ISC 2016

2016 中国互联网安全大会 China Internet Security Conference

协同联动 共建安全+命运共同体

国家网络安全审查制度的法律塑造

马　宁

西安交通大学
信息安全法律研究中心

目录

·国家网络安全审查的缘起

·国家网络安全审查的法理基础

·国家网络安全审查的实施

ISC 2016 中国互联网安全大会

360互联网安全中心

国家网络安全审查的缘起

——从美英安全审查案例的实证分析谈起

2012年10月9日，美国国会众议院情报委员公布了调查报告，该报告认为，美国应该以怀疑的目光审察中国电信公司在美国电信市场的持续渗透，不管是政府还是私营部门，都不应该和华为、中兴合作。

英国国家安全委员会于2013年7月对华为的网络安全中心进行了审查，形成了《华为网络安全中心：国家安全委员会审查》的报告，并向英国首相进行了汇报。

美英针对华为的审查结论

美国	英国
建议1：美国应该以怀疑的目光审察中国电信公司在美国电信市场的持续渗透。	结论1：华为网络安全评估中心能够有效进行运营，现有的管理制度保证了华为网络安全评估中心充足的独立性。
建议2：（委员会）强烈建议美国私营部门实体考虑与华为、中兴进行设备或服务业务往来相关的长期安全隐患，强烈建议美国网络提供商或系统开发商为他们的项目寻求另外合作厂商。	结论2：英国政府需要监管其中潜在的安全问题，最小化设备入侵的安全风险。
建议3：美国国会司法委员会和行政部门的执行机构应该对中国电信部门的不公平贸易行为进行调查，尤其应当关注中国对主要公司的持续财务支持。	结论3：针对华为网络安全评估中心设立专门的监管委员会。
建议4：中国公司应该迅速变得更加开放和透明，包括在有高度透明要求的西方股票交易所上市，提供独立第三方评估机构对于他们财务信息和网络安全进程的一致性评估，遵守美国信息和证据的合法标准，遵守所有知识产权法和标准。特别是华为，对于美国法律义务应该更加透明和应答性。	结论4：对华为网络安全评估中心进行年度审查。
建议5：美国国会司法委员会应该考虑潜在的立法，以更好应对与其他国家政府相关的电信公司所带来的风险，否则就不要充分信任他们来建造关键基础设施。这样的立法应该包含增加私营部门实体的信息共享，提升美国外国投资委员会对于参与采购协议所发挥的作用。	

安全审查中的WOLF CLAUSE：SEC516到SEC515

美国“2013年合并与持续拨款法案”第516条

• 第a款规定，美国商务部、司法部、国家宇航局和国家科学基金会不得利用任何拨款采购信息技术系统，除非上述联邦机构负责人与联邦调查局或其他适当机构对网络间谍或破坏行为进行了风险评估，该风险包括由中国拥有、管理或资助的一个或多个机构所生产、制造或组装的信息技术系统有关的任何风险。

• 第b款规定，上述联邦机构不得利用任何拨款采购根据第a款规定需要进行评估的信息技术系统，不得采购由中国拥有、管理或资助的一个或多个机构所生产、制造或组装的信息技术系统，除非第a款规定的评估机构的负责人决定并向众议院和参议院的拨款委员会报告，该系统采购符合美国的国家利益。

Information Technology Industry Council

美国网络安全政策需要回到正确轨道

丹妮尔·克里兹（Danielle Kriz）& 白石(Jimmy Goodrich)
美国信息技术产业理事会(ITI)
2013 年 4 月 8 日

我们请求国会审查该规定对网络安全和市场竞争的影响，并就解决这一问题考虑更具有建设性的方法。我们还主张类似条款不再出现在任何其他法律文件中，希望得到你们的支持”

美国“2015年合并与持续拨款法案”第515条

该法案第a款规定，美国商务部、司法部、国家宇航局和国家科学基金会不得利用任何拨款采购NIST SP199中规定的高影响（High-impact）或中度影响（Moderate-impact）的信息技术系统，除非上述联邦机构：

（1）根据NIST制定的有关标准进行供应链风险审查；

（2）通过由联邦调查局或其他相关机构提供的威胁信息审查供应链风险；

（3）联邦调查局或其他机构对与系统采购相关的网络间谍或破坏行为进行了风险评估，包括由美国政府认定实施了网络威胁的一个或多个组织生产、制造或组装的信息系统，包括但不限于由中国拥有、管理或资助的组织；

我国现有政策立法规定

我国将推出的网络安全审查制度规定

审查范围	关系国家安全和公共利益的系统使用的重要技术产品和服务
审查重点	产品的安全性和可控性
审查目的	防止产品提供者非法控制、干扰、中断用户系统，非法收集、存储、处理和利用用户有关信息
如何管理	对不符合安全要求的产品和服务，将不得在中国境内使用

国家网络安全审查的法理基础

国家网络安全审查的制度独立性：

外商投资安全审查 VS 网络安全审查

外资并购国家安全审查制度是为“防止外资进入本国市场而影响国家安全”，其主要通过政府干预，降低外国资本通过直接或间接投资控制本国重要行业的风险，主要关注的是国家经济安全，我国也在2008年的《反垄断法》中建立了外资并购国家安全审查制度。

国家网络安全审查的制度价值：

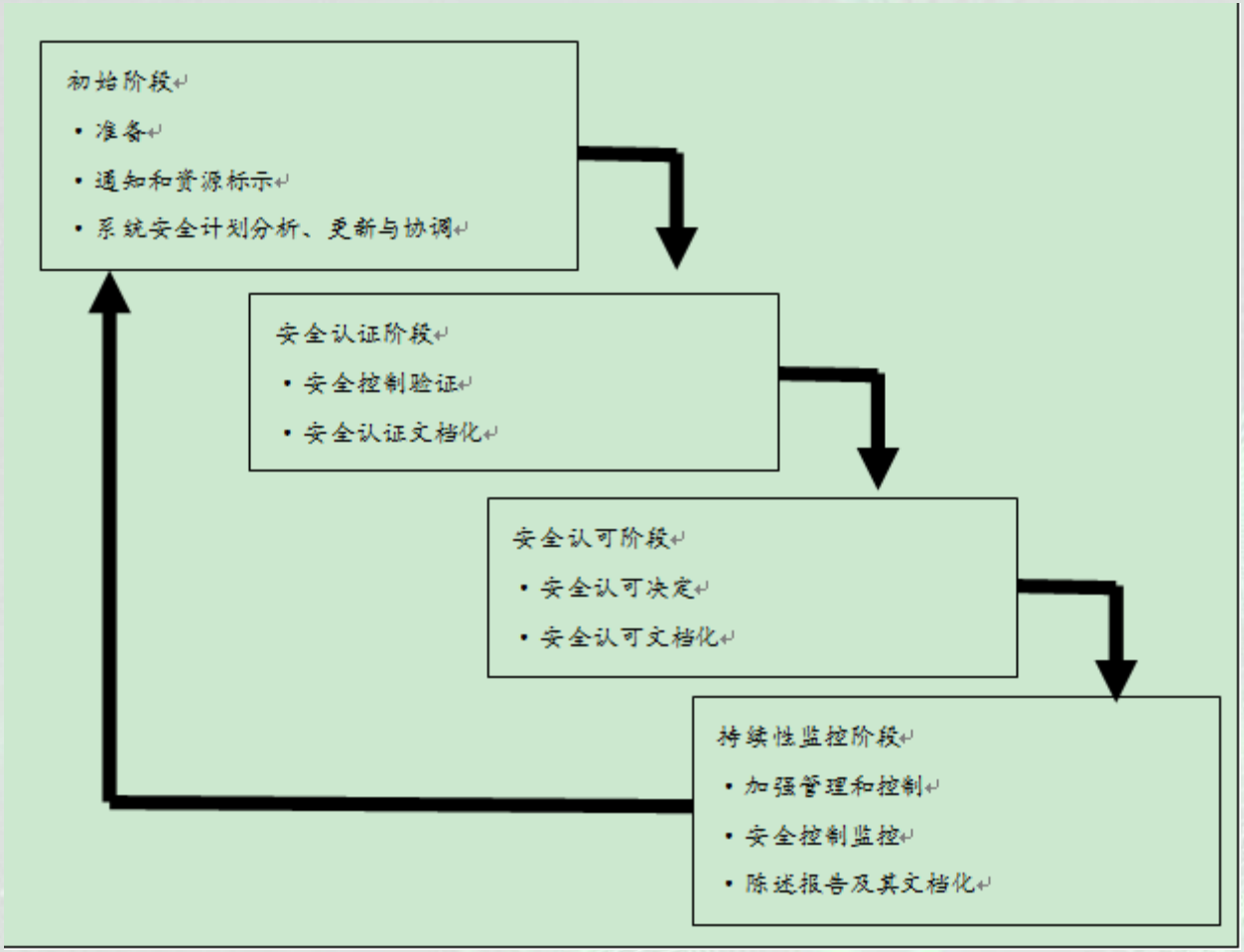
反制措施 VS 风险控制措施

对于信息技术的依赖性是我们的基本判断，国家重要领域和关键部门的持续性运行高度依赖于广泛部署的信息技术产品和服务，其安全性和可靠性成为评估国家网络风险的重要指标。与此相伴的是，网络安全风险正在变得日益严峻，各国政府均毫不讳言地对此表示了担忧。

国家网络安全审查的制度理念：威胁态势感知的引入

节点控制 VS 过程控制

2015年7月，意大利黑客公司“HACKING TEAM”遭黑客攻击，泄露了400G的内部资料。该事件引人注意的并不是资料泄露本身，而是资料披露出该公司向多国政府出售漏洞 进行监控或入侵。这表明使用尚未披露的漏洞进行入侵和攻击在实践中非常有效。因为这类漏洞通常不为公众所知，也缺乏相应的补丁和应对措施，安全审查过程几乎不可能对此进行识别。


初始阶段
• 准备
• 通知和资源标示
• 系统安全计划分析、更新与协调
安全认证阶段
• 安全控制验证
• 安全认证文档化
安全认可阶段
• 安全认可决定
• 安全认可文档化
持续性监控阶段
• 加强管理和控制
• 安全控制监控
• 陈述报告及其文档化

国家网络安全审查的对象：

终端产品和服务VS IT供应链

• 美国政府《国家网络安全综合计划》（CNCI）

美国政府应当建立多元化的全球供应链风险管理，应对试图通过供应链渗透进行未经授权的数据访问、数据篡改及通信信息拦截等供应链风险。

• 美国政府《全球供应链安全国家战略》

进一步阐明美国重点关注威胁供应链系统功能的风险，指出美国政府应当理解并解决那些企图引入有害产品或材料的系统开发和由恶意攻击、事故或自然灾害引发的中断所带来的供应链脆弱性

• 美国政府问责局（GAO）

通过全球供应链提供的IT产品和服务存在威胁，该威胁会降低联邦关键和敏感机构网络和数据的保密性、完整性和可用性，要求联邦机构识别和防范IT供应链风险。

ISC 2016
中国互联网安全大会

360互联网安全中心

国家网络安全审查的实施

国家网络安全审查的三个层次和两大内容

三个层次：

信息技术产品与服务审查

- 安全性和可控性审查；

CIIP持续性运营审查

•2014年美国关键基础设施保护框架，加拿大CYBER RESILIENCE REVIEW）；

国家网络安全状态审查

•2009年美国、2014年澳大利亚，包括网络安全政策审查）。

国家网络安全审查的三个层次和两大内容

两大内容：

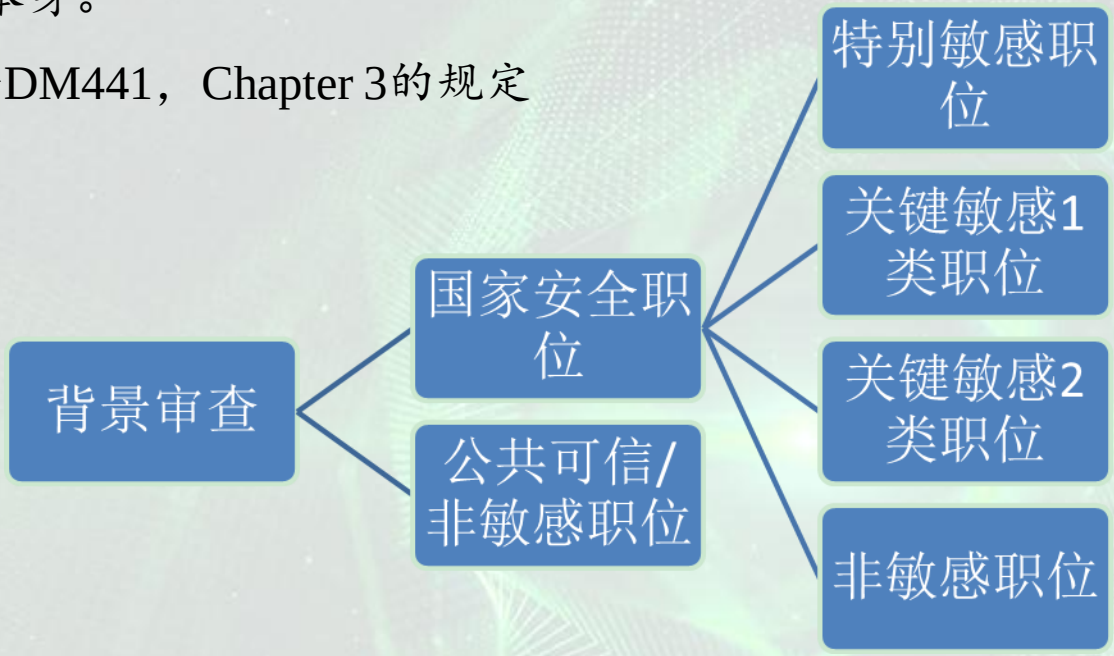
- 人员安全审查（VETTING）

- 技术审查（REVIEW）

美国内政部（DOI）安全审查实证分析

人员审查：背景审查仅针对可能访问DOI信息资源的供应商人员，并不包括供应商本身。

根据DM441，Chapter 3的规定



美国内政部（DOI）安全审查实证分析

DOI信息技术安全审查	
商业现货供应（Commercial Off-the-Shelf）软硬件	
产品质量审查	要求所有的软硬件不存在病毒、木马、蠕虫、间谍程序等恶意代码，并且供应商必须通过合同的方式将该安全保障确定化。
开发和维持客户端应用的服务/外包类信息技术服务/在线支持服务	
背景审查	价值评估审查
培训审查	独立性验证审查
位置审查	认证认可审查
系统开发完整性审查	漏洞分析审查
安全控制审查	

THANK YOU