# 全球网络安全挑战

## 解决供应链风险，正当其时

**安迪 • 珀迪**
美国网络安全官
华为技术有限公司

2016年6月

HUAWEI

# 作者

在此，我想要感谢那些给我提出了宝贵意见并对本文档做出重大贡献的人：John Suffolk、南建峰、王唯践、张静斐、薛勇波、牟德俊、张志亮、Wout Van Wijk、David Pollington、Tero Tammisalo、 王 瑞、 罗 明、Peter Rossi、Hosoi Yoichi、Ulf Feger、Jorg Alexander Albrecht、David Francis，以及其他直接或间接对本白皮书做出贡献的人，恕不一一列举。

安迪・珀迪

# 目录

2016年6月


1 前言 ..... 1

2 引言 ..... 2

3 执行概要 ..... 3

4 前几期白皮书 ..... 5

5 组织应对网络安全风险的成功要素 ..... 6

6 NIST框架—评估组织网络安全的工具 ..... 7

7 供应链风险—组织需要理解并解决 ..... 8

7.1 什么是供应链风险 ..... 8

7.2 组织开始理解供应链风险的重要性 ..... 9

8 应对供应链风险的项目 ..... 11

8.1 SAFECode ..... 11

8.2 Underwriters Laboratory ..... 11

8.3 ENISA ..... 11

8.4 中国政府活动 ..... 12

8.5 英国政府的供应链风险应对方法 ..... 12

8.6 日本 ..... 13

8.7 美国 ..... 14

8.8 EWI ..... 15

9 华为应对供应链风险的方法 ..... 16

10 O-TTPS ..... 21

11 推动变化：怎么促进组织采取行动 ..... 24

12 结束语—共同前进 ..... 26

13 关于华为 ..... 27

# 1 前言

随着时间的推移，客户和政府越来越关注网络安全。2012年以来，我们发布了三版安全白皮书，强调了紧要的事情，但是整个行业仍然没有充分意识到这些事情的重要性；只有通过供应商、客户，以及政策和法律制定者之间的全球合作，我们才能在应对全球网络安全挑战方面取得显著成绩。

虽然目前仍然没有简单的答案或者解决方案可以应对网络安全挑战，但是越来越明显的是，要想在减少网络安全风险方面取得明显进展，需要国际社会以及各个组织采取一些行动，包括在原则、法律、标准、最佳实践、行为准则和协议方面达成一致，而且要取得信任并持续加强这些信任。华为承诺将会支持这方面的努力。

这一版白皮书在华为之前三版安全白皮书的基础上，探讨了我们应对网络安全最大挑战之一——全球供应链风险的方法。

我想以华为董事会副主席和全球网络安全与用户隐私保护委员会主席的身份，再次确定，我们公司将会坚持我们的承诺，继续与所有利益相关方合作，提高我们安全技术设计、开发和部署的能力和有效性，降低信息通信技术（ICT）风险。我们重申这个承诺：

> **我们将支持和采用广义的国际认可的网络安全标准或最佳实践；我们将支持增强网络防御能力的研究工作；我们将继续改善和采用开放透明的方法，让政府和客户能够评估华为的安全能力。最后，正如我们迄今为止所做的一样，我们热烈欢迎政府和客户来帮助我们增强流程、提高技术、改进网络安全的方法，让我们可以为他们以及他们的客户带来更多的利益。**

正如我之前所说，我们坚信，如果技术的使用所带来的创新和能力得以最大化，能够服务更多世界人口，那么世界将会更加美好，也就是说，可以改善人们的生活，提高经济水平。华为将会继续在运营中和我们做的所有事情上坚持开放透明的方针和负责任的立场。

**胡厚崑**

# 2 引言

第四版白皮书属于华为发布的网络安全白皮书系列，这一系列探讨的是全球信息基础设施以及支持和依赖这些设施的组织所面临的棘手挑战，本版白皮书关注供应链风险。组织和消费者需要能够充分利用全球供应链中的信息和通信技术。供应链风险管理并不只是为了确保产品和服务因需而达，还是一种产品生命周期管理方法，减少产品被恶意篡改的风险，减少产品被伪造或包含伪造部件并被恶意利用的风险。

一个组织想要成功，就必须理解和管理所有的网络安全风险，而供应链风险是网络安全风险的一部分。重要的是，要意识到一个组织如果没有全面地执行风险应对措施，就无法较好地应对供应链风险。因此，我们首先要看组织应该考虑的主要因素有哪些，包含他们采用方法中的主要因素，以更有效地管理风险。接下来，在关注供应链风险之前，组织必须要理解其整体网络安全风险和准备状态，其中网络安全风险是重要部分，然后制定和执行风险应对计划。这时就需要美国国家标准与技术研究院（NIST）的网络安全框架。[1]

组织可以把NIST框架作为工具，理解风险，制定方法，以进入更恰当和可持续的风险环境及准备状态。在这个背景下，我们将探讨，一个组织要想进入更恰当、可持续和透明的供应链风险状态，必须做到以下三件事：（1）理解供应链风险会带来什么；（2）知道如何应对风险；（3）受内外驱动而采取行动，并且对其造成的问题进行问责。

利益相关方需要担心的是风险意识。尽管我们也是最近才认识到供应链和第三方风险，而且认识还不全面，但是我们在这方面已经取得长足的进展。在本版白皮书中，我们将探讨供应链风险：什么是供应链风险，有哪些威胁，识别并管理供应链和第三方风险等任务的范围是什么。一些组织至少已经大致理解了风险的重要性，但是其中许多组织仍然无所适从，不太确定需要做什么，尤其是当面对大量标准和最佳实践时。我们将探讨全球为了更好的理解和应对供应链风险正在采取的一些行动。

接下来我们将详细探讨华为应对供应链风险的方法，这并不是说华为的方法很完美，而是分享我们满足客户要求的做法，收集意见，鼓励共享经验，加强利益相关方合作，在减少风险方面取得实质进展。

我们还会探讨帮助组织应对网络安全风险的另一个重要工具：开放可信技术供应商标准（O-TTPS）[2]。O-TTPS关注供应链和第三方风险，是由开放可信技术论坛（OTTF）制定的，华为是论坛的成员。2015年下半年，国际标准组织（ISO）认可了O-TTPS。

在应对供应链风险方面，我们将讨论东西方研究所（EWI）在网络空间项目方面，推动关键网络利益相关方的合作，应对重大和困难的安全问题，我们将特别关注突破小组（由华为、微软和开放组织主导）。突破小组通过为ICT产品制定一种基于已知风险和事实、可应用到全球的框架，促进采用更加安全的ICT产品和服务，并推动其全球可用性。

最后，我们将讨论最重要的问题是：对于意识到供应链风险重要性并知道该怎样去做的利益相关方，如何推动其采取必要行动，并且对其造成的问题进行问责。如果我们能够充分利用ICT技术，让世界更美好，底线就是：政府和主要私营组织需要加大力度，加强协调，在应对供应链风险方面取得更大的进展。

[1] NIST还未将供应链和第三方风险完全纳入框架，但是他们说将会以某种方式（框架覆盖或者路标图）纳入到框架中，方便组织管理从供应商到第三方的风险。

[2] 开放可信技术供应商标准 – 消减恶意篡改和伪造产品(O-TTPS) V1.0， https://www2.opengroup.org/ogsys/catalog/C139

# 3 执行概要

华为网络安全系列第四版白皮书关注供应链风险。组织和消费者需要能够充分利用全球供应链中的信息和通信技术。供应链风险管理并不只是为了确保产品和服务因需而达，还是一种产品生命周期管理方法，减少产品被恶意篡改的风险，减少产品被伪造或包含伪造部件并被恶意利用的风险。

一个组织要想成功，必须理解和管理其风险，包括供应链风险。一个组织如果没有全面地执行风险应对措施，就无法较好地应对供应链风险。各组织意识到并相应地建立起可以帮助组织成功管理风险的制度，是进入更安全的风险状态的重要部分。

对组织建立有效风险管理能力有着重要意义的行动包括：致力于应对安全和隐私风险，建立组织高级领导层主导的内部治理机制，识别组织各部分的要求和基线，执行健壮的验证和合规，将优先级较高的要求纳入到部门/事业部目标和度量指标以及个人绩效指标中，提供激励，促进问责。

接下来，组织必须理解其整体网络安全风险和准备状态，其中网络安全风险是重要部分，并制定和执行风险应对计划。这时就需要NIST网络安全框架。[3]

组织可以把这个框架作为重要的工具，理解风险，制定方法，以进入更恰当和可持续的风险环境及准备状态。NIST框架可以帮助组织采取风险应对措施，这个不依赖于标准的工具可以评估组织的网络安全风险和准备状态，能够制定方法，进入更符合当前风险环境的安全状态。框架中也有标准和最佳实践参考，组织可以根据自己具体需要进行选择。

一个组织要想进入更恰当、可持续和透明的供应链风险状态，必须做到以下三件事：（1）理解供应链风险；（2）需要知道怎么应对风险；以及（3）组织需要受内外驱动而采取行动，如果出现问题就要负责。

虽然作为行业来说，利益相关方需要担心的是风险意识。尽管我们也是最近才认识到供应链和第三方风险，而且认识还不全面，但是我们在这方面已经取得长足的进展。在本版白皮书中，我们将探讨供应链风险：什么是供应链风险，有哪些威胁，识别和管理供应链和第三方风险等任务的范围是什么。ICT产品的供应链可以涉及到来自许多全球化公司的几十个甚至成百上千个部件。对于可能疲于应对自身运营风险的组织来说，应对供应链风险是个严峻的挑战。

依赖ICT的公司慢慢地意识到再也无法忽略或不重视供应链风险。随着意识的提升，关键网络利益相关方不再是偶尔激情地演讲，而是以通力协作的方式在应对供应链方面取得切实的进展。

一些组织至少已经大致理解了风险的重要性，但是其中许多组织仍然无所适从，不太确定需要做什么，尤其是当面对大量标准和最佳实践时。全球采取的行动中至少有一部分与供应链风险相关：SAFECode；Underwriters Laboratory；欧洲ENISA关于供应链完整性的报告；EWI安全项目；英国CPNI和可信软件项目；中国网络安全和

[3] NIST还未将供应链和第三方风险完全纳入框架，但是他们说将会以某种方式（框架覆盖或者路标图）纳入到框架中，方便组织管理从供应商到第三方的风险。

反恐立法；日本政府执行关于供应链风险的战略；美国在能源、国防和金融领域应对供应链危机的项目。

接下来我们将详细讨论华为应对供应链风险的方法，这是华为大型端到端全球保障项目的一部分，意在共享华为实践，收集反馈，促进利益相关方就如何更好地应对供应链风险展开更广泛的对话，在全球ICT供应链中强化信任。

出于向前发展的需要，本版白皮书基于华为安全白皮书的潜在主题和信息：迫切需要全球政府、行业和最终用户进行合作，在如何制定具体行为规范、标准、优秀实践和法律法规方面达成一致，在如何促进和推动减少全球和国家重大网络和通信系统中的隐私和安全风险方面达成一致。

重要的是通过强大的合作，推动供应商在行为规范、标准、优秀实践和法律方面，以及独立的验证机制方面达成一致，以教育和组织ICT买家利用购买力量促进更安全产品的可用性。但是为了达到这个目的，更需要将安全要求，包括风险，告知买家，更需要买家一如既往地根据这些要求购买产品或服务，更需要通过将想法一致的买家聚集在一起沟通共有的要求。

这种需求使得全球认可的工具O-TTPS[4]更重要。O-TTPS最近得到了ISO的认可，可以帮助组织应对供应链和第三方风险。O-TTPS标准对相应的技术行业安全工程和供应链完整性最佳实践进行了识别和分类，系统地采用这些实践可以让商业或政府企业客户认为产品更加安全，更加可信。更重要的是，只有在独立第三方评估机构确认[5]之后，才会授予证书。O-TTPS可以帮助满足ICT供应商和买家的需求，比很多标准更清晰。供应商开发什么产品、如何开发，买家购买什么产品、为何购买，都会受此影响。

我们也将讨论另一个非常重要的问题：怎么激励利益相关方，虽然这些相关方可能理解风险，也知道从网络风险角度怎么做，但是仍需要激励，并且对相关方造成的问题进行问责。很明显的是，如果没有实质的推动因素或激励以及严格的问责机制，很少有组织能够基于风险采取措施。政府和私有组织有责任为制定这些推动因素和激励做出贡献。

[4] 开放可信技术供应商标准 – 消减恶意篡改和伪造产品 (O-TTPS) V1.0， https://www2.opengroup.org/ogsys/catalog/C139 请见ISO/IEC 20243:2015，信息技术 – 开放可信技术供应商TM标准（O-TTPS） – 消减恶意篡改和伪造产品（2015年）http://www.iso.org/iso/catalogue_detail.htm?csnumber=67394

[5] http://reports.opengroup.org/membership_report_all.pdf

# 4 前几期白皮书

在我们的第一版白皮书《网络安全透视：21世纪的技术和安全— 一场艰难的联姻》（2012年9月发布）中[6]，我们坦诚地阐述了华为网络安全方法，以及可能对技术、社会和我们的生活所产生的影响。我们对网络安全进行了概要描述：历史背景、关键参与者以及全球ICT供应链给我们大家带来的挑战。

我们也总结了华为网络安全方法和全球供应链挑战，也为我们参与的行业提供了积极务实的行动建议。我们强调，要想在整体上积极管理网络安全，特别是全球供应链风险，就需要行业里的私有部门和公有部门采取持续透明、公平和合作的方法。

我们也强调，华为致力于与其他全球组织合作、持续创新、共建标准，确保我们所提供的网络解决方案和服务的完整性和安全性能够满足或超越我们客户的需求，并为他们的客户提供必要的保障。第一版白皮书是为了促进全行业对我们的理解而采取的一个具体举措，促进行业理解我们在全球范围内为确保我们将来有一个安全和更好的网络而做出的努力，并就企业和政府在管理全球网络安全挑战方面需要采取的行动提出自己的意见。

在我们的第二版白皮书《构筑公司的网络安全基因——一套综合流程、政策与标准》（2013年10月发布）中[7]，我们详细讨论了我们认为很全面的端到端网络安全流程方法。我们注意到，网络安全是我们的客户非常关注的一件事情，也是政府和供应商非常关注的事情。这也是华为关注的一个焦点，保障网络安全是我们公司的核心战略之一。

当时我们说（现在我们仍然这么认为），只有通过供应商、客户和政策与法律制定者之间的全球合作，我们才能在应对全球网络安全挑战方面取得显著成绩。我们也说过，我们必须共享经验，知道什么行得通、什么行不通，从而减少人们将技术用于恶意目的的风险。

在我们的2014年白皮书《网络安全透视：与你的技术供应商考虑端到端网络安全时的100个要求》（2014年12月发布）中[8]，我们详细阐述了TOP 100要求清单，聚焦于技术购买商向其技术供应商提出的安全问题。我们根据别人向华为提出的问题以及我们针对一系列的标准和最佳实践所做的评估制定了这个清单，希望帮助购买商在招投标时系统性地分析供应商的安全能力。

我们认识到，在很多国家，与网络安全相关的法律和行业要求越来越多。政府和监管机构开始让国家关键基础设施提供商及计算机或信息技术服务提供商承担起网络安全义务和网络安全失败的后续责任。我们乐观的预计，越来越多的公司会被要求提供其网络安全方法，以及分析和评估其技术和服务供应商风险的方法。

TOP 100是一个开始，让组织开始评估供应商的网络安全能力，减少自身的风险。我们说过，我们相信购买者越知情，要求越高，在高质量的安全保障方面的要求越一致，ICT供应商对安全进行投资、提高其安全标准的可能性就越大。我们仍然同意这个观点，本版白皮书中就立足于这个观点。

我们很高兴地看到，EWI已经将TOP 100要求纳入到突破小组的工作中，该组旨在促进更安全的ICT产品和服务在全球的使用，推动其可获得性。期望小组的努力和在线调查会给TOP 100提供输入，帮助其完善。TOP 100可以成为组织和行业领域的好工具，帮助他们定制和创建自己的供应商要求清单。

6 http://pr.huawei.com/en/news/hw-187387-securitywhitepaper.htm#.Vw92Gfl97RY

7 http://www.huawei.com/en/cyber-security/hw_310548

8 http://pr.huawei.com/en/connecting-the-dots/cyber-security/hw-401493.htm

# 5 组织应对网络安全风险的成功要素

本章将讨论为了更有效地管理风险，组织应认真考虑的一些关键举措和活动，包含他们采用的方法。我们认为，这些成功要素是各组织提高安全状态过程中的重要部分。各组织一定要根据自己和其他组织的经验，认识到并建立起关键制度（根据自己的经验、组织架构和文化，以及风险环境进行定制），以成功管理风险，包括在我们第二版和第三版白皮书中提到的问题。

我们认为，解决组织安全风险的关键成功要素是：承诺、管治、清晰的安全要求、一致的流程、个人绩效指标、内部合规，以及透明。

为了成功地管理网络安全和隐私风险，需要在整个组织范围内承诺应对网络安全和隐私等风险。作为整体战略的一部分，组织要系统地将这些风险纳入企业风险管理方案，对当前和未来风险挑战，做到及时知会、分清轻重缓急，成功应对挑战。[9]

每个组织内部都需要清晰地划分与网络安全和隐私风险管治相关的角色和职责，包括整个组织高层和管理层的积极参与，这样高层才能持续地看到风险管理和项目执行的有效性。高层不需要也不应该对风险进行微观管理，但是需要“负责”风险管理流程和结果，而不仅仅只是抽象的承诺。

在全球环境和多样的供应链中，难以控制甚至识别所出现的各种风险，以及可能导致网络安全漏洞、事件或违规的条件。众所周知，不可能消减所有风险，至少在合理的成本范围内无法做到。因此，将网络安全风险纳入到组织风险管理中是至关重要的，包括要建立流程和机制，制定并实施消减计划，这些计划甚至也要涵盖极不可能出现的风险。

每个组织及其关键部门应该针对不同角色制定清晰具体的安全相关要求——与职能和风险相关的网络安全基线。比如，如果一个公司生产某个产品，基线应该保护产品的完整性、可溯性和真实性。同样，承担网络安全相关责任的个人应该将其绩效指标与基线要求、相应部门或业务单元的绩效指标及里程碑对齐。另外，组织应该努力制定一致并且可复制的流程，将该流程嵌入到组织的日常业务流程中，并且根据环境变化不断对其进行优化。

另外一个有效风险管理的基本成功要素就是基于职责分离原则的内部合规和验证项目，确保一直能进行独立评估，确定是否成功满足了组织和个人的要求以及满足程度，改进点和改进原因是什么。

最后，关于组织风险管理进度以及成功与否，组织需要要对客户和利益相关方保持开放透明，这一点是非常重要的。当组织在当前和未来变化的风险环境中不断应对风险时，这种透明，以及个人和组织的责任是必不可少的。

[9] 请见，例如《FFIEC网络安全评估工具：首席执行官和董事会概览》FFIEC（2015年6月， http://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_CEO_Board_Overview_June_2015_PDF1.pdf ）；《第三方关系：风险管理指导》美国货币监理办公室公告栏，2013-29，http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html

# 6 NIST框架—评估组织网络安全的工具

一些组织至少已经大致理解了网络安全风险的重要性，但是其中许多组织仍然无所适从，不太确定怎么评估面对的风险，怎么根据自己的情况制定方法，进入更知情的风险状态，尤其是当面对大量标准和最佳实践时。因此，当讨论NIST网络安全框架时[10]，我们感到很鼓舞，这个框架通过“自愿基于风险[……]的一系列行业标准和最佳实践，帮助组织管理网络安全风险”，被称为“优先、灵活、可复制、基于绩效和性价比高的方法”。该框架“聚焦于通过业务驱动，引导网络安全活动，将网络安全风险作为组织风险管理流程的一部分。”

不论组织可能使用或参考什么标准或最佳/优秀实践（如果有的话），都可以将该框架作为评估风险的好工具。该框架可以作为组织应对风险的一个元素，该框架不依赖于任何标准和供应商，可以评估组织的风险和准备状态，引导组织根据现有风险环境制定方法，进入更合适的安全状态。框架也可以帮助组织比较供应商和业务伙伴的风险状态[11]。对任何想更好理解当前风险状态并进行改进的组织来说，这个框架是个很好的起点。

在我们的第三版白皮书《网络安全透视：与你的技术供应商考虑端到端网络安全时的100个要求》（2014年12月发布）中，我们提出了TOP 100要求清单，聚焦于技术购买商向其技术供应商提出的问题，希望帮助购买商在招投标时系统性地分析供应商的网络安全能力。在白皮书中，我们提到，在面对大量标准时：

> **由于技术的广度，我们永远也无法达成“单一标准”。但是我们可以做的是关注那些在很多标准、准则和最佳实践中经常提到的关键要求（可能措辞有所不同），并让它们聚焦供应商应该共同采取的措施，以改进其产品安全。**[12]

NIST框架[13]的功能很有价值，可以通过购买组织的安全要求/问题清单（如华为的TOP 100）作为很好的补充。

值得注意的是，NIST框架的非正式名字是“风险分析工具”和“翻译引擎”。该框架是个风险分析工具，因为它完全不依赖于任何决定某个组织风险的标准，但是这个框架基于标准和最佳/优秀实践提出了风险分析的方法，所以任何组织都可以使用。该框架指导并告知组织，基于其风险环境以及领域/行业的本质，帮助其决定和实现进入更好风险管理状态的最佳方法。重要的是，该框架并不采用任何一个或一些标准，但是该框架是风险分析工具，可以从风险和准备状态角度帮助组织理解需要考虑什么，该框架也提供了组织可以参考的现有标准，评估风险，制定方法，进入更有意义的风险消减和管理状态。

另外，框架可以被视为风险“翻译引擎”，因为用户不需要知道任何标准或有相关标准的经验，可以直接使用该框架进行组织风险状态评估，与其他（一个或多个）组织的风险状态进行比较，即使其他组织采用的是完全不同的标准。就像从一个语言翻译到另外一个语言的挑战一样，如果没有这样一个风险分析工具，就会很困难、很费时，而且不好比较两个或多个组织的风险状态。重要的是，该框架可以将风险元素映射到任何适用要

[10] 《改善关键基础设施网络安全的框架》V1.0，NIST（2014年2月12日） http://www.nist.gov/cyberframework 请见《网络安全风险管理和最佳实践工作组4：最终报告》（2015年3月）[以下简称WG4最终报告]，请见 http://transition.fcc.gov/pshs/advisory/csric4/CSRIC_WG4_Report_Final_March_18_2015.pdf 和 https://transition.fcc.gov/bureaus/pshs/advisory/csric4/CSRIC_WG4_PresentationFinal_31715.pdf（工作组报告演讲）

[11] 虽然已经写好，NIST还未将供应链和第三方风险完全纳入框架，但是他们说将会以某种方式（框架覆盖或者路标图）纳入到框架中，方便组织管理从供应商到第三方的风险。

[12] http://pr.huawei.com/en/connecting-the-dots/cyber-security/hw-401493.htm 第3页

[13] 《改善关键基础设施网络安全的框架》V1.0，NIST（2014年2月12日） http://www.nist.gov/cyberframework

求或相关的标准，帮助对这些相应标准不理解或没有经验的组织。

在使用该框架时需要记住一个非常重要的概念，组织使用该框架应该出于商业驱动，而且非常重要的是要把网络安全风险纳入到组织的整体风险管理流程中。该框架并不是万能的工具。该框架把当前有效的标准、实践和其他行为规范放到一起，为网络安全使用的众多方法提供了组织和结构，组织可以根据自己在全球市场中的位置、行业领域或子领域以及具体的风险环境进行选择。

NIST框架通过提供以上优势，为那些想更好地理解和管理风险，希望找到评估其他组织风险状态方法的组织提供了起点。本版下文中我们将讨论到，这只是故事的开始，也是非常重要的开始。

# 7 供应链风险—组织需要理解并解决

## 7.1 什么是供应链风险

供应链风险的定义是：“……对手可能故意破坏、恶意引入不需要的功能，或者破坏被保护系统的设计、完整性、制造、生产、分配、安装、运营或维护的风险，意在监视、阻止、干扰或者影响这些系统的功能、使用和运行”[14]，供应链威胁包括：妨害、篡改、伪造、盗版、偷盗、摧毁、毁坏、泄露、渗透、破坏、转移、出口管制违规、腐化、社会工程、内部人员威胁、伪内部人员威胁以及外部所有权。[15]

当然，外部所有权本身不是此类供应链威胁，但是可能会引起网络安全相关的威胁，例如：在其他国家，对实体及其流程和资源的控制与可见度更少；操作可能需要接受第三国安全和隐私相关的管辖和监管；在承包商产品中应用安全和隐私要求时，可能会有困难或需要额外的成本。

更具体的威胁例子如下：（1）硬件或软件上安装恶意逻辑；（2）安装伪造硬件或软件；（3）关键产品/服务的生产或发布出现故障或中断；（4）技术服务依赖恶意或不合格服务供应商；（5）不小心在硬件或软件上安装漏洞。[16]

现在，供应链风险常常得不到解决，或者对紧急信息技术供应链风险的管理不够到位、有效或高效。[17]有两种威胁是恶意篡改和伪造产品。[18]

风险可能会影响供应链上游（如软件或硬件部件供应商，像新品供应商或驱动开发者）和下游（如卖产品给收购方的集成商或分销渠道）。[19]

---

[14] 艾克•斯凯尔顿2011财年国防授权法案第806节，请见 https://www.gpo.gov/fdsys/pkg/BILLS-111hr6523enr/pdf/BILLS-111hr6523enr.pdf。Axelrod, C. Warren，“消减软件供应链风险”，ISACA JOnline，2013年8月，请见 http://www.isaca.org/Journal/archives/2013/Volume-4/Pages/JOnline-Mitigating-Software-Supply-Chain-Risk.aspx

[15] Goertzel, Karen M.等人《OTS ICT供应链风险管理最新报告》美国国防部，信息保障技术分析中心（IATAC）（2010年）第40页 https://www.csiac.org/content/state-art-report-soar-security-risk-management-shelf-ots-information-and-communications-tech

[16] http://www.gao.gov/assets/590/589568.pdf

[17] http://www.gao.gov/assets/590/589568.pdf

[18] 《开放可信技术供应商标准（O-TTPS）– 消减恶意篡改和伪造产品》V1.0（2013年4月9日）第1-2页， https://www2.opengroup.org/ogsys/catalog/C139 （1）恶意篡改产品——提供商生产，通过提供商授权渠道获取的产品，但是被恶意篡改；以及（2）伪造产品：由或为提供商之外的相关方生产，或者通过非授权渠道提供给提供商，伪装成合法产品，实际上不是。

[19] 同上出处，第14页。请见ISO/IEC 20243:2015：信息技术--开放可信技术供应商™标准（O-TTPS）--消减恶意篡改和伪造产品（2015年） http://www.iso.org/iso/catalogue_detail.htm?csnumber=67394

## 供应链威胁和相关方——开放组织

| 相关 / 主要威胁 | 篡改 | | 伪造 | |
|---|---|---|---|---|
| | 上游 | 下游 | 上游 | 下游 |
| 恶意软件 | √ | √ | √ | |
| 未授权部件 | √ | √ | √ | |
| 未授权配置 | | √ | | |
| 不合标准的报废部件 | | | √ | |
| 未授权生产 | | | √ | √ |
| 故意损坏 | √ | √ | | |


被篡改产品是供应链的主要威胁。因此，怎么防止产品被篡改是一项重要任务。一般来说，为组件和产品建立并维护有效的可追溯系统也是一项重要的任务，因为必须要尽可能减少被篡改和伪造产品进入供应链。

## 7.2 组织开始理解供应链风险的重要性

在供应链风险意识方面，我们慢慢取得了一些进步，但是还没有得到广泛认可。本章将讨论为什么组织需要认真对待供应链风险。对于本来就可能勉强应对运营中更传统的网络安全风险的组织来说，应对供应链风险是非常艰巨的任务。ICT产品的供应链可以涉及到来自许多全球化公司的几十个甚至成百上千个部件，涉及多个流程和地理位置。

如上所述，NIST网络安全框架对组织来说是很有价值的工具，一般来说可以更好地理解网络安全风险，也可以帮助制定符合组织情况的风险状态。然而，NIST框架并不能以类似的方式解决供应链风险，2016年NIST可能会以路标图的形式为组织提供解决解决供应链风险的指导。

目前，组织不太从供应商和第三方提供商的角度看待风险，而是更多地从网络或ICT系统用户或运营商的角度思考风险。他们可能会问，别人攻击系统并进行偷窃的可能性有多大，比如，偷窃知识产权或用于身份盗窃的信息，或者只是偷窃有财务价值的东西，以及带来的伤害或损失有多大。他们可能还会问，别人是否可能入侵系统进行破坏或使其崩溃，或者偷偷潜入系统以储备将来进行破坏的能力。

像华为一样，微软也很早就意识到攻击者可能会在整个全球ICT供应链系统中植入并利用恶意的、不需要的以及未授权的功能或伪造元素或部件，破坏或影响技术系统，或者便于监视。这至少对政府和企业来说提出了挑战，必须要意识到，供应链风险是共有的问题，需要利益相关方共同合作，根据标准和最佳实践去找到并实现解决方法。[20]

[20] 《安全：构建全球在线信任第4版：微软看政策制定者》第18页http://www.microsoft.com/en-us/twc/policymakers.aspx

这几年来，全球各国政府—包括美国—已经从原先过度依赖内部研发自己的ICT系统和产品，如硬件和政府现货（GOTS）软件，转变到商业产品，如硬件和商用现货（COTS）软件。大概十年前就很明显地出现了这种转变，政府开始从行业中采购信息和通信技术系统和部件。政府逐渐意识到，内部开发定制满足自己需求的解决方法费时太长，成本太高，而且确实跟不上技术变革的速度。至少他们无法跟得上私有领域创新和新增功能的速度。

因此，政府开始从内部定制开发转向COTS ICT的外部提供商，政府发现这些提供商生产的产品更稳定更创新，产品进化速度更快，成本少了很多。不久，政府就意识到他们转向商业供应商的同时也面临着供应链和产品完整性的风险，这在以前内部开发时并不是个大问题。当政府认真考虑购买COTS ICT时（这个方向是正确的），他们同时也意识到，这种方式使得他们面临更多风险，因为他们不知道，也没法总是简单地找到产品、部件和组件来自哪里，在整个供应链中谁有权限，对所有的ICT产品来说，供应链越来越全球化了。简而言之，他们对产品或部件的完整性和可信度不太有信心，这些产品或部件在供应链中可能被恶意篡改，添加了不需要的功能或方便以后利用的漏洞，或者这些产品或部件包括了伪造部件，同样不可信。

因此，各国政府决定，如果要购买COTS ICT，他们就需要确认购买的COTS ICT来自可信技术提供商，这些提供商在整个产品的生命周期（包括供应链）中遵循最佳实践。同时，涉及到许多恶意攻击者的威胁环境也成了首要考虑的事，随着恶意软件、身份盗窃以及可利用的漏洞的出现和扩散，而且也没有引起人们足够重视，产品用户暴露在对政府及私有网络和系统（包括关键基础设施）的攻击中。

人们普遍认为，将恶意软件引入到系统中可以通过各种机制，包括员工下载钓鱼或鱼叉式网络钓鱼邮件中的附件，连接外部设备（如U盘），访问已被攻击的网站，或者未授权方通过盗窃员工或第三方凭据直接在系统上安装恶意软件，或者在全球供应链中植入。[21]

最近众多事件中，破坏性恶意软件（destructive malware，DM）的使用[22]使得政府和其他关键网络利益相关方更担心以政府和关键基础设施服务为目标的潜在网络攻击，也更担心供应链风险。目前，DM的使用相对不太频繁，却可能是灾难性的，因为DM可以对组织的运营和业务连续性（及依赖运营和业务连续性的组织）带来极大的威胁，DM可以影响数据的机密性、完整性和可用性，可以给组织的攻击恢复能力带来负面影响。针对拉斯维加斯金沙集团和索尼娱乐网络的两起网络攻击就说明了，DM如何影响组织的数据完整性，中断业务运营，伤害品牌名誉。

一般来说，就像网络安全风险一样，供应链风险似乎也有一个规律。通常，从意识到风险，到逐渐认为需要应对风险，再到采取措施真正减少风险，提高信任和保障的过程，都是缓慢而漫长的。对于关注国家安全风险以及政府系统和关键基础设施风险的一些政府机构来说，尤其如此。现在，紧急信息技术供应链风险的解决通常不够有效。[23]有两种重要的威胁是恶意篡改和伪造产品。[24]

这些都影响到开放可信技术论坛（OTTF）的成立以及O-TTPS的发展，本版白皮书稍后探讨。

---

21 《破坏性软件联合声明》FFIEC https://www.ffiec.gov/press/PDF/2121759_FINAL_FFIEC%20Malware.pdf

22 《破坏性软件联合声明》FFIEC https://www.ffiec.gov/press/PDF/2121759_FINAL_FFIEC%20Malware.pdf

23 http://www.gao.gov/assets/590/589568.pdf

24 《开放可信技术供应商标准（O-TTPS）– 消减恶意篡改和伪造产品》V1.0（2013年4月9日）第1-2页， https://www2.opengroup.org/ogsys/catalog/C139 （1）恶意篡改产品 – 提供商生产，通过提供商授权渠道获取的产品，但是被恶意篡改；以及（2）伪造产品：由或为提供商之外的相关方生产，或者通过非授权渠道提供给提供商，伪装成合法产品，实际上不是。

# 8 应对供应链风险的项目

本版白皮书基于华为前三版安全白皮书的主题和信息：迫切需要全球政府、行业和最终用户进行合作，在如何制定具体行为规范、标准、优秀实践和法律法规方面达成一致，在如何推动减少全球和国家网络通信系统的隐私风险和安全风险方面达成一致。

下面我们将与供应链风险应对相关的全球活动和项目作为样例。

## 8.1 SAFECode

卓越代码软件保障论坛（SAFECode）是全球性的非盈利组织，以行业为主导，旨在通过促进更安全和更可靠的软件、硬件和服务的可用性、意识和使用，提高对信息和通信技术产品和服务的信任。[25]SAFECode把领域专家聚集在一起，这些专家在管理软件开发、完整性控制和供应链安全的全球复杂流程方面很有经验。

SAFECode创建了一个框架[26]，在没有适用的国际标准时帮助组织基于流程选择最合适的方法，评估商业技术提供商的开发流程。

## 8.2 Underwriters Laboratory

Underwriters Laboratory (UL)[27]是一家独立的全球性安全公司，他们通过提供“全面功能性安全服务”，帮助保护人们、产品和地点。UL有一个针对众多产品的测试和认证方案，带有UL标记的产品表明其遵守相应的特定要求。比如，UL可以根据已发布的规格，帮助识别出工业控制系统（ICS）里的软件缺陷，帮助提供技术标准以便于管理软件缺陷相关的风险。UL已经启动了一个新的业务线作为网络安全保障项目（CAP），对连接的设备进行测试、评级以及认证，最初主要关注工业控制系统和医疗设备[28]，将来他们希望扩展到ICT产品。

## 8.3 ENISA

欧盟网络和信息安全局（ENISA）最近更新了一篇报告[29]《供应链完整性—ICT供应链风险和挑战概览，以及未

[25] http://www.safecode.org/

[26] Shaun Gilmore (微软)，Reeny Sondhi (EMC)，Stacy Simpson (SAFECode)《软件保障评估原则—商业技术提供商安全开发流程检查框架》，SAFECode，http://safecode.org

[27] http://industries.ul.com/functional-safety/cybersecurity

[28] https://sid4gov.cabinetoffice.gov.uk

[29] 《供应链完整性—ICT供应链风险和挑战概览，以及未来的愿景》，ENISA，第10页 https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/sci-2015。在参考各种供应链工作的表格中，ENISA报告陈述Open Group工作与SCI（供应链完整性）没有什么关系，同上出处第11页。请参见Croll, Paul《供应链风险管理—理解你购买、构建或整合代码里的漏洞》CrossTalk（2012年3月4月）http://static1.1.sqspcdn.com/static/f/702523/17039817/1331310005287/201203-Croll.pdf?token=NawZKwikQkEjI7VEFo86BdQjAKo%3D

来的愿景》，其中推荐供应链参与者遵循可以帮助理解并应对ICT供应链风险的优秀实践。非常重要的是，该报告也推荐政府与私有行业一起合作，制定国际框架，比较评估ICT供应链风险的管理。ENISA推荐框架应该透明、一致且灵活，应该基于风险、好的威胁建模、标准，以及国际贸易关系中的互惠特点[30]。

ENISA报告指出，尽管许多国家、行业和机构担心供应链风险，但是他们的努力太分散，缺乏协同。报告包含了许多他们认为必要的措施，包括：需要一致的观点、实践和度量指标，这些是适当协调项目的前提条件，包括在研发领域；需要独立评审和认证；如上所述的供应链完整性框架；以及需要考虑立法措施。[31]

报告推荐欧洲机构，以及某些情况下的国家政府，采用几乎所有的推荐。关于供应链完整性框架的需求，ENISA推荐由ISO制定度量框架，对供应链完整性进行度量和评估。ENISA报告发布不久后，ISO也将O-TTPS认可为新标准，说明了供应链完整性框架是大家共有的需求。

## 8.4 中国政府活动

我们要讨论几个政府活动：反恐怖主义法和网络安全法草案。

首部中国《反恐怖主义法》（CTL，简称《反恐法》）于2016年1月1日起施行，规定了电信和互联网企业对政府部门调查恐怖主义活动的协助义务，这可能对中国互联网和技术公司的运营产生较大影响。电信和互联网服务提供者应当为政府和国家安全机关进行防范、调查恐怖活动提供支持和协助，[32]但是《反恐法》没有规定要求的程序和文档。《反恐法》也要求互联网服务提供者落实网络安全、信息内容监督制度和安全技术防范措施，防止含有恐怖主义、极端主义内容的信息传播。

2015年7月，中国发布了《网络安全法（草案）》，规定了多项内容，包括网络关键设备和网络安全专用产品的认证和检测[33]，以及关键信息基础设施运营者对网络产品或者服务采购的安全审查制度[34]。草案也包含对关键信息基础设施的运营者本地化个人数据的要求。[35]

## 8.5 英国政府的供应链风险应对方法

英国国家基础设施保护中心（CPNI）向组织发出警告，国家安全威胁可以通过ICT全球供应链中扩散，主要是恐怖主义、民族国家发动的网络攻击，以及大型网络犯罪。[36]CPNI已推荐组织将供应链风险作为已有风险管理方法中的一部分。

CPNI也建议组织实施风险消减计划，包括内容如下：将上下游供应链的各个层级全面匹配到个人合同的级别

---

30 同上出处第5页。

31 同上出处第25-27页。

32 见《反恐法》第十八条

33 见《网络安全法（2015年7月6日草案）》第十九条

34 见《网络安全法（2015年7月6日草案）》第三十条

35 见《网络安全法（2015年7月6日草案）》第三十一条

36 https://www.cpni.gov.uk/highlights/Security-in-the-Supply-Chain

中；根据组织已有的安全风险评估，为每个合同的风险进行打分；对供应商（和潜在供应商）进行尽职调查、认证和保障，通过合同采取相应的合适措施以消减风险；审计安排和合规监控；以及合同退出安排。[37]

总部在英国的可信软件项目（TSI）[38]，由英国政府国家网络安全项目（NCSP）支持和资助，TSI的使命是，在基于风险的整个生命周期过程中，帮助在供应、需求和教育社区中促进可信软件（“让软件更好”）。为了提供指导，TSI已制定了相关标准和最佳实践的纲要，将其纳入到可信软件框架（TSF）中[39]。框架已经通过英国标准机构可公开提供的规范PAS 754:2014《软件可信性规范（治理和管理）》正式化了，该规范“包括技术、物理、文化和行为措施，以及有效的领导和治理方法，以解决五大关键可信方面：安全、可靠性、可用性、恢复力和防护”[40]。

在英国政府内阁办公室和内政部的赞助下，SID4GOV[41]（前身为医疗部门通用的供应商信息数据库）已经修改为在线平台，英国公共部门购买商从同一个在线系统就能获取到供应商信息，促进持续性和信息安全报告。供应商可以直接往平台输入信息，购买商就能获取到单一视图下关于重要供应商的最新数据。SID4GOV门户和数据库由NQC有限公司协调，NQC是2003年由政府采购专家合伙成立的。

NQC通过他们的系统提供供应链服务，方便供应商参与，旨在度量和报告供应商信息，作为整体风险管理的一部分提供供应链保障。NQC支持的数据库可以供购买商使用，查看里面已有的供应商信息。目前，系统里有225,000多家公司资料，估计有1700多家公共行业购买商正在使用这些资料。系统包括供应商填写的公司背景调查问卷，由邓白氏（Dunn and Bradstreet）数据进行补充，还包括持续性、信息保障等的数据收集。问卷是根据特定的采购进行定制，比如食品供应合同，问卷可能包含基于平衡记分卡设计的采购透明度方面的问题。

## 8.6 日本

日本于2015年9月发布了最新的网络安全战略[42]，强调要通过更加重视在设计中构建安全（Security by Design）的方法等，加强组织能力，加强整个组织间供应链的网络安全[43]。在风险管理领域，日本政府将为组织提供网络安全相关管理和制度的支持，制定一个框架以客观评估组织使用第三方认证方式等活动。日本还保证，要通过国际合作，帮助建立起相互认可的安全标准框架，将通过必要的研发以及与东盟和其他国家的区域合作有效地促进供应链风险管理。

在最新的日本关键基础设施保护政策[44]《关键信息基础设施保护的基本政策》[45]中，日本政府“考虑到专业知

---

37 https://www.cpni.gov.uk/highlights/Security-in-the-Supply-Chain/#sthash.v6L3m2o3.dpuf 请参见《供应链风险场景，消减国家基础设施供应链中的安全风险—雇主优秀实践指导》（2015年4月）
https://www.cpni.gov.uk/documents/publications/2015/13-april-2015-mitigating-security-risk-in-supply-chain.pdf?epslanguage=en-gb

38 TSI是非盈利组织，旨在收集、组织和共享英国公私行业和学术中已有的可信软件知识、经验和能力财富，为人们提供明智和精心组织的信息。TSI由许多利益相关方支持，由英国商业创新和技能部(BIS) 以及国家基础设施保护中心(CPNI)的管理董事会领导，请见 http://www.uk-tsi.org

39 http://www.uk-tsi.org/trustworthy-software-framework---tsf

40 http://www.uk-tsi.org/pas754

41 https://sid4gov.cabinetoffice.gov.uk/

42 http://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf

43 同上出处第20页。

44 《关键信息基础设施保护的基本政策》（第三版）（2014年5月19日）信息安全政策委员会（2015年5月25日）（修订版）日本政府网络安全战略总部

45 [原脚注] 信息和通信服务、金融服务、航空服务、铁路服务、电力供应服务、天然气供应服务、政府和行政服务（包括地方政府）、医疗服务、供水服务、物流服务、化工行业、信用卡服务，以及石油行业

识和技能对工业控制系统和其他相关设备的购买及运营来说是非常必要的，因此将促进国际认可的第三方认证方案，对安全合规级别进行客观评估”。[46]

## 8.7 美国

除了NIST[47]，美国有许多网络风险管理和供应链风险管理相关的项目，我们将探讨其中的几个。

美国总统奥巴马的网络安全行政令工作中，美国总务署（GSA）和国防部（DoD）制定并实施六大改革，从恢复力和网络安全风险角度改善美国联邦采购系统，包括为所有联邦采购制定可复制的流程，在整个产品生命周期（开发、采购、维护和处理）中消减网络安全风险。

国防部已将供应链风险的考虑纳入到联邦采购要求中[48]。2015年初，联邦首席信息官（CIO）委员会和首席采购官（CAO）委员会建立了一个工作组，评审当前合同条款以及信息技术采购政策和实践中的承包商信息系统安全。这种跨部门合作由采购、安全和合同管理专家组成，他们的推荐也纳入到了关于加强联邦机构在联邦购买中的网络安全保护指导书初稿中[49]。指导书初稿包括了总务署关于建立“业务尽职”能力的要求，减少联邦供应链中网络相关的威胁和漏洞。指导书终稿即将发布。[50]

行政管理和预算局（OMB）于2015年10月30日发布了《联邦公民政府网络安全战略级实施计划（CSIP）》（OMB备忘录M-16-04）。M-16-04要求美国总务署“开发业务尽职信息服务，帮助政府各部门在整个购买流程中具有识别、评估和管理网络及供应链风险的能力。”[51]

2016年1月，联邦能源监管委员会（FERC）发布了一个最终法规（Final Rule），修改了七个可靠性标准，以保护关键基础设施，解决通信网络和主干电力系统中的供应链网络风险；制定了供应链管理安全控制标准，以保护主干电力系统不受恶意软件威胁和安全漏洞影响[52]。修订旨在保护主干电力利益相关方的通信连接和敏感数据。委员会并没有解决供应链风险管理问题，但是组织召开了一个以员工为主导的技术会议，促进关于供应链风险管理问题方面的对话，帮助决定采取相关行动。

美国金融监管机构联邦金融机构检查委员会（FFIEC）[53]，协调美国六个金融监管组织的风险指导，包括网络安

---

46 同上出处第25页。

47 基于网络安全框架工作，2016年NIST将会组织提供供应链风险指导。除了2015年NIST的特刊，还有《联邦信息系统和组织的供应链风险管理》，SP 800-161, NIST，美国商务部（2015年4月）
http://dx.doi.org/10.6028/NIST.SP.800-161 最近，NIST发布了框架信息请求，潜在刷新以及未来管理， http://www.nist.gov/itl/acd/20151210rfi.cfm

48 DoD 5200.44《可信系统和网络》通过保护项目为关键功能识别和保护建立了政策和职责，CNSS 505。国防联邦收购要求（DFAR），第239.73分篇，《供应链风险相关的信息要求》 http://www.acq.osd.mil/dpap/dars/dfars/html/current/239_73.htm

49 https://policy.cio.gov/

50 https://www.fbo.gov/notices/230732591f542b7da9b9fc3e6c167eec/ 请见 https://www.gpo.gov/fdsys/pkg/FR-2015-05-29/html/2015-13016.htm 2016年4月6日和7日，NIST在马里兰州盖瑟斯堡举办2016年网络安全框架研讨会，请见 http://www.nist.gov/itl/acd/upload/Agenda_Cybersec-2.pdf

51 https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf，第II.d节

52 修改会在最终法规颁布65天之后生效。《联邦法规18章》第40款 [备案号：RM15-14-000]，刷新的关键基础设施保护可靠性标准（2016年1月21日） http://www.ferc.gov/whats-new/comm-meet/2016/012116/E-2.pdf

53 FFIEC由以下美国金融监管机构主管构成：美国联邦储备委员会、联邦存款保险公司、全国信贷联合会管理局、货币监理办公室、消费者金融保护局和州联络委员会。

全相关风险[54]。委员会发布了网络安全评估工具（简称评估）[55]，供各机构评估其网络安全风险和准备状态。美国通货监理局（OCC）检查人员会逐渐把评估纳入到对各种规模的国家银行、联邦储蓄机构及联邦银行分支和机构的检查中。

该项目与上文的英国采购项目相似，只是该项目由私有行业组织和运营。美国国防和航空行业的大公司联盟——洛克希德•马丁（Lockheed）、波音（Boeing）、雷神（Raytheon）、BAE以及Rolls JV——建立了在线可信采购平台，已变成独立公司，被称为Exostar。Exostar公司已建立了一个平台，名称为“全球网络安全信息共享、合作和流程整合的可信工作空间”。[56]本项目促进了供应商风险信息的收集和共享，除了成员的输入，主要的数据收集方式是通过22个问题进行调查。

## 8.8 EWI

EWI网络空间全球合作项目旨在利用和促进关键网络利益相关方的合作，应对重大和困难的安全问题，包括促进更安全的ICT产品和服务在全球的使用，推动其可获得性。该小组正在制定一种基于已知风险和事实、可应用到全球的框架。

2016年EWI将在全球落实、完善及组织关键政府和私有利益相关方对框架的支持。预计EWI的交付件将包括三大关键要素：（1）一系列原则；（2）基于内部（和其供应商）的要求，供应商该考虑的相关标准和最佳实践的纲要；（3）ICT购买商可以采用的机制，通过自己的购买力刺激供应商/提供商提高其安全和产品完整性流程和要求。

[54] www.ffiec.gov/cybersecurity.htm

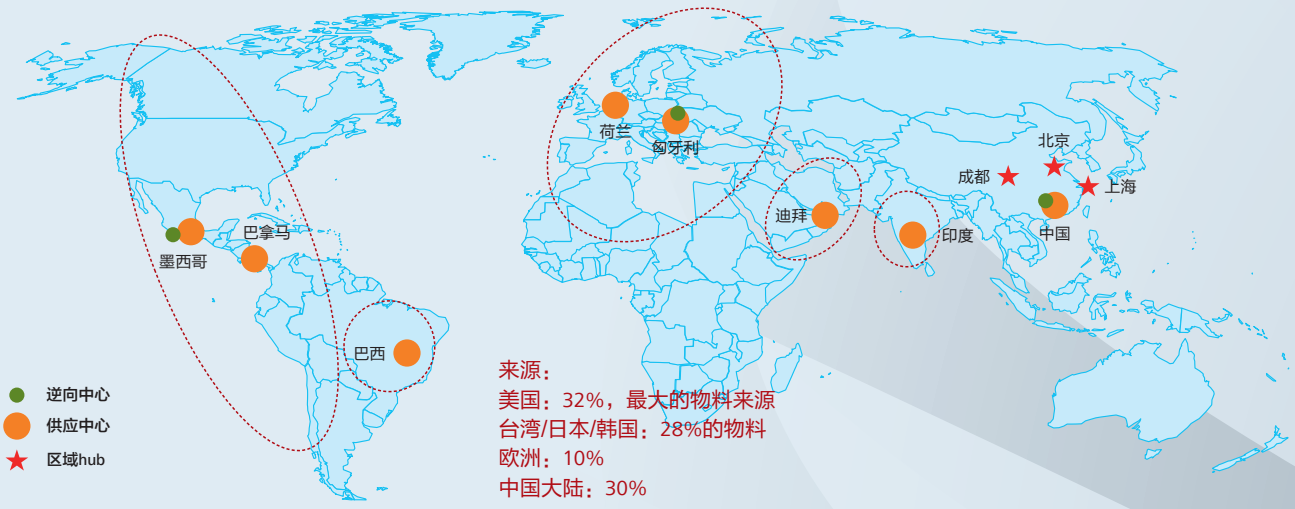
[55] 《FFIEC网络安全评估工具：首席执行官和董事会概览》
FFIEC（2015年6月， http://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_CEO_Board_Overview_June_2015_PDF1.pdf）；
《第三方关系：风险管理指导》美国通货监理局公告栏，2013-29，http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html

[56] http://exostar.com

# 9 华为应对供应链风险的方法

应对华为供应链风险是公司级整体保障项目的一部分。在第二版网络安全白皮书《网络安全透视：构筑公司的网络安全基因——一套综合流程、政策与标准》中，我们详细探讨了相关内容。华为网络安全和隐私管理最高机构——全球网络安全与用户隐私保护委员会（GSPC）负责审批网络安全和隐私保障战略并监督其实施。GSPC成员是网络安全战略背后的决策者和负责者，是网络安全战略在本领域实施的责任人并接受审计委员会的监督。

## 华为全球供应网络




| 供应中心 | 逆向中心 | 本地EMS |
| --- | --- | --- |
| • 中国（面向全球交付）<br>• 欧洲（面向西欧和北非交付）<br>• 拉美（面向巴西以外的美洲区域交付）<br>• 巴西（面向巴西交付）<br>• 印度（面向印度交付）<br>• 迪拜（面向中东交付） | • 中国<br>• 墨西哥<br>• 欧洲 | • 巴西、墨西哥、印度和匈牙利供应中心与本地伙伴合作制造和交付 |

## 全面供应链管理项目

供应链是嵌入到安全保障的业务流程之一，其他流程还有研发、销售和营销、交付以及技术服务。这种嵌入是质量管理系统的基本要求。华为通过进行内部审计、接受外部认证、接受安全机构以及独立第三方机构的审计来加强网络安全保障体系的实施。从2004年起，华为已经通过了BS7799-2/ISO 27001认证。华为遵守相应的网络安全标准并接受的第三方认证（如果适用的话）有ISO 9001、ISO 14001、OHSAS18001、ISO 26000、ISO 27001、TAPA、C-TPAT、ISO 15408等。

华为全面的信息安全管理体系基于ISO 27000标准，包括ISO 27001认证。根据华为的质量保障、信息安全、环境保护和IT保障的要求和流程，以及ISO 28000（供应链安全管理）和C-TPAT10（海关—商贸反恐怖联盟）的要求，华为建立了一个供应链安全管理体系。该体系已经通过了ISO 28000的第三方认证。

华为供应链管理（SCM）体系把产品质量作为其核心战略的一部分，通过活动提高产品质量和流程效率，如六西格玛、优化项目、品管圈（QCC）、传统的意见箱和华为生产系统（HPS）。例如，自2002年启动六西格玛以来，华为的质量工作已经从内部产品质量扩展到了外部客户满意度，从生产延伸到了端到端的供应链流程，如计划和订单管理。通过参考开放可信技术供应商标准（O-TTPS），华为优化了开发和供应链管理实践，下文另作探讨。

华为认为，蓄意破坏会出现在供应链的任何活动中。因此，不仅要关注单一活动，还要关注整个供应链，这很重要。供应链威胁分为两个主要类型——受篡改产品和伪造产品。可以导致受篡改和伪造产品的威胁包括：恶意软件、未授权部件、未授权配置、废弃或不合格部件、未授权生产、蓄意破坏。

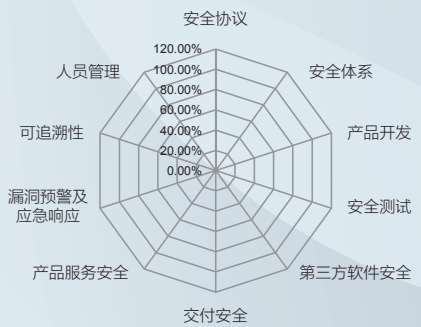
为了应对供应链风险，华为建立了一个符合ISO 28000的全面供应链安全管理体系，从来料到客户交付的端到端流程中识别和控制安全风险。华为根据供应商的体系、流程和产品选择和认证供应商，并持续监控、定期评估合格供应商的交付绩效，选择那些对华为所采购的产品和服务的质量和安全做出贡献的供应商。对于第三方部件，华为会在来料、生产和交付流程中检查其完整性，记录其表现，并建立了一个全流程可视的可追溯系统。

## 供应商网络安全体系认证标准

| | | | |
|---|---|---|---|
| 供应商名称 | | 审核日期 | |
| 考察地点名称 | | 联系人及职位 | |
| 审核组长 | | 审核成员 | |

| 序号 | 项目 | 权重 | 得分率 % | 加权得分 | 备注 |
|---|---|---|---|---|---|
| 1 | 安全协议 | 7% | | | |
| 2 | 安全体系 | 12% | | | |
| 3 | 产品开发 | 18% | | | |
| 4 | 安全测试 | 20% | | | |
| 5 | 第三方软件安全 | 6% | | | |
| 6 | 交付安全 | 5% | | | |
| 7 | 产品服务安全 | 5% | | | |
| 8 | 漏洞预警及应急响应 | 16% | | | |
| 9 | 可追溯性 | 5% | | | |
| 10 | 人员管理 | 6% | | | |
| **综合得分** | | | | | |
| **评价等级** | | | | | |

**审计检查表包括10项要求和49个问题， 每项占总分的权重从5%-15%不等。每项要求包含1-10个问题，用以评估供应商的网络安全。**




| 分数 | 评价等级 | 风险等级 |
|---|---|---|
| <70% | D不合格 | 高风险 |
| ≥70% | C一般 | 中风险 |
| ≥80% | B良好 | 低风险 |
| ≥90% | A优秀 | 标杆 |

# 严格评估供应商

通过全球物流管理流程以及区域和国家的物流流程，华为分层管理（全球——区域——国家）全球物流业务，支撑供应链安全管理体系。华为已经部署了名为HTM（华为运输管理）的IT系统，使得整个运输流程可视、可监控。华为致力于业界最新的安全实践在物流过程中的应用。

## 物流过程透明化管理


**信息准确：**发货到正确地址
**时间准确：**正确时间交货
**配置准确：**发正确的货

**正确的地点：**GPS电子围栏管控
**正确的时间：**派送/签收时间**互锁**，收/验完成上传现场**照片**
**正确的货物：**条码采集

**真实性&完整性检查：**客户可通过网管和电子标签确认设备真实性&配置准确性

# 华为建立了供应链逆向管理流程

华为制定了处理逆向产品的可行方法，我们根据当地法律法规识别可能存在个人数据的部件并对他们在华为产品数据管理系统（PDM）进行标识，优化我们的物流管理系统，以便华为各个分支机构的人员在这些物料出入库时自动进行识别和管控，以满足当地所有针对过时的和逆向产品的要求。为了保证客户数据的安全，如避免逆向设备可能含有敏感数据的风险，华为要求客户在设备返回之前对数据进行清除。

我们制定了供应链网络安全基线，用于确保产品在供应链中的完整性、可追溯性和真实性。基线包括以下方面的要求：物理安全（实物交付安全）、软件交付安全、组织、流程和人员的安全意识。物理安全基线是为了防止可能造成篡改或执行未授权代码的物理接触。

# 供应链网络安全基线

46条采购网络安全红线覆盖了5大类：物料安全、软件外包安全、EMS安全、物流安全和工程服务安全。

| 安全属性 |
| --- |
| 保护个人数据和隐私 |
| 不攻击或破坏客户网络 |
| 无未授权操作 |
| 无后门或病毒 |
| 背景数据安全 |
| 一致性 |
| 不得使用未授权账号 |
| 无未授权访问 |
| 安全测试 |
| 应急响应 |
| 不安装或运行未授权软件 |
| 协议签署 |
| 可追溯性 |
| 培训和教育 |
| 关键人员安全管理 |
| 开源软件安全 |
| 软件外包交付安全 |
| 安全认证 |
| 配置管理 |
| 软件烧录安全 |
| 逆向物料维护安全 |
| 运输安全 |
| 仓库安全 |
| 物流体系安全 |
| 安全防护管理 |

| 采购网络安全基线结构 | | | | | |
| --- | --- | --- | --- | --- | --- |
| 管理类别 | 物料安全 | 软件外包安全 | EMS 安全 | 物流安全 | 工程服务安全 |
| 交付安全 | 无后门或病毒 | 安全测试 | 一致性 | 一致性 | 保护个人数据和隐私 |
| | 背景数据安全 | 软件外包交付安全 | 软件烧录安全 | 运输安全 | 不攻击或破坏客户网络 |
| | 一致性 | | 安全测试 | 仓库安全 | 无未授权操作 |
| | 安全测试 | | 病毒检测和杀毒 | | 不得使用未授权账号 |
| | 开源软件安全 | | 配置安全 | | 无未授权访问 |
| | | | 逆向物料维护安全 | | 不安装或运行未授权软件 |
| | | | 交付安全 | | |
| 保障管理 | 应急响应 | | 应急响应 | | 应急响应 |
| | 协议签署 | 协议签署 | 协议签署 | 协议签署 | 协议签署 |
| | | 安全认证 | 安全认证 | 安全认证 | |
| | 可追溯性 | 可追溯性 | 可追溯性 | 可追溯性 | 可追溯性 |
| | | 配置管理 | | 培训和教育 | 培训和教育 |
| | | | | 关键人员安全管理 | 关键人员安全管理 |
| | | | | 物流体系安全 | 安全防护管理 |

## 华为建立了清晰的基线标准，保证供应链安全

软件交付安全确保软件端到端的完整性，防止对软件的未授权物理访问，并进行技术验证。为了管理来料相关的风险，华为根据来料技术规格、相关质量标准和物料指南进行检验，在产品生命周期的以下每个阶段都遵从专门的流程：采购、开发和供应链。

软件管理是安全管理中一个非常重要的活动。华为在供应链中采用密钥软件安全管理的方法，包括严格的访问控制和物理安全。每个交付给客户的软件版本（VRC）都有一个唯一的物料编号，这个编号贯穿整个软件交付流程。在软件交付流程中，系统会根据合同信息自动生成相关的授权和许可证，同时，系统会自动给制造服务器（ATE）发送软件预加载请求，在ATE测试结束时删除软件。系统之间的所有数据交换都是自动进行的，没有人工干预，从而避免篡改的风险。华为详细记录软件加载和测试的信息，需要追溯某个东西时，比如某个站点设备的软件版本，就可以快速定位。

华为持续改进其支持系统和软件发布平台，支撑服务工程师的工作，向客户提供升级服务，并为客户的自升级提供支持。我们采用一个分级授权管理方法，只有授权的员工才能根据合同或设备需求，申请从Support网站以及软件发布平台下载软件（包括数字签名文件或数字证书）或软件许可证。否则，系统会拒绝登录或下

载——所有的请求以及接受这些请求的人员全部都有记录，以便进行审计。

作为供应链安全管理体系的一个重要部分，华为建立了从物料接收、物料分发、单板制造与测试、整机装配与测试、包装、运输、区域派送整个供应链的追溯链，通过这个追溯链我们可以知道，从哪个供应商采购了什么物料，这些物料使用到了哪些产品上，这些产品加载了什么软件，这些加工好的产品通过哪个承运商发到了哪个国家和客户，以及整个过程中的操作人员是谁等。目前我们生产上已经可追溯的物料类别为258类，包括IC、存储器件、电阻、电容、PCB、焊接使用的锡膏等占生产使用到的物料类别的98%（仅紧固件、标签、包装材料、资料、外壳，以及说明书未追溯）。同时通过和发货合同的耦合以及在区域库房推行条码系统，我们实现了对货物交付客户、合同、软件版本、时间、站点的准确记录。为了实现以上的追溯，我们每年约采集2亿个以上的条码信息，条码涉及到的字段总数超过了300亿个。

华为在软件交付系统（SDP）中建立了可追溯链，记录申请人、审批人、客户名称、合同号、手机号、软件部件号、软件版本以及许可证版本，方便查询和追溯。通过在区域库存中整合合同和编码应用，可追溯系统可以精确地记录产品交付相关的信息、合同、软件版本、时间和站点。

2000年起华为就开始建立了编码可追溯系统，一直不断地完善系统。当前，华为可以在1小时内成功追溯以下信息：

- 采购物料（硬件、软件）信息
- 采购物料（硬件、软件）应用到哪个部件上的追溯
- 部件用到哪个产品
- 部件预加载了哪个软件什么版本以及什么license
- 部件和产品生产过程以及操作人员
- 部件和产品发到哪个国家、哪个客户、哪个合同
- 运输过程
- 客户国库房inbound和outbound
- 生产过程和逆向返回坏件进行维修。

# 10 O-TTPS

一个令人鼓舞可能也非常重要的消息是，现在有一个帮助组织应对供应链安全、第三方提供商、产品完整性的风险并且得到国际认可的工具——开放可信技术供应商™标准（O-TTPS）[57]，O-TTPS最近被国际标准组织（ISO）国际电工委员会（IEC）认可为ISO/IEC 20243:2015[58]标准。新标准提供了一系列规定性要求和组织最佳实践推荐，可以应用到产品的整个生命周期，其中许多与恶意篡改和伪造产品的威胁紧密相关，其他的就比较基础。[59]

应对供应链风险的新标准超过了现有ISO标准的深度和广度[60]，主要因为该标准关注COTS ICT，可应用到供应链里所有的IT提供商，新标准的已有认证项目可以保证合规并通过公开登记信息识别出合规的开放可信技术提供商™。该标准由开放可信技术论坛（OTTF）制定，OTTF由跨行业的提供商和其他利益相关方组成，华为是论坛的成员。OTTF识别并记录收集适用的安全工程和供应链安全最佳实践，通过系统性地使用可以让商业或政府企业客户认为供应商的产品更加安全、可信。作出贡献的成员组织包括许多全球供应商、产品购买商以及第三方测试实验室。

## 开放可信技术论坛

**全球性以行业为主导的计划，为安全工程和供应链完整性定义最佳实践，这样就可以“完整地构建、有信心地购买™”。**


[57] 开放可信技术供应商标准 – 消减恶意篡改和伪造产品 (O-TTPS) V1.1，（2015年7月），第16页 https://www2.opengroup.org/ogsys/catalog/C147 请见ISO/IEC 20243:2015 信息技术--开放可信技术供应商TM标准（O-TTPS）--消减恶意篡改和伪造产品（2015年）http://www.iso.org/iso/catalogue_detail.htm?csnumber=67394

[58] http://www.opengroup.org/news/press/OTTPS-approved-as-ISO-IEC-international-standard. 请见ISO/IEC国际标准（ISO/IEC 20243:2015）请见ISO/IEC 15408：信息技术 – 安全技术 – IT安全的评估准则（通用标准）；ISO/IEC 27000:2009：信息技术 – 安全技术 – 信息安全管理系统 – 概述和词汇；请见供供应商关系中的信息安全，ISO/IEC 27086-1-204，http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=59648

[59] 请见《联邦信息系统和组织的供应链风险管理实践》NIST特刊800-161（2015年4月）http://dx.doi.org/10.6028/NIST.SP.800-161

[60] 请见，例如，ISO/IEC 15026（系统和软件保障：共4个部分的国际标准，提供与生命周期流程相关的“保障案例”）以及ISO/IEC 27036（供应商关系的信息安全：该国际标准关注怎么在供应商和收购商的关系中保护数据问题）

O-TTPS旨在消减被篡改和伪造产品中的风险，这些产品会导致产品故障、性能下降以及安全机制削弱，出现欺骗功能、重大损失以及知识产品盗窃。伪造产品还有几种后果：对客户来说，如果产品在关键时刻出现问题，会影响效率、收入和声誉；对提供商来说，会影响收入流、损害品牌和声誉。

非常重要的是，只有在独立第三方评估机构确认申请公司有足够的证明可以表明其遵从O-TTPS要求之后，才会授予认证。认证的范围可以是整个公司、业务单元或者一到多个产品线。

O-TTPS可以帮助满足ICT供应商和买家的需求，比很多标准更清晰。供应商开发什么产品、如何开发，买家购买什么产品、为何购买，都会受此影响。O-TTPS帮助组织从关注多个标准转移到转变为只瞄准之前多个来源都参考的关键要求，帮助利益相关方关注供应商/生产商应该一起做的事情，共同提高产品安全。

ISO对O-TTPS的认可、应用的广泛度以及对独立验证的要求，正是我们在安全白皮书中呼吁的：需要政府和私有组织在原则、法律、标准、最佳实践、行为准则和协议方面达成一致——必须认识到，已经得到了信任和持续的验证。

在O-TTPS之前，大多数认证都只看产品本身，政府对产品评估的关注是唯一能解决风险问题的方式。然而，这些基于产品的认证无法解决功能和流程的问题，如编码、外包编码、购买开源软件时出现的问题，以及设备制造期间和整个供应链出现的问题。另外，新标准通过满足流程要求，对关于产品安全功能和信息保障的现有标准，如ISO/IEC 15408（通用标准CC），进行了补充。[61]

O-TTPS可信技术供应商的行业最佳实践适用于IT供应链的各个部分：贴牌生产（OEM）、硬软件供应商、集成商以及增值代理商和分销商。

O-TTPS中的最佳实践已按照类别进行组织和定义，每个类别下的部分又包含针对该类别的最佳实践要求。O-TTPS认为，遵从最佳实践类别下要求的组织在管理产品安全风险上是最高效的。

这些类别是开发和制造相关流程中最关键的领域。在这些领域中，“风险管理和保障队COTS技术产品的质量和完整性有着最大的影响”[62]。随着技术提供商（技术部件供应商或产品/解决方案供应商）知道并采用的方法和技术的变化，类别和相关实践也会变化。

O-TTPS的重要类别主要分成两大类：产品生命周期技术开发和供应链安全。在技术开发类别下的COTS ICT产品提供商活动，主要是提供商内部监督是否执行以及执行的方式。

产品生命周期的技术开发类别包括产品开发/工程方法和安全开发/工程方法。根据OTTF当前实践和愿景，可信技术提供商“利用定义好的、有文档的及可复制的产品开发或工程方法和/或流程”[63]，一般通过度量指标和管理层监督管理有效性。

---

61 OTTF™《O-TTPF™ – 促进客户技术收购风险管理的最佳行业实践和推动行业采用的看法》（2011年2月），第5页https://www2.opengroup.org/ogsys/ServePublicationGraphic?publicationid=12341

62 同上出处，第8页

63 开放可信技术供应商标准 – 消减恶意篡改和伪造产品 (O-TTPS) V1.1，（2015年7月），第16页https://www2.opengroup.org/ogsys/catalog/C147，https://www2.opengroup.org/ogsys/catalog/C139 请见ISO/IEC 20243:2015 信息技术 – 开放可信技术供应商™标准（O-TTPS）– 消减恶意篡改和伪造产品（2015年）http://www.iso.org/iso/catalogue_detail.htm?csnumber=67394

同样，当设计和开发产品时，可信技术提供商使用安全工程方法。软件提供商和供应商经常通过方法或流程发现并解决（或补救）可被利用的漏洞，保证产品的安全和可恢复力。硬件提供商和供应商使用流程防止伪造软件或硬件，消减未经认证或已确认伪造的软件中的风险。

O-TTPS中的供应链类别关注的是开放可信技术供应商在采用已定义、监控和验证的供应链流程时如何管理供应链。O-TTPS供应链安全活动关注提供商的最佳实践，这些提供商必须与第三方交互，第三方按照既定的方式为产品的生命周期做贡献。在这里，提供商的最佳实践就是经常控制与外部供应商的交互点，可能包括检查、验证和合同。最佳实践要求和推荐中包括的要求是为了保证整个生命周期中供应链的安全。[64]

O-TTPS的认证项目确保了提供商按照O-TTPS要求采用特定的实践。当一个开放可信技术供应商™认证成功，就有对标准合规的正式认可。

通过描述公司及组织如何安全开发和制造产品，O-TTPS认证项目会提升整个行业对最佳实践的意识和应用。全球技术供应链由消费者、集成商、供应商和制造商组成。虽然只从可信的本地供应商处采购不太可能或者不太实际，但是O-TTPS可以更容易地让ICT购买商在采购战略和决策中对技术产品的完整性负责，让ICT利益相关方承担责任。

[64] 开放可信技术供应商标准 – 消减恶意篡改和伪造产品 (O-TTPS) V1.1，（2015年7月），第15页

# 11 推动变化：怎么促进组织采取行动

没有神奇的方法可以帮助组织从相对无知转变到有供应链风险意识，知道为理解决风险可以做和应该做的事，再到促进具体行动，但很明确的是，只说不做是无法成功的。过一段时间后，我们会面临越来越多的威胁，行动也更加不足，但是大部分的供应链风险不会变少。这就是为什么我们如此支持NIST框架、O-TTPS，以及我们所看到的世界范围内各种积极的行动和努力。这也是为什么我们为华为的三版安全白皮书而自豪。

促进（公有或私有）组织更好理解并减少风险的内外驱动力有很多，其中包括法律法规要求[65]、客户要求/客户合同条款、组织董事会和高级主管（CXO）的尽职要求、保障激励/要求、与竞争对手相比想维持业绩的意愿，以及销售产品和服务的意愿。

尽管正式的政府法律法规是组织采取行动的唯一动力，政府、大型组织、行业集团、智库和学术界都可以作为重要的号召者和推动者，采取行动，通过任何以上列出的促进因素取得显著进展。政府、关键基础设施的所有者和运营者，以及大型私有组织（包括ICT购买商和提供商）都在减少网络、系统、政府服务、关键基础设施和私有组织风险方面发挥着重要的作用。

政府的角色并不局限于对某个经济领域有着法律权威，或者政府是否使用其权威。与其不作为，或者只是等待未来某个带有清晰具体行动甚至建议的完美模型或机制出现，爬-走-跑的风险应对方法更具有优势。等待的风险太大。

在供应方面，全球ICT市场、政府、私有组织和行业集团可以帮助聚集主要的ICT供应商，促进合作，制定他们觉得成为可信提供商所需要的最合理标准、最佳实践和指导。在这些对话中，也可以将O-TTPS和NIST框架作为好的参考文档。

在需求方面，政府或私有集团可以在主要的ICT购买商中发起对话，讨论他们认为供应商应该满足的安全要求。召开关键基础设施重要领域代表的大会可以找到针对特定领域的安全要求。爬-走-跑的方法也许能鼓励领域代表提出一些基本要求，之后再由特定组织根据已知的风险补充更具体的要求，最后领域代表和各个组织根据领域或组织的经验和风险环境的变化进行不断修订。

如果可以的话，这些要求应该嵌入到合同条款中，这样的话，如果出现违规，就有清晰可量化的结果。不同领域和政府的任何共有要求都会实质性地在业务上推动供应商提高满足要求的标准。这是我们第三版安全白皮书《网络安全透视：与你的技术供应商考虑端到端网络安全时的100个要求》（2014年12月）的理念[66]。组织提高网络安全实践标准（包括应对供应链风险的方式）最大的驱动力之一就是销售产品和服务的意愿。购买商的行为对取得实质进步有着重要的作用。

[65] 美国2016年国防授权法案要求国防部长完成所有重大美国武器系统漏洞评估，并于12月31日前提出消减战略，定期向国会和其他人汇报 https://www.congress.gov/bill/114th-congress/house-bill/1735/text#toc-H6234F5DE9FA74324AF387AF9B14DBC16

[66] http://pr.huawei.com/en/connecting-the-dots/cyber-security/hw-401493.htm

政府、私有组织、行业集团等都可以从协作中吸取经验，这样才能决定是否以及怎么修订法律法规的要求，政府和私有组织可以共同通过法规外的促进因素，影响潜在自愿的集体行动。

比如，上述流程可以影响保险公司在制定组织获得保险金额的门槛要求时考虑网络风险，传统观点认为，有了网络风险消减工作，保险可能更加全面，人们可能更加付得起保险。另外，政府和网络保险的主要买家也可以召集保险公司，基于风险更有目标性地共享保险的安全要求。

政府和私有行业可以共同与行业协会、领域群组及各个组织沟通风险的重要性，怎么做才能比领域竞争对手和他人更加理解风险和相关风险状态。这种高层沟通——最好与行业集团和公司管理层合作——可以直接影响组织管理的尽职要求，特别是上市公司。这也可以促进组织管理层采取行动，与竞争对手至少保持一致或部分保持一致，就算不是为了竞争，也要防止与对手不一致而影响名誉。

# 12 结束语—共同前进

让我们回到篇首。我们必须根据已做的工作，树立供应链风险意识，制定行动方法，更加努力地、协同地在更好地理解和应对风险方面取得实质进步。政府和私有行业要合作，双方都不能等待他人采取行动。为了协助保护国家安全、公共安全和执法，政府服务、关键基础设施和私有组织的可用性，以及组织和个人信息的隐私，政府应该作为召集者和推动者（以及必要时作为监管者）利用其能力，希望在私有组织、学术界和政府专家指出的每个方面都能提高供应链意识，促进进步。

组织应该利用已验证的成功要素和活动，更好理解、认真对待以及有效管理网络安全和隐私风险。组织应该考虑NIST或其他类似框架，理解本组织的具体风险状态以及面向未来的风险状态。另外，组织应该重视在整个产品生命周期中供应商和第三方提供商的风险，并认真解决这些风险。

让我们采用已有的工具，如O-TTPS，或至少采用O-TTPS所参考的已验证的方法和流程，最好有独立的验证，这是为了我们的声誉和客户的信任，为了实现各个组织已经做出或应该做出的承诺，为了全球有效应对网络安全和隐私风险。

让我们支持EWI项目的目标和工作，基于ICT领域的原则、风险和事实，促进更安全的ICT产品和服务在全球的使用，推动其可获得性，这样全世界才能共享最现代信息和通信技术的创新、竞争和连接带来的好处。

最后，推动更安全的ICT产品和服务在使用和可获得性方面取得更快更实质进展的最大驱动力，可能就是我们TOP 100要求白皮书里的关键信息：我们需要共同努力，更需要将采购的安全要求告知ICT购买商，更需要买家一如既往地根据这些要求购买产品或服务，更需要通过将想法一致的买家聚集在一起加强并利用购买力，促进采用更安全的ICT产品和服务，推动其可用性，并且对其造成的问题进行问责。

总之，我们希望本版白皮书能够促进更广泛的合作、讨论、理解、承诺和具体行动，减少全球ICT供应链中的风险。

# 13 关于华为

华为是全球领先的信息与通信技术(ICT)解决方案供应商，专注于ICT领域，坚持稳健经营、持续创新、开放合作，在电信运营商、企业、终端和云计算等领域构筑了端到端的解决方案优势，为运营商客户、企业客户和消费者提供有竞争力的ICT解决方案、产品和服务，并致力于使能未来信息社会、构建更美好的全联接世界。目前，华为业务遍及全球170多个国家和地区，服务全世界三分之一以上的人口。我们有170,000多名员工，平均年龄32.5岁，海外员工本地化平均比例为72%。华为LTE已进入140多个首都城市，成功部署400多张LTE商用网络和180多张EPC商用网络。

华为通过不断的创新保持在行业中的领先地位，拥有电信行业最有价值的知识产权组合之一。华为尊重和保护他人知识产权。华为每年将超过10%的销售收入投入到研发，45%的员工从事研发，2015年研发投入596亿人民币（91.8亿美元），增长46.1%，占2015年销售收入的15.1%。近10年累计研发投入超过2400亿人民币（约369.7亿美元）。

截至2015年12月31日，累计获得专利授权50,377件，累计申请中国专利 52,550 件、申请外国专利 30,613 件。相比数量，华为更加关注知识产权的商业价值和质量。从2010年至今，华为已有849项3GPP LTE核心提案获得通过，位居业界第一。在FTTH（光纤到户）、OTN（光传送网）、G.711.1（固定宽带语音）等技术领域持有的专利处于全球领先地位。知识产权保护对华为持续成功至关重要。因此，华为坚决拥护对知识产权的保护。

华为在全球有16个研究所，36个联合创新中心和45个培训中心。约60%的营业额来自于海外。华为使用的70%的物料来自于中国大陆之外的供应商，其中美国的供应量最大，占32%。

华为IT和CT管理服务累计获得超过450个合同；支持全球排名前30运营商中的23家，服务超过85个国家的150多张网络，帮助客户实现卓越运营。华为云计算合作伙伴达500多家，客户1000多家，部署了255个云数据中心。

2015年，智能手机发货超1亿台，同比增幅大于40%。

华为支持主流国际标准，并为这些标准的制定积极做出贡献，加入300多个标准组织、产业联盟和开源社区，担任280多个重要职位，在IEEE-SA、ETSI、WFA、TMF、Openstack、Linaro、OASIS和CCSA等组织担任董事会成员。2015年提交提案超过5,400篇，截至2015年12月31日，累计提交提案43,000篇。

截至2015年12月31日，公司的员工持股计划参与人数为79,563人。员工持股计划将公司的长远发展和员工的个人贡献有机地结合在一起，形成了长远的共同奋斗、分享机制。这让我们能够有长远的眼光，保证在风险、激励和战略之间达成平衡。员工知道如果自己不能很好地服务客户，或者进行不当的活动，他们的股权和奖金将会受到影响。