NSFOCUS

网络安全法解读及安全建设交流

NSFOCUS

Contents

目录

1 网络安全法简介

2 企业实施要点分析

3 绿盟科技解决方案

» 01 网络安全法简介

网络安全法 – 国际背景

合作与共赢

- 2015年9月，习主席访美提出“打造中美合作亮点，让网络空间更好地造福两国人民和世界人民”
- 2015年12月，中美达成了《打击网络犯罪及相关事项指导原则》，
- 2015年以来，中英、中俄、中德先后签署了合作协议。中英，中加德国之间开展高级别对话深化网络犯罪国际合作。
- 2016年11月，习主席在第二届世界互联网大会系统论述了“网络空间命运共同体”的理念，重点提出“四点原则”和“五个主张”的中国方案。

网络安全法 – 国际背景

- 网络冲突和攻击成为国家间对抗的主要形式。
- 网络空间战略和政策升级调整
- 注重安全保障与攻击能力双向提升
- 加强对数据资源跨境传输的管控
- 2015年以来，国家行为体实施的大规模网络监控和网络攻击造成了国家间的严重不信任情绪，对国际局势的稳定带来不良影响。

冲突与对抗

网络安全法 – 国内背景

地下黑产不断扩大，网络攻击越来越多

我国信息化建设的突飞猛进

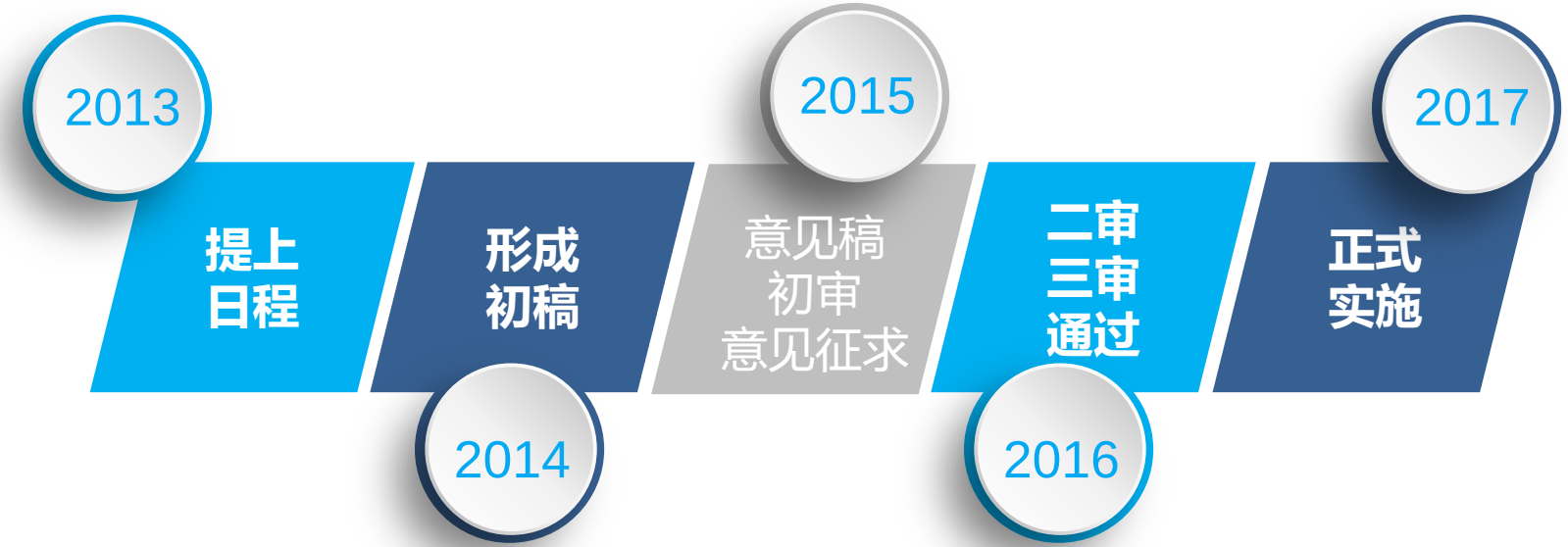
法律法规条文的分散和监管的滞后

大量的网络安全事件和经济损失

新技术的持续发展与应用

网络安全人才建设滞后

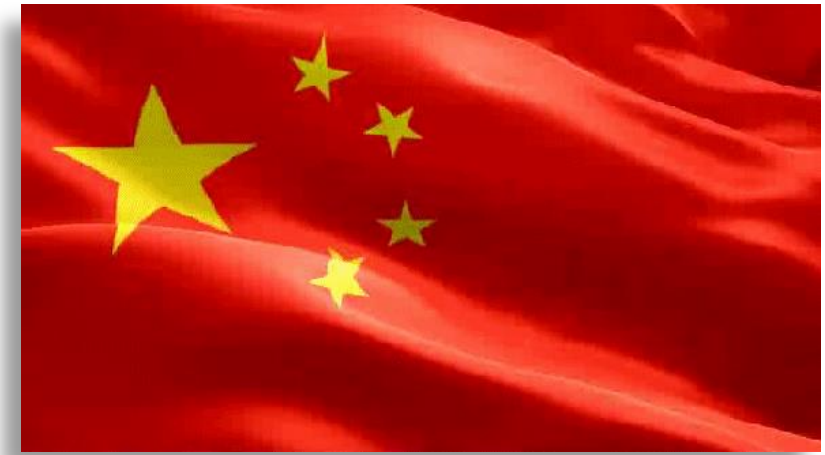
网络安全法 – 制定历程



网络安全法 – 颁布执行

《中华人民共和国网络安全法》

- 2016年11月7日第十二届全国人民代表大会常务委员会第二十四次会议通过
- 2017年6月1日正式实施



网络安全法

亮点

1. 战略入法
2. 确认关键信息基础设施概念
3. 形成综合安全范畴
4. 制度机制衔接有力
5. 综合应对境外网络攻击
6. 注重国家队与社会队的协同
7. 发展并重特色

网络安全法

定位及管辖范围

法律定位

互联网领域网络安全的基础性法律

国内管辖范围

国内管辖权
司法独立权
网络自卫权
依赖性主权

境外管辖范围

攻击行为管辖权
攻击行为防御权
攻击行为惩治权
攻击行为制裁权

网络安全法 – 关键信息基础设施基础定义

关键信息基础设施

指的是面向公众提供网络信息服务或支撑能源、通信、金融、交通、公用事业等重要行业运行的信息系统或工业控制系统，这些系统一旦发生网络安全事故，可能影响重要行业正常运行，对国家政治、经济、科技、社会、文化、 国防、环境及人民生命财产造成严重损失。

来源：中国网信网 http://www.cac.gov.cn/2016-07/08/c_1119185700.htm

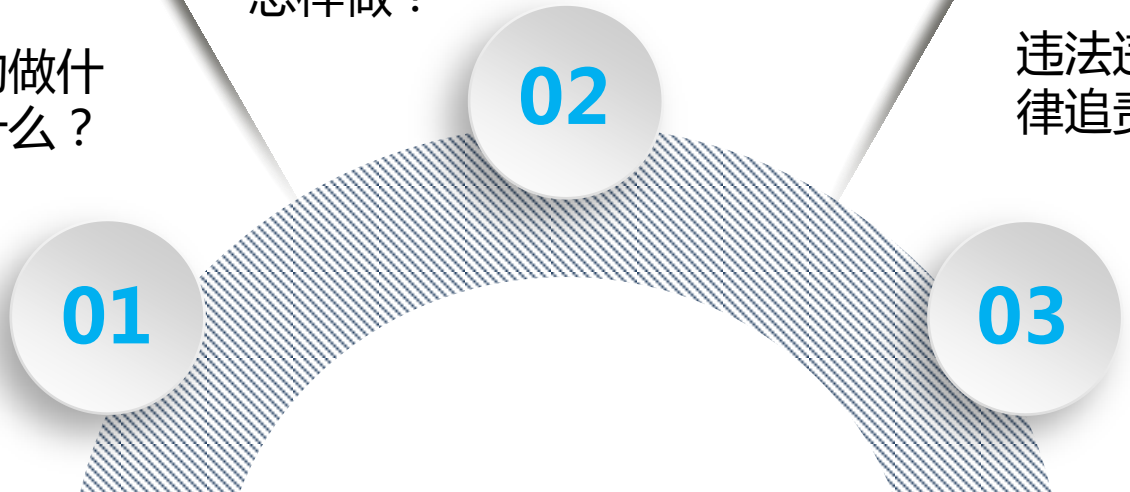
NSFOCUS

网络安全法

关键信息基础设施认定

	认定标准	网络安全事件的潜在影响
网站类	1. 县级（含）以上党政机关网站。 2. 重点新闻网站。 3. 日均访问量超过100万人次的网站。 4. 一旦发生网络安全事故，可能造成右边列影 响之一的。 5. 其他应该认定为关键信息基础设施。	1. 影响超过100万人工作、生活； 2. 影响单个地市级行政区30%以上人口的工作、生活； 3. 造成超过100万人个人信息泄露； 4. 造成大量机构、企业敏感信息泄露； 5. 造成大量地理、人口、资源等国家基础数据泄露； 6. 严重损害政府形象、社会秩序，或危害国家安全。
平台类	1. 地市级以上政府机关面向公众服务的业务 系统，或与医疗、安防、消防、应急指挥、 生产调度、交通指挥等相关的城市管理系 统。 2. 规模超过1500个标准机架的数据中心 3. 一旦发生网络安全事故，可能造成右边列 影响之一的。 4. 其他应该认定为关键信息基础设施。	1. 造成1000万元以上的直接经济损失； 2. 直接影响超过1000万人工作、生活； 3. 造成超过100万人个人信息泄露； 4. 造成大量机构、企业敏感信息泄露； 5. 造成大量地理、人口、资源等国家基础数据泄露； 6. 严重损害社会和经济秩序，或危害国家安全
生产业务类	1. 注册用户数超过1000万，或活跃用户（每日至少登陆一次）数超过100万。 2. 日均成交订单额或交易额超过1000万元。 3. 一旦发生网络安全事故，可能造成右边列影响之一的。 4. 其他应该认定为关键信息基础设施。	1. 影响单个地市级行政区30%以上人口的工作、生活； 2. 影响10万人用水、用电、用气、用油、取暖或交通出行等； 3. 导致5人以上死亡或50人以上重伤； 4. 直接造成5000万元以上经济损失； 5. 造成超过100万人个人信息泄露； 6. 造成大量机构、企业敏感信息泄露； 7. 造成大量地理、人口、资源等国家基础数据泄露； 8. 严重损害社会和经济秩序，或危害国家安全

网络安全法 – 内容解读



产品商、关键基础设施运营者、网络运营者应该做什么，应该怎样做？

国家及监管机构做什么，政策支持什么？

违法违规之后的法律追责是什么？

网络安全法

国家和监管机构

网络安全法

产品商/运营使用者

NSFOCUS

网络安全法

个人信息保护

责任原则

（第四十条）网络运营者对其搜集的用户信息严格保密，建立健全用户信息 保护制度

告知原则

（第四十一条）网络运营 者收集、使用个人信息，应公开搜集、使用规则， 明示搜集、使用信息的目的、方式和范围并经被搜 集者同意

搜集原则

（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、必要原则；不得搜集与其服务提供无关的个人信息

使用原则

（第四十二条）未经被搜 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；（第四十四条）不得非法出售或非法向他人提供个人信息

自主选择原则

（第四十一条）网络运 营者收集、使用个人信息，应经被搜集者同意；（第四十二条）未经被 搜集者同意，不得向他人提供个人信息

完整性原则

（第四十二条）网络运营者不得泄露、篡改、毁损 其搜集的个人信息

安全管理原则

（第四十二条）网络运营 者不得泄露、篡改、毁损其搜集的个人信息

访问及更正原则

（第四十三条）个人发现网络运营者违反法律、行政法规的规定或双方约定收集、使用个人信息的，有权要求删除其个人信息，发现有错误的有权要求网络运营者更正。

预防损害原则

（第四十九条）网络运营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 息安全的投诉与举报

NSFOCUS

网络安全法

法律追责与处罚

	违规行为	单位	负责人
1	未实施等保，未设定安全应急预案	1-10万	0.5-5万
2	未执行三同步，为履行安全义务，未每年开展至少1次安全评估	10-100万	1-10万
3	违法收集、使用、篡改、出售公民信息，未妥善保护公民信息	50万以下 严重吊销执照	1-10万
4	采购安全产品导致安全风险	采购金额 1-10倍	1-10万
5	数据存储国外或向国外提供数据	5-50万 严重吊销执照	1-10万

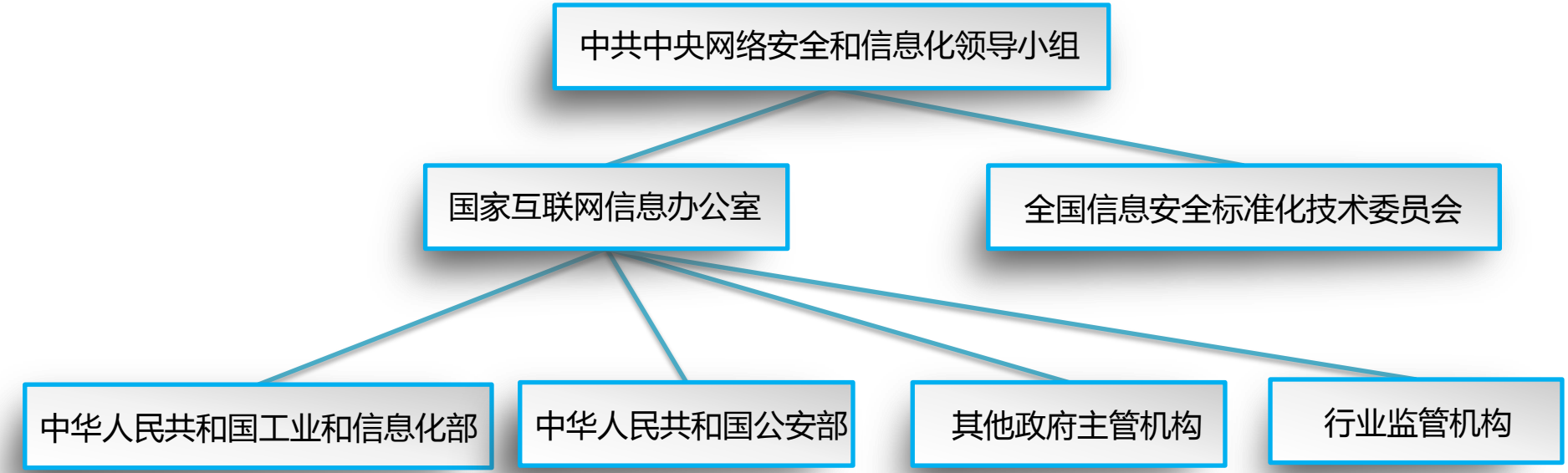
NSFOCUS

网络安全法

法律追责与处罚

	违规行为	单位	负责人
6	协助实施犯罪未构成犯罪的，发布与实施犯罪相关信息的	1-50万 1-15日拘留	10-50万
7	未及时阻止违规信息发布，消除及记录保存	10-50万 严重吊销执照	1-10万
8	未及时上报，未按要求采取措施，未配合国家机关	5-50万	1-10万
9	未及时修补产品缺陷，未合同要求履行安全售后服务	5-50万	1-10万
10	违法开展认证、检测、评估活动，违法泄露风险信息	1-10万 严重吊销执照	0.5-5万

网络安全法 – 监管执行


中共中央网络安全和信息化领导小组
国家互联网信息办公室
全国信息安全标准化技术委员会
中华人民共和国工业和信息化部
中华人民共和国公安部
其他政府主管机构
行业监管机构

小结

我国网络安全法是以预防、控制安全风险与打击网络犯罪活动为特征，建立以等保为基础、关键基础设施保护未重点和综合性监测预警为基本内容的法律宽假和以调动社会网络安全服务机构力量为监管策略的法律体系

02 企业实施要点分析

CIIP认定过程

CII认定

《关键信息基础设施确定指南（试行）》

NSFOCUS

CII认定

	认定标准	网络安全事件的潜在影响
网站类	1. 县级（含）以上党政机关网站。 2. 重点新闻网站。 3. 日均访问量超过100万人次的网站。 4. 一旦发生网络安全事故，可能造成右边列影 响之一的。 5. 其他应该认定为关键信息基础设施。	1. 影响超过100万人工作、生活； 2. 影响单个地市级行政区30%以上人口的工作、生活； 3. 造成超过100万人个人信息泄露； 4. 造成大量机构、企业敏感信息泄露； 5. 造成大量地理、人口、资源等国家基础数据泄露； 6. 严重损害政府形象、社会秩序，或危害国家安全。
平台类	1. 地市级以上政府机关面向公众服务的业务 系统，或与医疗、安防、消防、应急指挥、 生产调度、交通指挥等相关的城市管理系 统。 2. 规模超过1500个标准机架的数据中心 3. 一旦发生网络安全事故，可能造成右边列 影响之一的。 4. 其他应该认定为关键信息基础设施。	1. 造成1000万元以上的直接经济损失； 2. 直接影响超过1000万人工作、生活； 3. 造成超过100万人个人信息泄露； 4. 造成大量机构、企业敏感信息泄露； 5. 造成大量地理、人口、资源等国家基础数据泄露； 6. 严重损害社会和经济秩序，或危害国家安全
生产业务类	1. 注册用户数超过1000万，或活跃用户（每日至少登陆一次）数超过100万。 2. 日均成交订单额或交易额超过1000万元。 3. 一旦发生网络安全事故，可能造成右边列影响之一的。 4. 其他应该认定为关键信息基础设施。	1. 影响单个地市级行政区30%以上人口的工作、生活； 2. 影响10万人用水、用电、用气、用油、取暖或交通出行等； 3. 导致5人以上死亡或50人以上重伤； 4. 直接造成5000万元以上经济损失； 5. 造成超过100万人个人信息泄露； 6. 造成大量机构、企业敏感信息泄露； 7. 造成大量地理、人口、资源等国家基础数据泄露； 8. 严重损害社会和经济秩序，或危害国家安全

三同步建设

（第33条）

同步规划

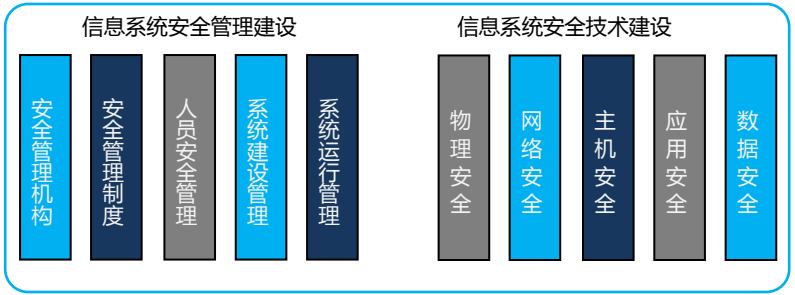
同步建设

同步运维

- 网络安全部门在规划阶段的参与与发言权重
- 系统建设阶段对安全措施的资金预留
- 安全验收与功能验收同等重要
- OP包括IT和Sec
- 安全不只是网络安全部门的的参与

等级保护变化

- 《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27号文件)
- 《信息安全等级保护管理办法》（公通字［2007］43号 ）
- 信息系统安全等级保护实施指南 （GB/T 25058-2010）
- 信息系统安全保护等级定级指南 （GB/T 22240-2008）
- 信息系统安全等级保护基本要求 （GB/T 22239-2008）



- 政策监管要求加强
- 《信息安全技术 网络安全等级保护基本要求》22239新版
- 10项大类缩减至8项大类，但整体内容增加
- 云等保相关标准要求

安全管理

安全机构

安全人员

安全制度

操作规范

安全培训

- 设立专门安全管理机构和安全管理负责人（第34条第1款）
- 制定内部安全管理制度和操作规程（第21条第1款）
- 定期人员安全培训与考核（第34条第2款）

安全技术

网络攻击防护

安全评估

- 采取防护计算机病毒、网络攻击与网络侵入的措施（第21条第2款）
- CII的运营者应自行或委托第三方每年进行至少一次的安全评估（第38条）

安全运维

人员背调

- 刑事和治安记录调查
- 上岗准入

安全评估

- 网络安全评估
- 每年至少一次
- 评估结果上报

应急预案

- 应急预案编制
- 定期修编

应急演练

- 定期演练

安全培训

- 定期培训
- 定期考核

安全运维 - 安全人员背景调查

背景调查的必要项

- 刑事犯罪记录背景调查
- 因泄密等原因受到行政或内部处罚的背景调查
- 国籍调查
- 简历核实调查
- 离职原因调查
- 安全技能调查

背景调查的可选项

- 政治面貌
- 家庭成员及社会关系
- 信用情况

个人信息保护

责任原则

（第四十条）网络运营者对其搜集的用户信息严格保密，建立健全用户信息 保护制度

告知原则

（第四十一条）网络运营 者收集、使用个人信息，应公开搜集、使用规则， 明示搜集、使用信息的目的、方式和范围并经被搜 集者同意

搜集原则

（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、必要原则；不得搜集与其服务提供无关的个人信息

自主选择原则

（第四十一条）网络运营者收集、使用个人信息，应经被搜集者同意；（第四十二条）未经被 搜集者同意，不得向他人提供个人信息

使用原则

（第四十二条）未经被搜 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；（第四十四条）不得非法出售或非法向他人提供个人信息

完整性原则

（第四十二条）网络运营者不得泄露、篡改、毁损 其搜集的个人信息

安全管理原则

（第四十二条）网络运营 者不得泄露、篡改、毁损其搜集的个人信息

访问及更正原则

（第四十三条）个人发现网络运营者违反法律、行政法规的规定或双方约定收集、使用个人信息的，有权要求删除其个人信息，发现有错误的有权要求网络运营者更正。

预防损害原则

（第四十九条）网络运营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 息安全的投诉与举报

个人信息保护

- 机构的规章制度
- 业务评估及需求的明确
- 明确的告知
- 信息数据保护机制
- 企业内控及审计机制
- 法律安全培训

安全产品与服务

网络产品和服务安全审查办法（试行）

2017年05月02日 13:57:12　　来源：中国网信网　　【打印】【纠错】

网络产品和服务安全审查办法

（试 行）

第一条 为提高网络产品和服务安全可控水平，防范网络安全风险，维护国家安全，依据《中华人民共和国国家安全法》《中华人民共和国网络安全法》等法律法规，制定本办法。

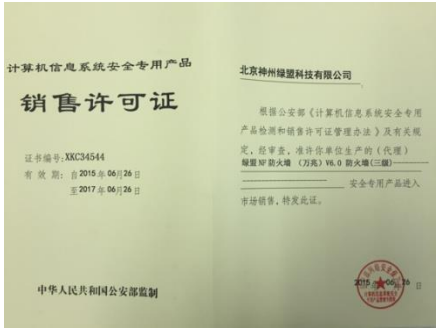
第二条 关系国家安全的网络和信息系统采购的重要网络产品和服务，应当经过网络安全审查。

第三条 坚持企业承诺与社会监督相结合，第三方评价与政府持续监管相结合，实验室检测、现场检查、在线监测、背景调查相结合，对

安全产品与服务

- 网络产品和服务安全审查办法（试行）（共16条）
- 强制认证、采购和使用准入
- 重点审查安全性和可用性
- 工作开展（网络安全审查委员会、办公室）
- 统一认定网络安全审查第三方机构

安全产品与服务 –产品选择


计算机信息系统安全专用产品

销售许可证

证书编号:XKC34544

有效期：自2015年06月26日

至2017年06月26日

北京神州绿盟科技有限公司

根据公安部《计算机信息系统安全专用产品检测和销售许可证管理办法》及有关规定，经审查，准许你单位生产的（代理）绿盟NF防火墙（万兆）V6.0 防火墙(三级)安全专用产品进入市场销售，特发此证。

中华人民共和国公安部监制

中华人民共和国公安部


涉密信息系统

产品检测证书

国保测 2016C04762

兹证明：北京神州绿盟科技有限公司

研制生产的 绿盟NF防火墙（万兆）V6.0

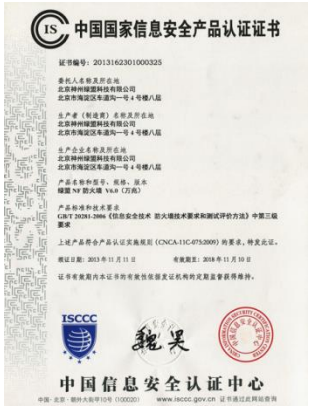
经国家保密科技测评中心检测，符合国家保密标准BMB11-2004《涉及国家秘密的计算机信息系统防火墙安全技术要求》的要求。

本证书有效期自2016年6月15日至2019年6月14日

批准人：

国家保密科技测评中心

国家保密科技测评中心


中国国家信息安全产品认证证书

证书编号：2013162301000325

委托人名称及所在地

北京神州绿盟科技有限公司

北京市海淀区车道沟一号4号楼八层

生产者（制造商）名称及所在地

北京神州绿盟科技有限公司

北京市海淀区车道沟一号4号楼八层

生产企业名称及所在地

北京神州绿盟科技有限公司

北京市海淀区车道沟一号4号楼八层

产品名称和型号、规格、版本

绿盟NF防火墙 V6.0（万兆）

产品标准和技术要求

GB/T 20281-2006《信息安全技术 防火墙技术要求和测试评价方法》中第三级要求

上述产品符合产品认证实施规则（CNCA-11C-075:2009）的要求，特发此证。

认证日期：2013年11月11日 有效期至：2018年11月10日

证书有效期内本证书的有效性依据认证机构的定期监督获得维持。

ISCCC

中国信息安全认证中心

中国·北京·朝外大街甲10号（100020） www.isccc.gov.cn 证书通过此网站查询

中国信息安全认证中心


军用信息安全产品

认证证书

军密认字第1458号

产品名称：绿盟NF防火墙(万兆)V6.0

研制单位：北京神州绿盟科技有限公司

认证等级：军B级

有效期：2015年9月至2017年9月

中国人民解放军

信息安全测评认证中心

2015年7月24日

中国人民解放军信息安全测评认证中心


国家信息安全测评

信息技术产品安全测评证书

证书号：CNITSEC2014N00375

级别：EAL3+

北京神州绿盟科技有限公司

（北京市海淀区车道沟一号4号楼八层 邮编：100089）

绿盟NF防火墙（万兆）V6.0

测评标准：GB/T 18336-2008《信息技术 安全技术 信息技术安全性评估准则》（idt ISO/IEC 15408:2005）

测评方法：《信息技术安全通用评估方法》（idt ISO/IEC 18045:2005）

测评报告编号：4670R20130726-EAL3+

测评机构：中国信息安全测评中心信息安全实验室

此证书仅适用于该产品的上述版本或型号

签发日期：2014年4月22日

有效期至：2017年4月21日

批准人：

中国信息安全测评中心

中国信息安全测评中心信息安全实验室

安全产品与服务 – 服务选择

中国信息安全认证中心

国家网络与信息安全通报中心

国家计算机网络应急技术处理协调中心

ISO27000认证机构

中国信息安全测评中心

中国通信协会

中国人民共和国工业和信息化部

CSA组织

国家保密科技测评中心

出境数据安全

网络产品和服务安全审查办法

（征求意见稿）

第一条 网络产品和服务的安全性、可控性直接影响用户利益、关系国家安全。为提高网络产品和服务安全可控水平，防范供应链安全风险，维护国家安全和公共利益，依据《中华人民共和国国家安全法》《中华人民共和国网络安全法》，制定本办法。

第二条 关系国家安全和公共利益的信息系统使用的重要网络产品和服务，应当经过网络安全审查。

第三条 坚持企业承诺与社会监督相结合，第三方评价与政府监管相结合，实验室检测、现场检查、在线监测、背景调查相结合，对网络产品和服务及其提供者进行网络安全审查。

第四条 重点审查网络产品和服务的安全性、可控性，主要包括：

（一）产品和服务被非法控制、干扰和中断运行的风险；

出境数据安全

- 个人信息和重要书出境安全评估办法（共14条）（意见稿）
- 数据本地化与跨境流动的关系-原则和例外
- 评估的内容
- 模式（行业主管评估，自评估，第三方评估）

运营影响

投入增加

- 个人信息保护条款遵从的资源投入
- 网络运营安全要求条款遵从的资源投入
- 事件报告要求条款遵从的资源投入
- 应急响应要求条款遵从的资源投入
- 违规处罚条款遵从的资源投入

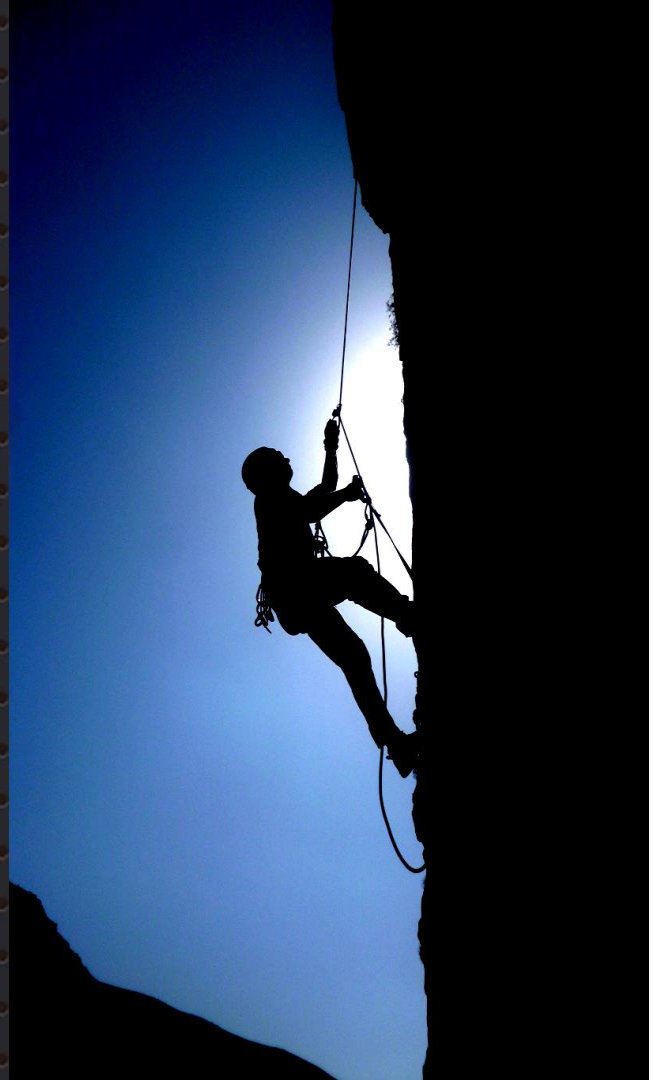
管理主动性

- 等保建设
- 三同步
- 信息安全内控
- 与监管的互动

安全建设重点

- 网络安全评估
- 网络安全审计
- 网络安全应急与演练
- 网络安全培训
- 网络安全内控
- 数据安全防泄漏
- 企业安全管控平台
- 应急响应中心
- 安全漏洞闭环管理
- 未知威胁检测与防护

小结



网络安全法的颁布实施对企业而言从遵从性的角度看是一个前所未有的压力和挑战；从改善内部网络安全治理，更好维护和保障业务运行的角度看则是一个有力的政策抓手和发展契机

» 03 绿盟科技解决方案

NSFOCUS

绿盟安全解决方案

网络安全评估

- 等级保护建设咨询评估
- 网络架构/网络域/网络安全策略评估
- 云安全评估服务
- 业务系统安全评估
- 业务连续性安全评估
- 合规遵从性评估
- 其它类评估

网络安全审计

- 网络安全审计解决方案
- 数据库安全审计解决方案
- 网络安全运维审计解决方案
- 商业银行征信系统安全托管平台解决方案

网络安全应急与演练

- 网络安全应急服务
- 网络安全预案咨询及编制服务
- 网络安全应急演练支撑服务
- 重大时期安全保障支撑服务

网络安全培训

- 网络安全管理培训
- 网络安全意识培训
- 网络安全技能培训
- 安全人员认证资质培训
- 攻防竞技类培训
- 其它类培训

网络安全内控

- 网络安全审计服务
- 网络安全内控咨询服务

安全建设重点

- 企业DLP数据防泄漏解决方案
- 金融行业邮件安全解决方案
- 商业银行征信系统安全托管平台解决方案

数据安全防泄漏

- 安全态势感知解决方案（TSA）
- 互联网资产核查解决方案
- 绿盟企业安全平台解决方案（ESP）

企业安全管控平台

- 绿盟企业安全应急响应中心解决方案

应急响应中心

- 远程安全评估系统
- Web应用漏洞扫描系统
- 绿盟云安全服务（漏扫）
- 网站安全监测服务
- 绿盟威胁和漏洞管理方案（TVM）

安全漏洞闭环管理

- 未知威胁分析系统
- 下一代高级威胁安全解决方案

未知威胁检测与防护

NSFOCUS

Thank You