美国国土安全部

保卫物联网（IoT）的战略原则

版本1.0

2016年11月15日

简介与概述

组成物联网（IoT）的网络连接设备，系统和服务的增长为我们的社会创造了巨大的机遇和利益。但是，物联网安全跟不上创新和部署的快速步伐，带来巨大的安全和经济风险。本文档解释了这些风险，并提供了一组非约束性原则和建议的最佳实践，旨在为企业设计，制造，拥有和运营的设备和系统建立负责任的安全级别。[1]

物联网的增长和普及

互联网连接设备可实现人，网络和物理服务之间的无缝连接。这些连接提供了对制造商和消费者都有吸引力的效率，新颖用途和定制体验。从健身追踪器，心脏起搏器和汽车到向家中供水和供电的控制系统，网络连接设备已在日常生活的各个方面变得无处不在，甚至对生活至关重要。物联网提供的承诺几乎是无限的。

优先考虑物联网安全

虽然物联网的优势不可否认，但现实是安全性无法跟上创新步伐。随着我们越来越多地将网络连接集成到国家关键基础设施中，曾经手动执行的重要流程（因此具有一定程度的对恶意网络活动的免疫力）现在容易受到网络威胁的攻击。我们国家对网络连接技术的依赖性日益增长，其增长速度超过了保护网络连接技术的增长速度。

物联网生态系统带来的风险包括恶意行为者操纵往返于网络连接设备的信息流或篡改设备本身，可能导致敏感数据被盗和消费者隐私丢失，业务运营中断，互联网速度减慢。大规模分布式拒绝服务攻击的功能，以及对关键基础设施的潜在破坏。

去年，在乌克兰部分地区造成暂时性电网瘫痪的网络攻击中，全世界看到了互联系统故障可能造成的严重后果。
由于我们国家现在依靠运行正常的网络来开展众多维持生命的活动，因此物联网安全现在属于国土安全问题。

1在这种情况下，术语“物联网”指的是通常内置于互操作协议中的，具有主要物理目的的系统和设备（如传感，加热/冷却，照明，电机驱动，运输）与信息网络（包括互联网）的连接。嵌入式系统。

至关重要的是，政府和行业必须迅速合作，以确保物联网生态系统建立在可信赖和安全的基础上。 2014年，总统国家安全电信咨询委员会（NSTAC）强调了采取紧急行动的必要性。

> 物联网的采用将在速度和范围上都将增加，[将]几乎影响我们社会的所有部门。 Nation面临的挑战是确保采用物联网不会造成不当风险。另外…。有一个小窗口（迅速关闭）以确保以最大程度地提高安全性和风险最小化的方式采用物联网。如果该国不这样做，它将应付子孙后代的后果。[2]

现在是解决物联网安全的时候了。本文件为就这些关键问题与公共和私营部门接触奠定了基础。激励和组织有关物联网开发人员，制造商，服务提供商和购买和部署设备，服务及系统的用户之间有关物联网安全积极措施的对话，这是第一步。以下原则和建议做法将战略重点放在安全性上，并增强支撑物联网生态系统的信任框架。

战略原则概述

可以通过公认的安全最佳实践来缓解IoT中的许多漏洞，但当今太多产品甚至都没有采用基本安全措施。造成此安全漏洞的因素很多。在一个公司可以设计设备，另一家提供组件软件，另一家运营嵌入设备的网络，另一家部署设备的世界中，一个人负责安全决策尚不清楚。缺乏全面，广泛采用的物联网安全国际规范和标准，这一挑战更加严峻。其他促成因素包括缺乏激励开发人员充分保护产品的动力，因为不一定承担失败的成本，以及对如何评估竞争性期权的安全性认识不一。

下一节阐述的以下原则为利益相关者提供了一种组织思考如何应对这些物联网安全挑战的方式：

在设计阶段整合安全性

预先进行安全更新和漏洞管理

以成熟的安全实践为基础

2国家安全通信咨询委员会向物联网主席致辞，2014年11月19日。

根据潜在影响优先考虑安全措施
促进物联网透明
小心谨慎地连接

与所有网络安全措施一样，缓解物联网风险是政府与私营部门之间不断发展的共同责任。公司和消费者通常对自己制造或购买的产品的安全功能做出自己的决定。在某些特定监管环境和执法活动之外，政府的作用是提供工具和资源，以便公司，消费者和其他利益相关者可以做出有关物联网安全的明智决策。

范围，目的和受众

这些非约束性原则的目的是为利益相关者提供建议的实践，帮助他们在开发，制造，实施或使用网络连接的设备时考虑安全性。具体来说，这些原则旨在：

1	物联网开发人员在设计和开发设备，传感器，服务或物联网的任何组件时会考虑安全性；
2	物联网制造商提高消费者设备和供应商托管设备的安全性；
3	通过物联网设备实施服务的服务提供商应考虑这些物联网设备提供的功能的安全性，以及支持这些服务的基础设施的基础安全性；和
4	工业和企业级别的消费者（包括联邦政府和关键基础设施所有者和运营商）作为领导者，就物联网设备安全吸引制造商和服务提供商。

保护物联网的战略原则

下述原则旨在提高物联网在整个设计，制造和部署活动中的安全性。这些战略原则和相关建议实践的广泛采用将大大改善物联网的安全状况。但是，还没有一种万能的解决方案可以缓解物联网安全风险。并非以下列出的所有实践在物联网设备的多样性之间具有同等相关性。这些原则旨在通过基于风险的方法进行调整和应用，其中应考虑相关的业务环境，以及涉及网络连接的设备，系统或服务的事件可能造成的特定威胁和后果。

在设计阶段整合安全性

安全性应作为整体评估

任何网络连接设备的组件。尽管有例外，但在许多情况下，经济驱动因素或对风险的意识不足，导致企业在不考虑安全性的情况下将设备推向市场。在设计阶段建立安全性可减少潜在中断，并避免在产品开发和部署后尝试为产品增加安全性的难度更大，成本更高的工作。通过将安全性作为网络连接设备的一项功能，制造商和服务提供商也有机会实现市场差异化。下面的做法是在设计，开发和生产的最早阶段解决安全问题的一些最有效方法。

在设计过程中未建立安全性有哪些潜在影响？

未能设计和实施适当的安全措施可能会对制造商的财务成本，声誉成本或产品召回成本造成损害。虽然目前尚无针对物联网环境的判例法，但传统的产品责任侵权法原则有望应用。

建议做法：

默认情况下，通过难破解的唯一默认用户名和密码启用安全性。制造商提供的物联网设备的用户名和密码为

通常不会被用户更改，而且很容易破解。僵尸网络通过持续扫描受已知出厂默认用户名和密码保护的物联网设备运行。强大的安全控制措施应成为工业用户故意禁用而非故意启用的功能。

使用技术上可行且经济上可行的最新操作系统构建设备。许多物联网设备使用Linux操作系统，但可能未使用最新操作系统。使用当前操作系统，可以确保已知漏洞已得到缓解。

使用包含安全功能的硬件来增强设备的保护和完整性。例如，使用计算机芯片，将芯片级安全性集成到处理器中，并提供加密和匿名功能。

设计时要考虑系统和操作中断。了解设备故障可能带来的后果，将使开发人员，制造商和服务提供商能够做出更明智的基于风险的安全决策。在可行的情况下，开发人员应构建能够安全可靠地发生故障的物联网设备，以免导致更大的系统破坏。

促进安全更新和漏洞管理

即使在设计阶段包括安全措施，也可能会在产品部署后发现漏洞。可以通过修补，安全更新和漏洞管理策略来缓解这些缺陷。在设计这些策略时，开发人员应考虑设备故障，相关产品的耐用性以及预期的维修成本。如果没有部署安全更新的能力，制造商可能会面临代价高昂的召回与让已知漏洞的设备在流通之间做出决定。

专注于：NTIA Multi-利益相关者修补和更新流程

美国国家电信和信息管理局（NTIA）召集了一个有关“物联网可升级和补丁”的多方利益相关者流程，召集各利益相关者就安全可升级性和补丁问题交换意见，并为行业制定更具体的目标广泛采用。

建议做法：
考虑通过网络连接或自动方式保护设备安全的方法。理想情况下，应自动应用补丁，并利用加密完整性和真实性保护更快地解决漏洞。
考虑考虑在第三方供应商之间协调软件更新，以解决漏洞和安全改进问题，以确保消费类设备具有完整的当前保护措施。
开发解决漏洞的自动化机制。例如，在软件工程领域，有一些机制可以实时提取来自研究和黑客社区的关键漏洞报告中的信息。这样，开发人员可以解决软件设计中的这些漏洞，并在适当时做出响应。
制定有关协调披露漏洞的政策，包括解决已识别漏洞的相关安全措施。协调一致的披露政策应包括开发人员，制造商和服务提供商，并包括与上报给计算机安全事件响应小组（CSIRT）的任何漏洞有关的信息。美国计算机应急准备小组（US-CERT），工业控制系统（ICS）-CERT和其他CSIRT提供定期技术警报（包括重大事件发生后），提供有关漏洞和缓解的信息。
为物联网产品制定使用寿命终止策略。并非所有的物联网设备都可以无限期修补和更新。开发人员应提前考虑产品日落问题，并与制造商和消费者沟通有关该设备的期望以及超过其可用日期使用设备的风险。

以公认的安全惯例为基础

传统IT和网络安全中使用的许多经过测试的实践都可以应用于物联网。这些方法可帮助识别漏洞，检测违规行为，响应潜在事件以及从对物联网设备的损坏或破坏中恢复。

专注于：NIST网络安全风险管理框架
美国国家标准技术研究院（NIST）发布了网络安全风险管理框架，该框架已由私营行业广泛采用，跨部门和组织内部整合。该框架被广泛认为是组织网络风险管理的全面试金石https://www.nist.gov/cyberframework。考虑风险和最佳实践提供了起点。

建议做法：

从基本软件安全和网络安全实践开始，以灵活，自适应和创新的方式将其应用于物联网生态系统。

请参考相关的行业特定指南，作为考虑安全实践的起点。一些联邦机构针对其监管的独特行业制定安全规范。例如，国家公路交通安全管理局（NHTSA）最近发布了有关解决自动驾驶或半自动驾驶汽车所面临的一些独特风险的指南。同样，食品和药物管理局发布了有关的指南草案。

深入练习防御。开发人员和制造商应采用整体安全措施，包括针对网络安全威胁的分层防御，包括用户级工具作为恶意行为者的潜在切入点。如果没有可用的修补程序或更新机制或不足以解决特定漏洞，这一点尤其有用。

参与信息共享平台报告漏洞，并从公共和私人合作伙伴接收有关当前网络威胁和漏洞的及时和关键信息。信息共享是确保利益相关者意识到威胁发生时的关键工具。例如，国土安全部国家网络安全和通信集成中心（NCCIC），以及多州和特定行业的信息共享和分析中心（ISAC）以及信息共享和分析组织（ISAO）。

3"国家网络安全和通信信息中心。"Information Sharing,

根据潜在影响优先考虑安全措施

整个物联网生态系统的风险模型差异很大。例如，工业消费者（如核反应堆所有者和运营商）与零售消费者的考虑因素不同。在不同客户之间发生安全故障的后果也将有很大不同。

因此，在确定应将特定安全措施定向到何处以及最有能力减轻重大后果的方面，着眼于整个消费者频谱的破坏，破坏或恶意活动的潜在后果至关重要。

物联网安全措施应重点关注物联网设备吗？

由于所有物联网流程的目的都是在物理点接收信息并根据该信息做出决策（有时会带来物理后果），因此安全措施可以集中于物联网流程的一个或多个部分。如前所述，物联网的风险始于特定设备，但不仅限于此。开发人员，制造商和服务提供商应考虑对物联网设备以及流程和服务的特定风险，并根据对这三者的相对影响制定最强有力的措施。

建议做法：

尽可能了解设备的预期用途和环境。这种认识有助于开发人员和制造商考虑物联网设备的技术特征，设备如何运行以及必要的安全措施。

执行“红队”练习，开发人员在其中积极尝试绕过应用程序，网络，数据或物理层所需的安全措施。最终的分析和缓解计划应有助于确定在何处以及如何合并其他安全措施的决策的优先级。

识别和验证连接到网络的设备，特别是对于工业用户和企业网络。对已知设备和服务应用身份验证措施，可使工业用户控制其组织框架内的设备和服务。

促进物联网透明

在可能的情况下，开发人员和制造商需要了解他们的供应链，即与组织外部供应商提供的软件和硬件组件是否存在任何关联漏洞。依靠物联网中使用的许多低成本，易于访问的软件和硬件解决方案可能会带来挑战。由于开发人员和制造商依靠外部来源提供低成本，易于访问的软件和硬件解决方案，因此在开发和部署网络连接设备时，他们可能无法准确评估组件内置的安全级别。此外，由于许多物联网设备利用开源软件包，因此开发人员和制造商很多人无法识别这些组成部分的来源。

增强意识可以帮助制造商和工业用户确定在何处以及如何实施安全措施或建立冗余。根据所涉及产品的风险状况，开发人员，制造商和服务提供商将具备更好的能力，通过补丁，产品召回或消费者咨询，尽快适当地缓解威胁和漏洞。

建议做法：

进行端到端风险评估，尽可能评估内部和第三方供应商风险。开发人员和制造商应将供应商和供应商纳入风险评估流程，这将提高透明度，使他们能够意识到潜在的第三方漏洞，并促进信任和透明度。当供应链中的组件被更换，移除或升级时，应持续重新解决安全问题。

考虑创建一个使用漏洞报告的公开机制。例如，错误赏金 程序依靠众包方法识别公司内部安全团队可能无法捕获的漏洞。

考虑开发和使用软件物料清单，可用作在供应商和制造商之间建立共享信任的手段。开发人员和制造商应考虑提供保护知识产权问题的方式，在设备包装中提供已知硬件和软件组件的列表。列表可以作为物联网生态系统中其他人员了解和管理其风险并在发生任何事件后立即修补所有漏洞的宝贵工具。

小心谨慎地连接

物联网消费者（尤其是在工业环境中）应慎重考虑到使用物联网设备及其中断相关的风险，是否需要连续连接。物联网消费者还可以通过谨慎有意地连接，权衡潜在物联网设备损坏或故障的风险，以及限制互联网连接的成本，帮助遏制网络连接带来的潜在威胁。

在当前的网络环境中，任何给定的物联网设备很可能在其生命周期中受到干扰。物联网开发人员，制造商和消费者应考虑中断后如何影响物联网设备的主要功能和业务运营。

是否每台联网设备都需要连续，自动连接到互联网？
2015年，联邦贸易委员会发布了题为“从安全开始：企业指南”，以帮助他们确定这个问题。虽然连续网络访问可能很方便，但出于设备和系统的目的，可能不必要。例如，核反应堆，如果持续连接到互联网，就有可能入侵潜在的巨大后果。

建议做法：

向物联网消费者建议任何网络连接的预期用途。运营物联网设备的关键功能可能不需要直接互联网连接，尤其是在工业环境中。有关连接性质和目的的信息可以为消费者做出决策。

进行故意连接。在某些情况下，对于用户而言，不是直接连接到互联网，而是连接到可以聚合和评估任何关键信息的本地网络。例如，工业控制系统（ICS）应通过深度防御原则（由）发布保护。

内置控件，允许制造商，服务提供商和消费者在需要或需要启用选择性连接时禁用网络连接或特定端口。根据物联网设备的用途，向消费者提供有关最终实施的指导和控制可能是一种合理的做法。

结论

我们国家负担不起部署很少考虑安全性的物联网设备。考虑到可能损害我们关键基础设施，个人隐私和经济的后果，后果实在太大。

在国土安全部发布这些原则时，我们认识到其他联邦机构同事的努力，以及私营部门实体为解决IoT安全问题而推进架构和制定实践的工作。该文件是阐明总体安全原则，加强这些努力的第一步。但是，肯定需要采取进一步措施。

国土安全部确定了政府和行业为加强物联网安全应采取的四项工作。

四点努力：
跨联邦部门和机构进行协调，与物联网利益相关方互动，共同探索减轻物联网风险的方法。 国土安全部与联邦合作伙伴将继续与行业合作伙伴合作，确定可进一步增强物联网安全的方法，并增进对可能解决物联网风险的技术发展趋势的了解。随着最佳实践和方法的进一步完善和理解，未来的工作还将集中于更新和应用这些原则。
跨利益相关者树立与物联网相关的风险意识。 重要的是，利益相关者必须意识到物联网风险，以便能够自行应对。国土安全部将与其他机构，私营部门和国际伙伴合作，加快公众意识，教育和培训举措。国土安全部将与其他机构一道，针对特定部门和个人消费者采取更直接的举措。
确定并推进整合物联网安全的激励措施。政策制定者，立法者和利益相关者需要考虑如何更好地激励人们增强物联网安全性。在当前环境下，通常不清楚由谁负责特定产品或系统的安全性。此外，安全状况差的成本通常不由最有可能提高安全性的人员承担。国土安全部和所有其他利益相关者需要考虑侵权责任，网络保险，立法，法规，自愿认证管理，标准制定计划，行业自愿计划以及其他机制如何在提高安全性的同时仍鼓励经济活动和突破性创新。展望未来，国土安全部将与合作伙伴召集讨论这些关键问题，并征求意见和反馈。
为物联网的国际标准制定流程做出贡献。 物联网是全球生态系统的一部分，其他国家和国际组织也开始评估许多相同的安全考虑因素。重要的是，与物联网相关的活动不得分裂为一组不一致的标准或规则。随着国土安全部越来越重视物联网工作，我们必须与我们的国际合作伙伴和私营部门合作，支持国际标准的制定，并确保它们符合我们对促进创新和促进安全的承诺。

国土安全部期待这些后续合作步骤。我们可以而且必须共同应对这些复杂的挑战。这样，我们将确保网络连接的未来不仅是创新的，而且是安全的和持久的。

附录：指导和其他资源

本文档中的原则是根据行业报告中收集的信息以及与私营行业，行业协会，非政府实体和联邦合作伙伴（特别是与NIST和NTIA）进行的讨论制定的。

国土安全部

- https://www.dhs.gov/sites/default/files/publications/draft-lces-security-comments-508.pdf
- https://www.dhs.gov/publication/security-tenets-lces
- https://www.dhs.gov/sites/default/files/publications/security-tenets-lces-paper-11-20-15-508.pdf

其他联邦实体

- National Security Telecommunications Advisory Committee
    1。Final NSTAC Internet of Things Report

- NTIA
    1. Notice and Request for Comments on the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things
        a) Comments
    2. Green Paper – Cybersecurity, Innovation and the Internet Economy, 2011
    3. New Insights into the Emerging Internet of Things
    4. Remarks of Deputy Assistant Secretary Simpson at Fostering the Advancement of the Internet of Things Workshop, 9/9/2016
        a) 的公告Fostering the Advancement of the Internet of Things Workshop
    5. 互联网政策工作组，负责政府在促进物联网发展中的优势，挑战和潜在作用。resource/review/cataloging

- 国家标准技术研究所
    1. 网络安全Framework
    2. Cyber-Physical Systems （CPS） Program
        a) CPS公共工作组（PWG）draft Cyber-Physical Systems (CPS) Framework Release 1.0
            Ø Comments accepted through 9/2/2015

3. Smart-Grid 程序
4. 国际技术工作组IoT-Enabled Smart City Framework
5. NIST特殊出版物（SP），物联网，2016年7月28日。800-183
    a) 国家标准技术研究所news release

- 联邦贸易委员会
    1. FTC员工报告，“物联网：互联世界中的隐私和安全”，2015年1月。

- 美国国会
    1. 参议院商业，科学和运输委员会听证会，“。”The Connected World: Examining the Internet of Things
    2. 参议院两党一致通过决议，要求制定一项指导物联网发展的国家战略。S. Res. 110
    3. 众议院能源和商业委员会的““The Internet of Things: Exploring the Next Technology Frontier
- 政府会计办公室
    1. GAO与DHS接触：GAO目前与物联网上的DHS接触，代码100435 [2016年1月15日，可通过此通知函]link
        a) 最新状态（2016年6月3日）List of Active GAO Engagements Related to DHS

外部来源

额外资源清单仅供参考，并不代表国土安全部（DHS）的认可。国土安全部不认可任何商业产品，服务或企业。

- 大西洋理事会
    1.智能家居和物联网–http://www.atlanticcouncil.org/publications/issue-briefs/smart-homes-and-the- internet-of-things
- 我是骑兵
    1. 五星级汽车网络安全框架–https://iamthecavalry.org/5star
    2. 希波克拉底誓言-连接医疗设备https://iamthecavalry.org/oath
- 在线信托联盟
    1。 Consumer Best Practices
- 工业互联网联盟：http://www.iiconsortium.org/IISF.htm
- 开放式网络应用程序安全项目（OWASP）

1. 物联网项目
   https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
2. 物联网安全指南
   https://www.owasp.org/index.php/IoT_Security_Guidance

- Safecode.org相关行业最佳实践www.safecode.org
- 美国电话电报公司
  1。 Exploring IoT Security
- 赛门铁克
  1.物联网参考架构
  https://www.symantec.com/content/dam/symantec/docs/white-papers/iot-security-reference-architecture-en.pdf