通过采购提高网络安全和恢复能力

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Improving Cybersecurity and Resilience Through Acquisition		
原文作者	美国国防部， 美国总务管理局	**原文发布日期**	2014 年 1 月 23 日
作者简介	美国国防部是美国联邦行政部门之一，主要负责统合国家安全与武装力量，总部大楼位于五角大楼。国防部设有三个军事部门：陆军部、海军部与空军部。 http://en.wikipedia.org/wiki/United_States_Department_of_Defense 美国总务管理局是联邦政府的采购部门，负责与各类商业企业订立各种长期的政府采购合同，以总额折扣定价的方式为政府采购数以百万计的商品和服务。 http://www.gsa.gov/		
原文发布单位	美国国防部，美国总务管理局		
原文出处	http://www.defense.gov/news/Improving-Cybersecurity-and-Resilience-Through-Acquisition.pdf		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
免责声明	本译文为安天实验室针对网络资料翻译而成，并未取得原作者授权，仅供内部学习和交流使用，安天实验室不对任何可能因此导致的版权问题承担责任。 • 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对		

	原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。

2014 年 1 月 23 日

国土安全部总统助理与经济事务总统助理备忘录

主题：国防部与总务管理局的最终报告

第 13636 号行政命令中第八条（e）《通过采购改善网络安全与网络恢复能力》要求我们向你们建议将安全标准合并入采购计划与合同管理中的可行性，安全效益及其优缺点。

附件是国防部与总务管理局联合工作组就通过采购提高网络安全与恢复能力问题签署的最终报告,该报告为政府全面实行的 13636 号行政命令与 21 号总统政策指令的一部分。

Chuck Hagel
Secretary of Defense

Daniel M. Tangherlini
Administrator of General Services

附录：如上所述

通过采购提高网络安全与恢复能力

国防部与总务管理局的最终报告

2013 年 11 月

这份给美国国防部的报告或研究的预算成本在 2012 - 2013 财年大约是 208,000 美元。预算

成本生成于 2013 年 11 月 13 日，参考号:5-C493D22

前言

美国国防部和美国总务管理局按照第 13636 号行政命令为总统准备了这份报告。该报告提供了一个调整联邦网络安全风险管理和采购流程的途径。

该报告为建议的实行提供了战略指导方针，解决了相关问题，对如何解决挑战提出了建议，并介绍了如何识别重要事项。这些建议的最终目标是：通过改善受到联邦采购系统影响的人员、流程和技术的管理来加强联邦政府网络的恢复能力。

Frank Kendall
Under Secretary of Defense
Acquisition, Technology, and Logistics

Daniel M. Tangherlini
Administrator of General Services

序言

本文是国防部与总务管理局联合工作组的《通过采购改善网络安全与网络恢复能力》的最终报告。该报告是政府执行第 13636 号行政命令与第 21 号总统政策指令的一部分。通过国土安全部综合特别小组的协助，以及与联邦机构和行业利益相关者的合作，本文得以形成。[1]工作组与商务部紧密合作，根据美国国家标准技术研究所(NIST)的降低关键基础设施网络风险的框架(网络安全框架)[2]开发，并与商务部、财政部和国土安全部实行平行的奖励机制,以促进自愿采用网络安全框架。[3] 这个联合发布的报告是跨部门工作组为期 4 个月工作的最高潮，该工作组是由从联邦政府选拔出来的专业知识人才组成的。[4]

网络风险管理和联邦采购系统的不同优先级是改变如何处理联邦采购网络安全的主要障碍之一。[5] 采购工作人员数量要大，[6] 有时在工作中会与政策目标产生冲突，但是网络安全是在任何给定的采购中都要优先竞争考虑的因素之一。网络安全对国家和经济安全的重要性决定了网络风险管理的明显优先级别，因为它既是企业风险管理的一个元素又是采购中呈现网络风险的技术要求。网络安全的重要性相对于其他联邦采购中的优先级别应该加以明确。

该报告旨在提出建议，使得网络风险管理和采购流程在联邦政府更好的协作。报告没有提供明确的实施指导，但为解决相关问题提供了战略指南，报告介绍了如何解决挑战并明确了建议实施中的重要注意事项。

---

[1] The Department established an Integrated Task Force (ITF) to lead DHS implementation and coordinate mteragency, and public and private sector efforts; see, http://www.dhs.gov/publicationlintegrated-task-force.

[2] 78 Fed. Reg. 13024 (February 26, 2013).

[3] See, 78 Fed. Reg. 18954 (March 28, 2013).

[4] Appendix I contains a list of the Working Group members.

[5] See, 48 C.F.R. § 1.102 (2013).

[6] Id.

目录

执行摘要

如果政府购买的产品或服务的网络安全性不足，则风险将持续于整个项目过程。这种产品或服务会带来持续的不利影响，所以改革采购流程对增强网络安全和恢复能力非常重要。在某些情况下，购买有合适网络安全设计和内置的产品和服务可能有较高的前期成本，但这样做能够缓解风险并减少修复漏洞的需要，从而降低了总成本。

联邦政府越来越多的依赖于网络连接、处理能力、数据存储以及其他信息通信技术（ICT）来完成它的任务。政府依赖的网络通常通过购买商业信息通信技术产品和服务得以获取和持续。这些功能大大有利于政府，但在某些情况下，也使政府更容易受到网络攻击。

防御网络风险已成为世界各地的企业和政府领导人的核心战略之一，是企业风险管理策略的重要组成部分。虽然该报告着重建议根据网络安全标准进行采购，[7] 但国防部和总务管理局认为建议的最终目的是加强联邦政府网络的适应能力，而这些则是要通过改善人员管理、流程管理和受联邦采购系统影响的技术的管理来实现。

要注意，这些建议并不与有关国家安全系统（NSS）的采购或网络安全的要求相冲突。国家安全系统委员会（CNSS）负责国家级信息安全保障措施的创建和维护，并提供全面战略规划和运行决策论坛，以保护美国国家安全系统。[8] 国家安全系统委员会还为国家安全系统设立了采购方法，这些方法不在本报告的范围之内。[9] 该建议旨在补充和配合采购国家安

---

[7] The terms "Federal acquisition(s)," or "acquisition(s)," are used throughout this report to mean all activities of Departments and Agencies to acquire new or modified goods or services, including strategic planning, capabilities needs assessment, systems acquisition, and program and budget development. See, e.g., "Big "A" Concept and Map," available at https://dap.dau.mil/aphomelPagesIDefault.aspx.

[8] The Committee on National Security Systems (CNSS) has been in existence since 1953. The CNSS (formerly named the National Security Telecommunications and Information Systems Security Committee (NSTISSC)) was established by National Security Directive (NSD)-42, "National Policy for the Security of National Security Telecommunications and Information Systems. This was reaffirmed by Executive Order (E.O.) 13284, dated January 23,2003, "Executive Order Amendment of Executive Orders and Other Actions in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security" and E.O. 13231, "Critical Infrastructure Protection in the Information Age" dated October 16,2001. Under E.O. 13231, the President re-designated the NSTISSC as CNSS. The Department of Defense continues to chair the Committee under the authorities established by NSD-42.

[9] OMB policies (including OMB Reporting Instructions for FISMA and Agency Privacy Management) state that for other than national security programs and systems, federal agencies must follow certain specific NIST Special Publications. See, e.g., Guide for Applying the Risk Management Framework to Federal Information System: A Security Life Cycle Approach, NIST Special Publication 800-37, Revision 1 (Feb. 2010), and Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53, Revision 4, (Apr. 2013).

全系统的现有程序与方法，并且通过与采购国家安全系统的机构进行磋商得到发展，包括国防情报局、国家安全局、联邦调查局和司法部首席信息官办公室。

这些建议不是孤立创建的。相反，这些建议是联邦政府对网络风险响应策略的一部分。此外，这些建议并没有明确解决如何统一规则。相反，这些建议重点关注了采购规则和将网络安全合并纳入采购技术要求的解释与应用。这些建议归纳如下：

Ⅰ. 将基线网络安全要求作为适当采购的合同条件

基本的网络安全为整个政府和私营部门广泛接受，以此来降低网络风险。对于出现网络风险的采购，政府应该只与满足自身运行与他们提供的产品与服务的基线要求的组织交易。基线应表达采购的技术要求，并应包括业绩考核以确保基线得到了保护，风险得到了识别。

Ⅱ. 在相关培训中解决网络安全问题

正如实践或政策上的任何改变，非常有必要培训相关人员以适应这种改变。将采购网络安全合并到相应人员所需的培训课程中。与政府有业务往来的机构应接受培训要求，培训有关于机构的行政合同中网络安全采购要求。

Ⅲ. 为联邦采购制定共同的网络安全定义

不明确和不一致定义的术语充其量导致达不到效能与网络安全方面的最佳标准。增加联邦采购中关键网络安全术语的清晰度将提高政府和私营部门的效率和效能。关键术语应根据联邦采购法规来定义。

Ⅳ. 提出一项联邦采购网络风险管理策略

从整个政府网络安全的角度来看，识别网络风险采购的危急程度。为了最大限度地保持采购法规应用的一致性，为相似类型的采购开发和利用“重叠”，[10]其始于呈现最大网络风险的采购类型。

[10] An overlay is a fully specified set of security requirements and supplemental guidance that provide the ability to appropriately tailor security requirements for specific technologies or product groups, circumstances and conditions, and/or operational environments.

Ⅴ．要求从原始设备或元件制造商、其授权经销商或其他可靠来源购买

在某些情况下，接收不可靠或其他不合格产品的风险可以通过仅使用来自原始设备厂商、他们的授权经销商、或其他可靠来源的所需产品来缓解。这种来源限制的应用的网络风险临界值应该在整个联邦政府中保持一致。

Ⅵ. 完善网络风险管理的政府问责制

识别和修改政府采购时间有助于网络风险的处理。将完整的安全标准纳入采购计划和合同管理。把网络风险纳入企业风险管理，并确保关键决策者对网络安全管理不足的风险负责。

建议的实施应与行业和政府的广泛持续的关键基础设施和网络安全工作紧密结合，最重要的是综合国家网络安全计划和网络安全框架要在行政命令下进行开发，同时也要与国家基础设施保护计划（NIPP）、相关的部门具体计划威胁和脆弱性的问题上信息共享工作、各部门的各种风险评估和风险管理活动，以及法律法规的变化紧密结合。

网络安全标准正在不断通过透明且一致的标准开发组织（SDO）建立和更新，[11] 基于共识的过程。许多程序是国际性的设计和范围，它们通常包括作为技术开发人员或用户的跨国公司和各种政府机构的积极参与。企业根据他们的角色、业务计划、文化或监管环境，自愿采用由此产生的最佳方法和标准，以最适合他们的独特需求。国际标准的体系架构有利于系统和具有竞争力的商业市场之间的互通性。这也刺激了创新和安全技术的开发和使用。

将自愿性国际标准和最佳方法纳入政府购买在提高网络安全和恢复能力中也十分有效。然而，联邦机构必须使用通过美国国家标准技术研究所开发与实施的标准和指南。[12] 在并购中使用的网络安全标准应调整到尽可能大的程度上与国际接轨，并强调应用组织灵活性的重要性。灵活性是应对动态威胁、制定可行解决方案中至关重要的因素，在整个联邦政府不同的配置和运行环境中都很重要。

---

[11] This includes, but is not limited to, established SDOs like ISO/IEC JTC1 and related standards (27001/2,15408, etc.) as well as work from other international SDOs.

[12] 40 USC § 11302(d) (2013).

几个采购法规的相关变更也正在进行中，并且在实施这些建议的过程中要享有优先权。倘建议与当前的联邦采购法规（FAR）或国防联邦采购规则附录（DFARS）规则制定紧密结合，本文提供了具体参考。一般情况下，建议的实施必须与现有的国际和基于共识的标准以及适用于该领域的法令法规相协调，包括 2002 年联邦信息安全管理法案（FISMA），[13] 1996 克林格科恩法案，[14] 2007 年国土安全部拨款法案，[15] 以及国防授权法案中的相关章节。[16] 最后，建议实施过程中必须与独立监管机构相配合。

虽然它不是主要目标，实施这些建议可能有助于在整个更广泛的经济区域内增加网络安全，特别是在联邦采购方法始终在整个政府中应用，并与实施网络安全框架的其他行动同时进行的情况下。然而，其他市场力量 - 更具体地说是广大客户对于更安全的 ICT 产品和服务的需求 - 对国家网络安全基线的影响将比对联邦采购方法的改变有更大的影响。[17]

联邦采购系统的改变因此应侧重于加强网络安全知识、方法、以及联邦政府的网络和域内的所有功能。实施方法应该充分利用自愿性国际标准的发展和网络安全框架的现有系统。政府应通过改变自有增加网络风险，并侧重于呈现最大的网络风险的方法上，使有限的资源投入提供最大的整体回报。

背景

2013 年 2 月 12 日，总统发了第布 13636 号行政命令，[18] 旨在改善关键基础设施网络安全（EO），以此指导联邦机构使用他们现有权限并增加与为公共部门和私营部门的网络系统的私营部门进行合作，这些网络系统对我们的国家和经济安全至关重要。根据该行政命令，

---

[13] 44 U.S.C. § 3541 et seq.

[14] 14 40 U.S.C. §11101 etseq.

[15] 15 P L. 109-295,120 Stat. 552.

[16] See, e.g., Section 806, Ike Skelton National Defense Authorization Act for Fiscal Year 2011, Pub. L. 1-11 -3 83 (Jan. 7, 2011).

[17] Input received in response to the Working Group's published Request for Information asserts that the Federal government's buying power in the global ICT marketplace, while significant, is insufficient to create a universal change in commercial practices, and reliance on this procurement power alone to shift the market will result in a number of suppliers choosing not to sell to the Federal government. See, General Services Administration (GSA) Notice:. Joint Working Group on Improving Cybersecurity and Resilience through Acquisition; Notice-OERR-201301, available at http://www.regulations;gov/#!documentDetail:D=GSA-GSA-2013-0002-0030.

[18] Exec. Order No. 13, 636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).

总务管理局和国防部成立了工作组履行行政命令第 8（e）条的要求，具体为：

> *（E）"自此命令实行之日起 120 日内，国防部长和总务管理局局长，与秘书和联邦采购法规委员会协商，经负责国土安全和反恐的副总统以及负责经济事务的副总统对其可行性、安全优势和安全标准纳入采购计划和合同管理的相关优缺点进行考量后，向总统提出建议。该报告应涉及可以采取哪些步骤来与现有的网络安全采购需求相协调和统一。"* [19]

通过在政府采购中强调安全标准使用的可行性、安全效益和相关优缺点，关键基础设施网络安全强调了网络风险响应的有效平衡需求，这些响应可能造成成本的增加。此外，采购规则应用的一致性可以推动额外效益。

网络风险与联邦采购

联邦采购是一个跨领域的行动，直接影响各部门和机构的运转。最重要的，它是使政府能够完成使命的一个方法。终端用户最关注的是程序的结果是否具有满足需要的能力。然而，采购能力只是存在网络风险的生命周期、或一系列生命周期的一部分。

联邦政府越来越多的依靠网络连接，处理能力，数据存储，以及其他信息和通信技术（ICT）的功能来完成它的使命。政府所依赖的网络通常通过购买商业信息和通信技术产品和服务来进行采购和维持的。这些增加的功能，极大地有益于我们的政府，但也在某些情况下，使政府更容易受到网络攻击和利用。

联邦政府每年花费超过 5000 亿美金来支付的一系列满足任务需要的产品和服务。这一数额的开支是很大的，但在全球范围内，[20] 它占市场总量还不到 1%。因此，尽管联邦政府是一个重要的客户，它通过购买以影响广泛市场变化的能力并不显著。

---

[19] Id.

[20] https://www.cia.g6v/libfarv/publications/tlie-world-factbook/geos/xx.html

联邦采购鼓励商业项目的采购，部分是通过价格竞争，但更重要的是因为它连接了迅速发展的技术。海外业务已经证明了其作为降低成本的手段的优点，因此大多数商业项目正由全球供应链生产。在美国以外生产的运动也吸引了越来越多的关注，比如外资拥有、控制、操纵，或影响了由政府购买或使用的与重要基础设施或任务基本系统相关的项目。

重要的是，这个问题不是一个简单的地理上的功能问题。系谱[21]是网络风险评估中需要考虑到的因素的一个分支，但在解决零部件和最终产品的安全性或完整性上还有更重要的因素，包括人员、流程和技术开发、交付和操作的谨慎，以及政府及其承包商对使用的产品和服务的处理。

现代信息和通信技术的供应链是复杂的全球分布的系统，是与地理上的路线不同并与多重国际采购层保持逻辑上一致的价值网络。网络该系统包括组织，人员，流程，产品和服务，并延伸于整个系统开发的生命周期中，包括研发、设计、开发、采集商业产品、交付、集成、运行和处置/退役。

漏洞可以有意或无意地被创建并可以来自自身供应链内部或外部。美国的敌对势力（外国政府，军队，情报机构和恐怖组织）和那些寻求推进自己的事业（黑客和犯罪分子）没有考虑到美国的国家安全利益，执法活动，或知识产权的人们给联邦政府和产业带来了重大的新风险。联邦政府及其承包商，分包商和供应商在供应链的各个层次都在遭到越来越多的诡计多端并且资金丰厚的敌对势力不断的攻击，他们旨在窃取、攻陷、改变或破坏敏感信息。在某些情况下，高端的威胁执行者深植于政府的供应链中站稳脚跟，然后选择“逆流而上”以获取敏感信息和知识产权。然而，值得注意的是，大多数已知的入侵不是由对手故意通过其供应链中插入恶意代码到信息和通信技术组件造成的，而是通过利用代码或组件（如远程访问攻击）无意的漏洞实现的。然而，无论是有意或无意的漏洞都会增加风险。为了实现网络恢复能力，联邦政府必须确保它能够缓解新兴威胁带来的风险。

多数联邦技术信息驻留在信息系统容易受为上述威胁和漏洞所困。因此，政府还必须考虑到这些有针对性的网络间谍活动的风险。这些信息往往是不保密的，但它包含有关于关键

[21] Pedigree is concerned with the original creation and subsequent treatment of ICT hardware or software, including computational objects such as programs and data, and changes from one medium to another. It emphasizes integrity, chain of custody and aggregation rather than content. It is a tool for establishing trust and accountability in information or an end item. See, e.g., Wohlleben, Paul, Information Pedigree, (July 29,2010); available at: http://www.fedtechmagazine.com/article/2010/Q7/inrormation-pediaree.

任务系统要求的数据和经营理念，技术，设计，工程，生产系统，及零部件制造的知识产权。对这些信息的攻陷会严重影响联邦系统的运作能力。

近日，假冒伪劣问题，“灰色市场”或其他不合格的信息与通信技术的部件和子部件的问题也已获得大量的关注。这些材料可以在初始采集和维持过程中引入到系统中。由于他们是不太可能有利于测试和维护，他们为终端客户创造漏洞，增加过早系统故障的可能性或创建潜在的安全漏洞，这些都可能会遭到对手的攻击。

此外，重大风险也呈现在操作维护阶段和处置过程。例如，未能更新到最新的安全配置文件，及时安装软件补丁，或不设置身份和访问管理要求的都将导致网络风险，但这些可以通过信息和通信技术采集过程进行管理。同样，对手可以从不当毁坏的媒体中提取有价值的数据。一个业内人士承认商业实体的不正确处理数据造成的风险比由丢失或窃取引起的数据外泄所造成的风险要高三倍，并且比涉及丢失财务信息的数据外泄所产生的风险高出六倍。[22] 此外，信息通信技术供应链很容易受到诸如知识产权盗窃、[23] 服务中断、[24] 以及假冒产品的使用。[25] 当处理临界系统或组件时，这些事件的后果是很重大的，它们会影响安全，安保，和可能数以百万计的人的隐私。

而商业信息通信技术供应链不是所有网络风险的来源，它为威胁和漏洞提供产生的机会，并且商业信息和通信技术激活了网络开发的必要元素连通性。此外，如果联邦政府采用一个不具备充分网络安全的解决方案，政府将在整个产品或服务的生命周期中遭受更多的风险，或者至少要导致修复计算机安全隐患的额外支出。它是网络安全漏洞的持久影响，因此采购对实现网络安全和恢复能力非常重要。在某些情况下购买那些具有网络安全设计的产品和服务可能更昂贵，但这样通过提供风险缓解和减少修复使用和处置过程中产生的漏洞却降低了总成本。

---

[22] Joint Working Group on Improving Cybersecurity and Resilience Through Acquisition, Request for Information, 78 Fed. Reg. 27966 (May 13, 2013) (hereinafter, "GSA RFI").

[23] See, e.g., "IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property" 2, The National Bureau of Asian Research (May 2013).

[24] See, e.g.," White Paper: Managing Cyber Supply Chain Risks," 5, Advisen Inc., (May 2013); available at: http://vmw.onebeaconpro.corn/sites/OneBeaconPro/blind/Advisen%20Supply0/o20Chain%20Risks%20Report.pdf.

[25] See, e.g., Section 818 "Detection and Avoidance of Counterfeit Electronic Parts," FY 2012 NDAA (PL 112 -81); and Defense Federal Acquisition Regulation Supplement: Detection and Avoidance of Counterfeit Electronic Parts (DFARS Case 2012-D055), Proposed Rule, 78 Fed. Reg. 28780 (May 16,2013)

减轻网络风险的重要途径就是遵守安全标准。联邦合同目前需要符合一系列安全标准，例如联邦采购条例，国防联邦采购条例补充，总务管理局采购手册，以及国土安全部采购手册中。政府可以通过一个成本效益好的方法利用安全标准，通过提高与其所适用的标准特异性和一致性来增加自身价值。[26] 通过确保合同要求是明确的，其中的特定标准的部分，更确切地说，需要对所获取的项目明确阐明的安全需要应用该标准。

这个任务适合一个有选择性的方法来完成，因为所有采购不会带来同一级别的风险。对于一些采购，基本的网络安全措施都是要充分解决所有的风险的，而对于其他采购，附加的网络安全控制是必需的。差异主要是由使用的被采集项目适应度不同造成的，这与终端用户的风险承受能力密切相关。例如，同一台打印机/复印机由两个不同的组织来执行同样的功能可能合法地根据工作环境和终端用户要求不同的安全保护。终端用户彼此风险承受能力上的差异可以根据许多其他的事物来决定，相关信息的敏感性和任务界性的差异与特定的部门和机构的技术操作有关。

政府必须努力确保以任务为基础的网络安全对产品的要求与实际购买的产品之间要匹配。需要注意的是必须执行美国国际协定义务，并切在联邦采购中自愿性国际标准随时被应用。最后，政府必须继续努力创新提高网络安全的标准。

建议

商业信息和通信技术在联邦网络中无处不在，即使是那些处理最敏感的信息和支持政府基本职能的地方。因此，建议主要集中在揭示与信息和通信技术采购有关的网络风险以及如何解决这些网络风险。然而，由于世界与日趋复杂的威胁的联系越来越紧密，本建议同样适用于信息和通信技术传统定义范围外的采购。

Ⅰ.将网络安全基线要求作为适当采购的合同条件

网络安全基线是指用来阻止未经授权的泄露、丢失，或危害的一级信息和安全措施。基本保护例如[27]更新病毒防护，多因素逻辑访问，确保数据的保密性的方法，以及当前在政府

[26] In some circumstances, this will reduce costs by reducing the level of effort required by the contractor to figure out which specific controls in a standard apply to the acquisition; see e.g., Microsoft response to GSA RFI, available athttp://www.regulations.gov/#!documentDetail;D=GSA-GSA-2013-0002-0005.

[27] This list is intended to be illustrative only.

和私营部门被广泛接受的安全软件补丁，能够减少网络风险的比例。当联邦政府直接或间接地与那些没有将基线网络安全保护纳入自己的业务和产品中的公司进行业务往来，将会增加风险。要确保人员，流程，以及接触风险中的资产的技术采用基线的要求提高了整个联邦企业网络安全的水平。

第一级保护措施通常作为开展业务基础课的一部分。不使用基本的网络安全措施将严重损害承包商和联邦商业运作，从而降低系统性能并导致有价值信息的潜在损失。同样需要认识到，为了保护信息系统而设计的慎重的经营手法是典型的日常运行的共同部分。因此，通过网络安全基线要求保护和减少信息系统脆弱性的效益为承包商和政府提供了重大的价值。

基线应符合用于采购的技术要求，并应包括绩效评估，以确保基线被保持，在整个进行采购的产品或服务的生命周期中风险已被识别。由于资源限制和联邦采购的不同风险状况，政府应该采取渐进的，基于风险的方法来增加其合同中超越基线网络安全的要求。

作为预备事项，网络安全要求必须是明确而且在合同具体阐述的要求范围内。通常情况下，网络安全要求均以符合大致规定标准的条款所宣告，并包括在合同不是政府寻求采集的产品或服务的技术说明部分的章节中。[28] 这种做法留下来太多不明确的问题，例如网络安全措施实际上存在于已交付的条款中。该建议预想了对承包人运行的基线网络安全要求，以及交付给政府的产品或服务的要求。

这一建议是为了与正在进行的联邦采购法规（FAR）和国防联邦采购规则附录（DFARS）的制定相协调，规章制定的主题为 “承包商信息系统的基本维护，”[29] 和“保护未分类控制的技术信息。”[30]

II. 在相关培训中解决网络安全问题

正如任何做法或政策的改变，培训相关人才以适应这种变化具有即时的必要性。特别是当改革涉及重大行为变化，例如在这些建议中列出的风险管理变化。此外，政府应实施针对

---

[28] See, Comment on FR Doc # 2013-11239, GSA-GSA-2013-000-000S, Nicholas, J. Paul, Microsoft: Corporation (Jun. 12,2013), available at http://www.regulations.gov/#!docketBrowser;rpp=I00;so=DESC;sb=docId;po=0;dct=PS; D=GSA-GSA-2013-0002.

[29] 77 Fed. Reg. 51496 (Aug. 24,2012), Proposed rule, FAR Case 2011 -020.

[30] DFARS Case 2011-D039, Interim Rule, under review by Office of Information and Regulatory Affairs (last accessed, June 10, 2013. http://www.acq.osd.mil/dpap/dars/opencases/dfarscasenum/dfars.pdf).

行业利益相关者的采购网络安全宣传活动。[31] 整个培训，特别是参与行业，应明确阐明政府正在通过采用基于风险的方法不断改变自身与网络安全相关的购买行为，因此，政府在某些类型的采购中将要求有更多的网络安全相关产业。

增加负责人员的知识将促进适当的网络风险管理，有助于避免过度详细的网络安全要求（这会导致更高的成本）或不够详细的网络安全要求（这会导致更大的风险）。

Ⅲ. 为联邦采购制定共同的网络安全定义

在联邦采购中增加关键网络安全术语的清晰度将增加政府和私营部门的效率和效益。有效地开发和满足要求的能力在很大程度上取决于对一个关键术语，特别是在像网络安全和采购这样的专门学科专业的含义上达成共识。当这些术语都包含在法律文本中作为采购过程的一部分时，这种需要尤为迫切。

不明确和不一致定义的术语充其量将导致效率和网络安全都不达最佳标准。当采购过程中存在误解时，它们可能会产生错误或困惑，如技术要求，市场调研，成本估算，预算，采购申请，游说，建议，源选择，与合同奖励和性能。在由法律手段支配的业务活动中，不同的定义可能更难以解决和制造非常真实的成本冲击，包括合同变更，终止和诉讼。这些定义的一个好的基线存在于具有共识的国际标准中。

这一建议是为了与正在进行的国防联邦采购规则附录（DFARS）规则制定相协调，规则题为 “检测和避免假冒电子零件”。[32]

Ⅳ. 提出一项联邦采购网络风险管理策略

政府需要一个跨部门采集网络风险管理的策略，这要求机构确保其性能符合采购战略网络风险的目标，并且是政府的企业风险管理战略的一部分。该战略应以整个政府的采购为视角，主要与为解决网络安全框架中的网络风险而开发的方法论和程序相匹配，它应识别采购

[31] E.g., GSA provides training about its Multiple Award Schedules (MAS) program through the "Pathway to Success" training. This is a mandatory training module that provides an overview of GSA MAS contracts. Potential offerors must take the "Pathway To Success" test prior to submitting a proposal for a Schedule contract. See, https://vsc.gsa.gov/RA/research.cfin. Additionally, contractors might, in certain circumstances, be required to complete ongoing training throughout contract performance. Specific training about an acquisition might also be included in requirements to become a qualified bidder, and become a source selection criterion.

[32] 78 Fed. Reg. 28780 (May 16,2013), Proposed Rule; DFARS Case 2012-D055.

的网络风险层级，并包括一个基于风险的采购优先级别。风险分析应与联邦企业体系结构[33]和美国国家标准技术研究所风险管理框架（RMF）[34]相一致。

该战略应包括 “重叠”的发展：完全规定的安全要求，提供能力的补充指导，提供的适当调整安全需求的能力，为特定的技术或产品群，环境、条件和/或操作环境。[35]

在开发策略上，政府应利用现有的风险管理流程和数据收集方法，始终把网络风险作为企业风险管理的一个元素。该战略应包括标准的网络安全实践，以解决信息易受网络入侵和外泄的问题。该战略应充分利用供应链风险管理程序，以减少不合格品（如假冒和被感染的产品）的风险。它应当包括适当的指标来定义风险和衡量机构应用经验风险建模技术的能力，这一技术在公共和私营机构机构中都有应用。在制定战略时，政府应该运用行业间积极的工作伙伴关系，在民用机构和情报机构之间，在不存在这样的伙伴关系的地方创造这样的伙伴关系，本着扩充有效的和以结果为基础的风险管理流程、最佳实践和经验教训的目标。

如果合适定义的相似类型的采购已经存在，政府应为那些采购类型制定重叠。[36] 该重叠的制定应与业界合作，并一致地应用于所有类型相似的联邦采购。要求的发展应该是网络安全框架的出发点。

该重叠应包括适当缓解采购风险的现实的和基于风险的控制，并应定义相似类型的任何采购可接受的最低控制。作为一般规则，该重叠不应包括直接进入合同的标准，并应避免具体做法、工具或特定国家的标准的指令性任务，因为这些方法的不灵活性往往在不经意间增加了成本，而没有实际降低风险。[37]相反，重叠应从应用到被分析的采购类型中的标准内部

---

[33] Available at http://www.whitehouse.gov/orab/e-gov/fea/.

[34] See, NIST Special Publication 800-37, Revision 1 (Feb. 2010).

[35] See, e.g., The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. Available at: http://www.gsa.gov/portal/category/102375. See also, the Information Systems Security Line of Business (ISSLoB) is a comprehensive and consistently implemented set of risk-based, cost- effective controls and measures that adequately protects information contained in federal government information systems. Available at: http://www.dhs.gov/information-systems-security-line-business.

[36] See e.g., FedRAMP, ISSLoB, and Federal Strategic Sourcing Initiative (FSSI) (available at: http://www.gsa.gov/fssi.), among others. These programs have defined categories of similar types of products and services.

[37] Directly incorporating standards could freeze the status quo and hamper or prevent the evolution of countermeasures required to address the dynamic threat and technology landscapes. It might also create a risk that other nations will adopt similar mandates which could further increase supply chain costs. Incorporating government-specific standards that would duplicate existing security-related standards or creating

具体地识别安全控制。该重叠还应该包括采购和合同控件，如源选择标准和合同措施。最后，在可能的最大范围内，重叠应表示为技术要求。这种方法将允许政府描述最高级网络安全要求，将它们分解到单个采购一个较低的级别，然后以类似其它部署解决方案要求的方式标明他们与要求相一致。

这一建议是基于一个事实，即并不是所有通过采集系统交付的资源都呈现相同的网络风险级别或保证网络安全的同等水平，并要求政府合同与联邦政府的规划和绩效的网络安全得到增强。这样的成本增加，必须与网络风险严重性的性质和相应的其他功能的成本相平衡。联邦政府可以减轻任何成本的增加量，如果它通过采用各种细分市场和类似类型采购的网络安全要求来创造确定性。

Ⅴ. 要求从原始设备或元件制造商、其授权经销商或其他可靠来源购买

确保提供给政府的商品均为正品，并且没有被修改或篡改是减轻网络风险的重要一步。假冒成品和部件往往不具备最新的安全相关的更新或不建立原始设备（或部件）制造商（OEM）的安全标准。在某些情况下，接收不真实的，伪造的，或者以其他方面不合格品的风险仅由来自原始设备制造商、他们的授权经销商，或其他值得信赖的来源取得所需的项目得到最好的缓解。[38]

原始设备制造商通过确保其产品的真实性会获得更高的利益，而这种利益通过贯彻他们的政策来实现，政策指用于指定若干供应商或经销商的“授权”。 仅对于这些类型来源所有采集的限制资格，未必与采集的规则、社会经济优先采购、或公开竞争的原则一致。其他可靠来源可以通过使用合格的产品、投标人或制造商列表（QBL）标识，[39] 以确保识别的来源符合相应提供正品的标准。该 QBL 应基于所使用可靠来源所提供的网络风险缓解的价值。

即使使用可靠来源，也可能有“可靠的”设备还存在网络安全漏洞。这种方法也代表可

---

country-specific requirements that could restrict the use of long-standing and highly credible global suppliers of technology could have significant negative effects on the government's ability to acquire the products and services it needs.

[38] See e.g., Solutions for enterprise Wide Procurement (SEWP) V, is a multi-award Government-Wide Acquisition Contract (GWAC) that provides IT Products and Product Solutions. SEWP is administered by NASA, and the recently released draft RFP includes this limitation of sources by requiring offerors for certain types of items to be an authorized reseller of the OEM; available at: https://www.sewp.nasa.gov/sewpv/.

[39] 8 C.F.R. § 9.203 (2013).

用资源的限制，因此应该只用于大到足以证明在可信和不可信来源之间的竞争或价格差异的负面影响存在风险的采集类型。对于呈现这些类型风险的采集，政府应限制给原始设备制造商、授权经销商，和可靠供应商的资源，并且这种限制应纳入全面采集和维持生命周期，从需求定义，收购计划，以及市场调研入手。

如果政府选择使用没有与原始设备制造商建立信任关系的经销商、分销商、批发商或经纪人，那么政府应该得到公司所购买产品安全性和完整性的能力保证。收购陈旧、翻新、或其成品原材料及零部件时，这样一个可靠的供应商符合要求尤为重要。

供应商或经销商必须满足以获取“可靠”来源的合同条款在细分市场之间有所不同，但一般的供应商将针对一组广泛的标准，包括长期的商业可行性，质量控制系统，评估安置和履行流程，客户支持，客户退货政策，和过去的记录，例如通过政府行业数据交换计划（GIDEP）[40]进行搜索。为了建立 QBL，这些标准的内容及应用必须由政府进行评估，或由政府授权，定期确保 QBL 提供的在真正缓解网络风险中的持续价值。

由政府进行的评估方法应根据收购类型的网络风险来决定。例如，对于表现出最大的风险收购类型，适当的评估方法可能是由政府工作人员进行审核。对于风险较小的种类，合适的评估方法可以是第一，第二，或公司顺应标准的第三方认证。至少，鉴定程序应当立足于网络安全框架，具有进行验证和测试的一致和良好定义的流程，使用第三方进行审查和批准，并且包括执法机制。

VI. 完善网络风险管理的政府问责制

如上所述，联邦系统在整个开发，采集，维持和处置的生命周期中都受制于网络风险。网络风险管理实践中的应用必须同样贯穿所有阶段和功能，包括但不限于技术与发展;工程设计与制造;生产;操作和支持;安全性;以及反间谍。这种做法的成功将依赖于网络安全风险集成到现有的采集流程，将每一个阶段和功能通知关键利益相关者和决策者。

这一建议是为了将安全标准整合到收购计划和合同管理中，并将网络风险纳入企业风险管理，以确保关键决策者对有关威胁、漏洞、可能性负责，并对部署网络安全风险解决方案

[40] GIDEP is a cooperative activity between government and industry participants seeking to reduce or eliminate expenditures of resources by sharing technical information. Since 1959, over $2.1 billion in prevention of unplanned expenditures has been reported. See, http://www.gidep.org.

的后果负责。

首先，定义了要求、分析了解决方案，网络风险应该得到解决。根据收购类型的网络安全重叠的要求，要求开发人员和收购人员确定哪些控制应包括在要求中，确定哪些风险决策是收购的关键，并确保关键决策是由主要利益相关者和网络风险管理计划告知的。

第二，招标发布之前，采集人员应当证明，合适的网络安全需求在招标中得到充分反映。这包括但不限于纳入的技术要求，定价方法，来源选择标准和评估计划，以及任何裁决后合同管理应用程序。

第三，来源选择过程中，收购人员应参与提案的评估进程，并确保明显具有最佳价值的建议符合招标的网络安全需求。

最后，在某种程度上任何一致性测试，技术更新检验，供应链风险管理措施，或任何其他有关网络安全的裁决后合同履约事项，负责人（例如，程序执行人员），在收购人员的协助下，应该证明该行动是按照规定的标准进行的。

结论

本报告的建议解决了可行性、效益、和将标准纳入收购计划和合同的优点，并通过关注网络安全基线要求，广大员工培训，和一致的网络安全术语统一采购要求。这些被建议与网络风险管理合并成企业风险管理，开发更加详细和标准的特殊类型采购安全控制的应用，限制购买某些高风险来源的采购，并提高整个政府对网络安全的责任，这种负责贯穿整个开发、收购、维持、使用和处置生命周期。

与改变细分行业或承包人员的行为相比，这些建议更多是关于转变政府项目管理人员和采购决策者的行为。政府不能让所有的承包人员成为网络安全专家，但它可以通过确立合适的网络风险管理责任制改善合适的问责制，将网络风险管理纳入收购过程。底线是政府将只能实现增强网络安全和恢复能力的目标。使用在这些建议中列出的方法将允许政府做出更好的关于哪些网络安全的措施应该在一个特定的收购来实现的选择。而选择是根据严格的实证网络风险分析做出的。

实现网络恢复能力要求对必要的管理风险的人员和资源的投资。建设网络的恢复能力也需要公共和私营部门（包括供应链的供货商和供应商之间）之间的机构间的协调与合作。这

还需要从一线人员到最高级领导都对这一问题有更强烈的认识。

总之，政府应该经过深思熟虑后协作处理这个复杂的问题，采取积极措施，确保其政策和做法是解决方案的一部分，以减少信息和通信技术市场上的不利影响。

附录 1：联合工作组名册

下表中列出的人员是起草报告和提出建议的核心团队。但也许多有来自公共和私营部门组织的人。所有人员都带来了具有高度的专业性和知识到工作中，并代表他们所在组织的股权，功能学科，以及联邦政府的利益。

机构	组织	姓名
国防部	主管采购、技术、物流的国防部长办公室；国防采购和收购政策	Michael Canales Mary Thomas
	主管网络政策的国防部副部长办公室	Joshua Alexander
	首席信息官办公室	Don Davidson Jenine Patterson
总务管理局	应急响应和恢复办公室	Christopher Coleman
	联邦采购服务局	Emile Monette Larry Hate Shondrea L ublanovits
	政府政策办公室	Marissa Petrusek
行政管理和预算局	联邦采购政策办公室	Jeremy McCrary
国土安全部	国家保护和计划署，网络安全和通信办公室	Joe Jarzombek Michael Echols
	董事会管理办公室首席采购官	Camara Francis Shaundra Dn ans
商务部	美国标准技术研究所	Jon Boyens

附录 2：利益相关方的参与

下面的列表列出了参与工作组审议和报告撰写过程的人员。这个名单不包括与 DHSITF 或工作组会议的定期会议。凡该基金或机构与工作组成员被确定，该种参与作为常规工作组和 ITF 过程的一种附属，或者是有特殊意义（如，向跨部门负责人概述报告草案）的一种常规参与。

日期	**活动参与者**
2013 年 1 月 9 日	TechAmerica
2013 年 1 月 10 日	专业服务委员会
2013 年 1 月 14 日	政府采购联盟
2013 年 1 月 28 日	技术美国
2013 年 1 月 29 日	联邦调查局
2013 年 2 月 8 日	技术美国
2013 年 2 月 12 日	政府采购联盟
2013 年 2 月 15 日	国土安全部集成工作小组
2013 年 2 月 19 日	国土安全部集成工作小组
2013 年 2 月 26 日	私营公司
2013 年 3 月 5 日	国家标准技术研究所软件保证论坛
2013 年 3 月 5 日	国防行业协会
2013 年 3 月 8 日	国土安全部集成工作小组
2013 年 3 月 11 日	美国银行家协会公共合同法部分，网络安全委员会
2013 年 3 月 13 日	国家标准技术研究所研究与开发
2013 年 3 月 14 日	国土安全部激励工作小组
2013 年 3 月 15 日	国际杀虫剂分析协作委员会信息技术部门协调委员会，供应链工作小组
2013 年 3 月 21 日	私营公司
2013 年 3 月 25 日	国际杀虫剂分析协作委员会信息技术与通信行业协调委员会
2013 年 4 月 1 日	国家网络安全综合计划 11 工作小组
2013 年 4 月 2 日	国防情报局
2013 年 4 月 2 日	国防行业协会
2013 年 4 月 4 日	为赛博-实物系统网络安全设计的国家标准技术研究

	所
2013 年 4 月 4 日	国防工业协会网络部门会议
2013 年 4 月 16 日	国际杀虫剂分析协作委员会信息技术部门协调委员会
2013 年 4 月 18 日	技术美国网络安全委员会
2013 年 4 月 19 日	专业服务委员会
2013 年 4 月 22 日	国际杀虫剂分析协作委员会信息技术与通信行业协调委员会
2013 年 4 月 30 日	美国银行家协会公共合同法部分，网络安全委员会会议
2013 年 5 月 1 日	国际杀虫剂分析协作委员会信息技术与通信行业协调委员会会议
2013 年 5 月 1 日	私营公司
2013 年 5 月 2 日	半导体行业协会会议
2013 年 5 月 2 日	国土安全部综合工作组成员简报
2013 年 5 月 2 日	财政部
2013 年 5 月 3 日	私营公司
2013 年 5 月 6 日	私营公司
2013 年 5 月 7 日	ACT 交互应用通信网络安全共享利益集团会议
2013 年 5 月 7 日	在网络信息处理中心跨部门会议上陈述
2013 年 5 月 9 日	政府采购联盟会议
2013 年 5 月 13 日	私营公司
2013 年 5 月 13 日	私营公司
2013 年 5 月 22 日	网络安全联盟董事会会议
2013 年 5 月 22 日	国家安全局，收缩政策
2013 年 5 月 22 日	采访，《华盛顿邮报》
2013 年 5 月 22 日	提供背景，《华尔街日报》
2013 年 5 月 23 日	电台采访直播，联邦新闻广播，"深度"
2013 年 6 月 3 日	私营公司
2013 年 6 月 3 日	财政部
2013 年 6 月 3 日	安全行业协会，政府首脑峰会
2013 年 6 月 4 日	信息技术工业协会
2013 年 6 月 4 日	美国马里兰大学