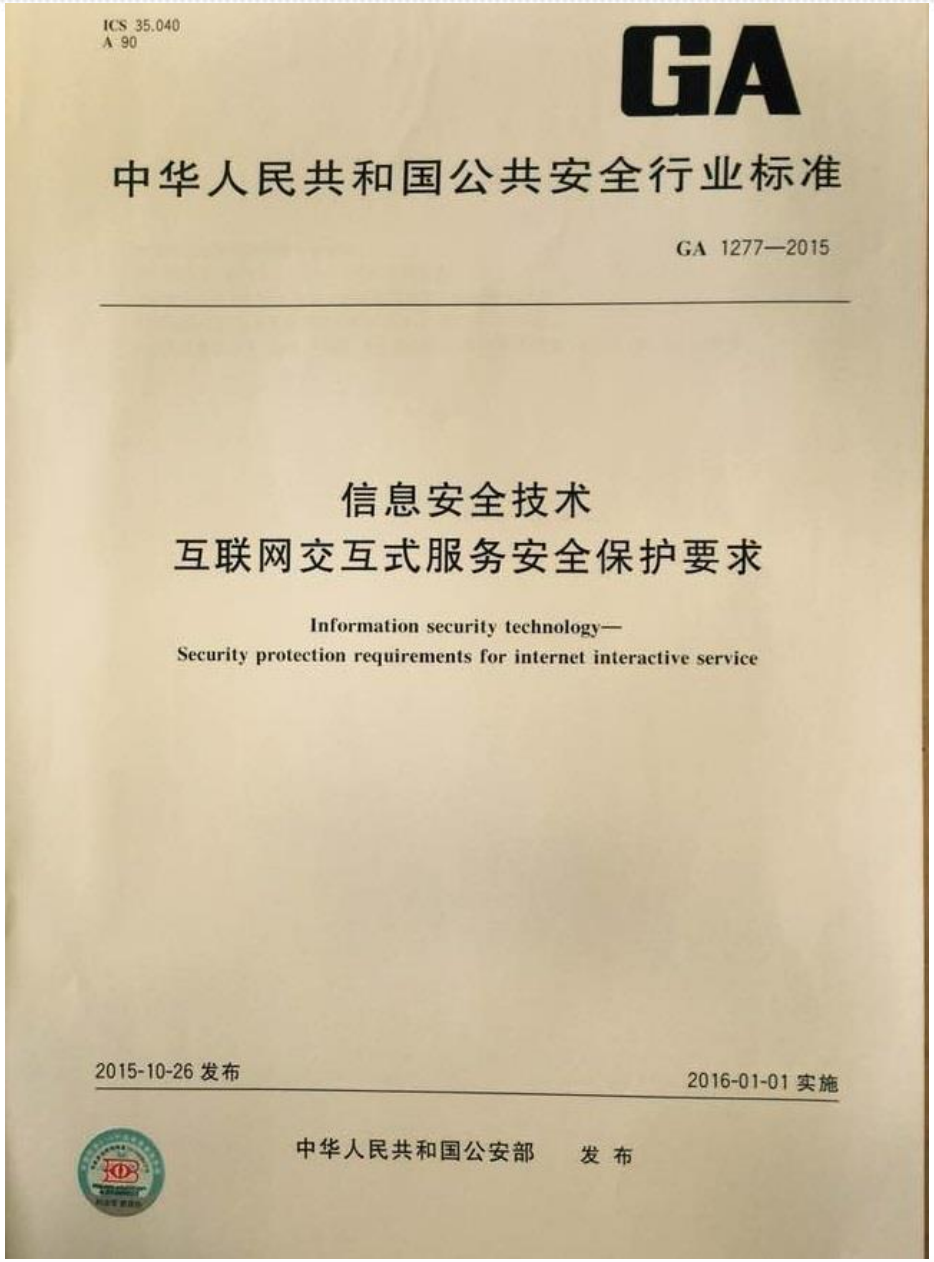
在调查的42家金融行业中，有隐私保护条款（包括网站声明中的个人信息保密制度）的13家（6家银行、7家保险公司），占39%。相比其他行业，金融行业的比重较大，而保险行业的隐私政策规定的较为全面。

	范围界定5	明示收集3	保护措施9	删除权2	披露11	专岗0	委托方1	变更2	用户投诉0	技能培训0	自我监督0	未成年人3
中行					√							
招行			√		√							
农银			√		√							
民生	√				√							
工商			√		√		√					
广发			√		√			√				
平安			√		√							√
人保					√							
人寿					√							
寿康	√	√	√	√								√
太平洋	√	√	√		√							
阳光	√	√	√	√	√							√
友邦	√		√					√				

公共安全行业标准：GA 1277-2015《互联网交互式服务安全保护要求》

互联网交互式服务安全保护要求

- 公安部历经近两年时间，依据相关法律法规和国内外标准规范，制定了《信息安全技术 互联网交互式服务安全保护基本要求》，已于2015年10月26日正式颁布，自2016年1月1日起开始实施。
- 强制性标准，颁布后必须贯彻执行，否则可以予以行政处罚。个人或单位处以罚款、停止联网、停机整顿。


ICS 35.040
A 90

GA

中华人民共和国公共安全行业标准

GA 1277—2015

信息安全技术
互联网交互式服务安全保护要求

Information security technology—
Security protection requirements for internet interactive service

2015-10-26 发布　　2016-01-01 实施

中华人民共和国公安部　发布

- 针对即时通信、微博客、博客、论坛、聊天室、社区、第三方支付等互联网交互式服务提供者，提出了其应落实的互联网安全保护要求。
- 包括安全制度文件、机构要求、人员安全、访问制度等管理制度，以及网络与操作安全、应用安全、个人电子信息保护、投诉处理、分包服务要求和安全事件管理等技术措施。

个人电子信息保护—处理规则

- 应制订明确、清楚的个人电子信息处理规则，并在显著位置予以公示。在用户注册时，应在与用户签订服务协议中明示收集与使用个人电子信息的目的、范围与方式。
- 网络交互式服务提供者仅收集为实现正当商业目的和提供网络服务所必需的个人信息；收集个人电子信息时，必需取得用户明确授权同意；将个人电子信息交给第三方处理时，处理方必须符合本标准要求，并取得用户明确授权同意；法律、行政法规另有规定的，从其规定。
- 修改个人电子信息处理规则时，应告知用户，并取得其同意。

个人电子信息保护—技术措施

- 应建立覆盖个人电子信息处理的各个环节的安全保护制度和技术措施，防止个人电子信息泄露、损毁、丢失，包括：
  - 采用加密方式保存用户密码等重要信息；
  - 审计内部员工对涉及个人电子信息的所有操作，并对审计结果进行分析，预防内部员工故意泄露；
  - 审计个人电子信息上载、存储或传输，作为信息泄露、毁损、丢失的查询依据；
  - 建立程序来控制对涉及个人电子信息的系统和服务的访问权的分配。这些程序应涵盖用户访问生存周期内的各个阶段，从新用户初始注册到不再需要访问信息系统和服务的用户的最终撤销；
  - 系统的安全保障技术措施应覆盖个人电子信息处理的各个环节，防止网络违法犯罪活动窃取信息，降低个人电子信息泄露的风险。

个人电子信息保护—泄露处理

- 当发生个人电子信息泄露事件后，应：
  - 立即采取补救措施，防止信息继续泄露；
  - 24小时内告知用户，根据用户初始注册信息重新激活账户，避免造成更大的损失；
  - 24小时内报告公安机关。

四、网络安全法的实施

《网络安全法》的配套制度——顶层设计

- 12月，互联网信息办公室发布《国家网络空间安全战略》；
- 1月，工业和信息化部正式发布《大数据产业发展规划（2016 - 2020年）》《信息通信网络与信息安全规划（2016-2020年）》；
- 3月，经中央网络安全和信息化领导小组批准，外交部和国家互联网信息办公室共同发布《网络空间国际合作战略》；
- 4月，工业和信息化部编制印发了《云计算发展三年行动计划（2017-2019年）》

《网络安全法》的配套制度——信息内容

- 7月3日，网信办印发《关于进一步加强管理制止虚假新闻的通知》；
- 7月4日，国家工商行政管理总局发布《互联网广告管理暂行办法》；
- 7月7日，文化部印发《关于加强网络表演管理工作的通知》；
- 9月9日，国家新闻出版广电总局下发《关于加强网络视听节目直播服务管理有关问题的通知》；
- 11月4日，国家互联网信息办公室发布《互联网直播服务管理规定》；
- 4月7日，国家新闻出版广电总局发布了《关于调整互联网视听节目服务业务分类目录（试行）》；

《网络安全法》的配套制度——网络犯罪

- 9月，最高人民法院、最高人民检察院、公安部联合出台了《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》；银监会、公安部《电信网络新型违法犯罪案件冻结资金返还若干规定》；最高法、最高检、公安部、工信部、中国人民银行、中国银行业监督管理委员会等六部门联合发布《关于防范和打击电信网络诈骗犯罪的通告》；
- 11月，工信部正式发布修订后的《中华人民共和国无线电管理条例》
- 12月，最高法、最高检察、公安部发布《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》；
- 4月，最高人民法院审议并原则通过《最高人民法院、最高人民检察院关于办理扰乱无线电通讯管理秩序等刑事案件适用法律若干问题的解释》；

《网络安全法》的配套制度——个人信息

- 1月，国务院法制办公布《未成年人网络保护条例（送审稿）》；
- 3月，十二届全国人大五次会议审议的民法总则草案规定，自然人的个人信息受法律保护；最高人民法院审议并原则通过《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》；
- 4月，《个人信息和重要数据出境安全评估办法（征求意见稿）》；十二届全国人大常委会第二十七次会议表决通过新修订《测绘法》

《网络安全法》的配套制度——其它

- 7月，《非银行支付机构网络支付业务管理办法》正式生效
- 9月，国务院印发《政务信息资源共享管理暂行办法》
- 10月，工商总局发布《关于加强互联网领域消费者权益保护工作的意见》
- 2月，国家互联网信息办公室官网公布的《网络产品和服务安全审查办法（征求意见稿）》
- 4月，国家邮政局发布的《邮件快件寄递协议服务安全管理办法（试行）》正式施行；工业和信息化部对外发布《电信业务经营许可管理办法》(修订征求意见稿)；国家密码管理局发布《中华人民共和国密码法（草案征求意见稿）》

网络安全法的实施

- 有效梳理与现行法律法规之间的关系，开启部门、地方的立法和政策的制定、调整和完善工作；
- 亟需出台系列配套规定，《关键信息基础设施安全保护条例》等下位法的制定，更为详细的制度规定、具体行业的网络安全规划和网络安全标准体系等，实现与基础性法律的有效衔接；
- 网络安全保护义务主体：政府、企业和个人层面的合规是接下来的重点。

联系方式

公安三所网络安全法律研究中心

邮箱：csplaw@stars.org.cn

电话：021-68571909

何治乐：hezhile@stars.org.cn

15021233476

欢迎交流