

STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS (IoT)

Version 1.0

November 15, 2016



Homeland
Security

INTRODUCTION AND OVERVIEW

The growth of network-connected devices, systems, and services comprising the Internet of Things (IoT)¹ creates immense opportunities and benefits for our society. IoT security, however, has not kept up with the rapid pace of innovation and deployment, creating substantial safety and economic risks. This document explains these risks and provides a set of non-binding principles and suggested best practices to build toward a responsible level of security for the devices and systems businesses design, manufacture, own, and operate.

Growth and Prevalence of the Internet of Things

Internet-connected devices enable seamless connections among people, networks, and physical services. These connections afford efficiencies, novel uses, and customized experiences that are attractive to both manufacturers and consumers. Network-connected devices are already becoming ubiquitous in, and even essential to, many aspects of day-to-day life, from fitness trackers, pacemakers, and cars, to the control systems that deliver water and power to our homes. The promise offered by IoT is almost without limit.

Prioritizing IoT Security

While the benefits of IoT are undeniable, the reality is that security is not keeping up with the pace of innovation. As we increasingly integrate network connections into our nation's critical infrastructure, important processes that once were performed manually (and thus enjoyed a measure of immunity against malicious cyber activity) are now vulnerable to cyber threats. Our increasing national dependence on network-connected technologies has grown faster than the means to secure it.

The IoT ecosystem introduces risks that include malicious actors manipulating the flow of information to and from network-connected devices or tampering with devices themselves, which can lead to the theft of sensitive data and loss of consumer privacy, interruption of business operations, slowdown of internet functionality through large-scale distributed denial-of-service attacks, and potential disruptions to critical infrastructure.

Last year, in a cyber attack that temporarily disabled the power grid in parts of Ukraine, the world saw the critical consequences that can result from failures in connected systems. Because our nation is now dependent on properly functioning networks to drive so many life-sustaining activities, IoT security is now a matter of homeland security.

¹ In this context, the term IoT refers to the connection of systems and devices with primarily physical purposes (e.g. sensing, heating/cooling, lighting, motor actuation, transportation) to information networks (including the Internet) via interoperable protocols, often built into embedded systems.

It is imperative that government and industry work together, quickly, to ensure the IoT ecosystem is built on a foundation that is trustworthy and secure. In 2014, the President's National Security Telecommunications Advisory Committee (NSTAC) highlighted the need for urgent action.

IoT adoption will increase in both speed and scope, and [will] impact virtually all sectors of our society. The Nation's challenge is ensuring that the IoT's adoption does not create undue risk. Additionally.... there is a small—and rapidly closing—window to ensure that IoT is adopted in a way that maximizes security and minimizes risk. If the country fails to do so, it will be coping with the consequences for generations.²

The time to address IoT security is right now. This document sets the stage for engagement with the public and private sectors on these key issues. It is a first step to motivate and frame conversations about positive measures for IoT security among IoT developers, manufacturers, service providers, and the users who purchase and deploy the devices, services, and systems. The following principles and suggested practices provide a strategic focus on security and enhance the trust framework that underpins the IoT ecosystem.

Overview of Strategic Principles

Many of the vulnerabilities in IoT could be mitigated through recognized security best practices, but too many products today do not incorporate even basic security measures. There are many contributing factors to this security shortfall. One is that it can be unclear who is responsible for security decisions in a world in which one company may design a device, another supplies component software, another operates the network in which the device is embedded, and another deploys the device. This challenge is magnified by a lack of comprehensive, widely-adopted international norms and standards for IoT security. Other contributing factors include a lack of incentives for developers to adequately secure products, since they do not necessarily bear the costs of failing to do so, and uneven awareness of how to evaluate the security features of competing options.

The following principles, set forth in the next section, offer stakeholders a way to organize their thinking about how to address these IoT security challenges:

Incorporate Security at the Design Phase

Advance Security Updates and Vulnerability Management

Build on Proven Security Practices

² National Security Telecommunications Advisory Committee Report to the President on the Internet of Things, November 19, 2014.

Prioritize Security Measures According to Potential Impact

Promote Transparency across IoT

Connect Carefully and Deliberately

As with all cybersecurity efforts, IoT risk mitigation is a constantly evolving, shared responsibility between government and the private sector. Companies and consumers are generally responsible for making their own decisions about the security features of the products they make or buy. The role of government, outside of certain specific regulatory contexts and law enforcement activities, is to provide tools and resources so companies, consumers, and other stakeholders can make informed decisions about IoT security.

Scope, Purpose, and Audience

The purpose of these non-binding principles is to equip stakeholders with suggested practices that help to account for security as they develop, manufacture, implement, or use network-connected devices. Specifically, these principles are designed for:

1	IoT developers to factor in security when a device, sensor, service, or any component of the IoT is being designed and developed;
2	IoT manufacturers to improve security for both consumer devices and vendor managed devices;
3	Service providers , that implement services through IoT devices, to consider the security of the functions offered by those IoT devices, as well as the underlying security of the infrastructure enabling these services; and
4	Industrial and business-level consumers (including the federal government and critical infrastructure owners and operators) to serve as leaders in engaging manufacturers and service providers on the security of IoT devices.

STRATEGIC PRINCIPLES FOR SECURING IOT

The principles set forth below are designed to improve security of IoT across the full range of design, manufacturing, and deployment activities. Widespread adoption of these strategic principles and the associated suggested practices would dramatically improve the security posture of IoT. There is, however, no one-size-fits-all solution for mitigating IoT security risks. Not all of the practices listed below will be equally relevant across the diversity of IoT devices. These principles are intended to be adapted and applied through a risk-based approach that takes into account relevant business contexts, as well as the particular threats and consequences that may result from incidents involving a network-connected device, system, or service.

Incorporate Security at the Design Phase

Security should be evaluated as an integral component of any network-connected device. While there are exceptions, in too many cases economic drivers or lack of awareness of the risks cause businesses to push devices to market with little regard for their security. Building security in at the design phase reduces potential disruptions and avoids the much more difficult and expensive endeavor of attempting to add security to products after they have been developed and deployed. By focusing on security as a feature of network-connected devices, manufacturers and service providers also have the opportunity for market differentiation. The practices below are some of the most effective ways to account for security in the earliest phases of design, development, and production.

What are the potential impacts of not building security in during design?

Failing to design and implement adequate security measures could be damaging to the manufacturer in terms of financial costs, reputational costs, or product recall costs. While there is not yet an established body of case law addressing IoT context, traditional tort principles of product liability can be expected to apply.

SUGGESTED PRACTICES:

Enable security by default through unique, hard to crack default user names and passwords. User names and passwords for IoT devices supplied by the manufacturer are

often never changed by the user and are easily cracked. Botnets operate by continuously scanning for IoT devices that are protected by known factory default user names and passwords. Strong security controls should be something the industrial consumer has to deliberately disable rather than deliberately enable.

Build the device using the most **recent operating system** that is technically viable and economically feasible. Many IoT devices use Linux operating systems, but may not use the most up-to-date operating system. Using the current operating system ensures that known vulnerabilities will have been mitigated.

Use **hardware that incorporates security features** to strengthen the protection and integrity of the device. For example, use computer chips that integrate security at the transistor level, embedded in the processor, and provide encryption and anonymity.

Design with system and operational disruption in mind. Understanding what consequences could flow from the failure of a device will enable developers, manufacturers, and service providers to make more informed risk-based security decisions. Where feasible, developers should build IoT devices to fail safely and securely, so that the failure does not lead to greater systemic disruption.



Promote Security Updates and Vulnerability Management

Even when security is included at the design stage, vulnerabilities may be discovered in products after they have been deployed. These flaws can be mitigated through patching, security updates, and vulnerability management strategies. In designing these strategies, developers should consider the implications of a device failure, the durability of the associated product, and the anticipated cost of repair. In the absence of the ability to deploy security updates, manufacturers may be faced with the decision between costly recalls and leaving devices with known vulnerabilities in circulation.

FOCUS ON: NTIA Multi-Stakeholder Process on Patching and Updating

The National Telecommunications and Information Administration (NTIA) has convened a multi-stakeholder process concerning the “Internet of Things Upgradability and Patching” to bring stakeholders together to share the range of views on security upgradability and patching, and to establish more concrete goals for industry-wide adoption.

SUGGESTED PRACTICES:

Consider ways in which to **secure the device over network connections or through automated means**. Ideally, patches would be applied automatically and leverage cryptographic integrity and authenticity protections to more quickly address vulnerabilities.

Consider **coordinating software updates among third-party vendors** to address vulnerabilities and security improvements to ensure consumer devices have the complete set of current protections.

Develop **automated mechanisms for addressing vulnerabilities**. In the software engineering space, for example, there are mechanisms for ingesting information from critical vulnerability reports sourced from the research and hacker communities in real time. This allows developers to address those vulnerabilities in the software design, and respond when appropriate.

Develop a policy regarding the **coordinated disclosure of vulnerabilities**, including associated security practices to address identified vulnerabilities. A coordinated disclosure policy should involve developers, manufacturers, and service providers, and include information regarding any vulnerabilities reported to a computer security incident response team (CSIRT). The US Computer Emergency Readiness Team (US-CERT), Industrial Control Systems (ICS)-CERT, and other CSIRTs provide regular technical alerts, including after major incidents, which provide information about vulnerabilities and mitigation.

Develop an **end-of-life strategy** for IoT products. Not all IoT devices will be indefinitely patchable and updateable. Developers should consider product sunset issues ahead of time and communicate to manufacturers and consumers expectations regarding the device and the risks of using a device beyond its usability date.



Build on Recognized Security Practices

Many tested practices used in traditional IT and network security can be applied to IoT. These approaches can help identify vulnerabilities, detect irregularities, respond to potential incidents, and recover from damage or disruption to IoT devices.

FOCUS ON: NIST Cybersecurity Risk Management Framework

The National Institute of Standards and Technology (NIST) published a framework for cybersecurity risk management that has been widely adopted by private industry, integrated across sectors, and within organizations. The framework is widely recognized as a comprehensive touchstone for organizational cyber risk management <https://www.nist.gov/cyberframework>. While not specific to IoT, the risk framework provides a starting point for considering risks and best practices.

SUGGESTED PRACTICES:

Start with **basic software security and cybersecurity practices** and apply them to the IoT ecosystem in flexible, adaptive, and innovative ways.

Refer to relevant **Sector-Specific Guidance**, where it exists, as a starting point from which to consider security practices. Some federal agencies address security practices for the unique sectors that they regulate. For example, the National Highway Traffic Safety Administration (NHTSA) recently released guidance on [Cybersecurity Best Practices for Modern Vehicles](#) that address some of the unique risks posed by autonomous or semi-autonomous vehicles. Similarly, the Food and Drug Administration released draft guidance on [Postmarket Management of Cybersecurity in Medical Devices](#).

Practice defense in depth. Developers and manufacturers should employ a holistic approach to security that includes layered defenses against cybersecurity threats, including user-level tools as potential entry points for malicious actors. This is especially valuable if patching or updating mechanisms are not available or insufficient to address a specific vulnerability.

Participate in **information sharing platforms** to report vulnerabilities and receive timely and critical information about current cyber threats and vulnerabilities from public and private partners. Information sharing is a critical tool in ensuring stakeholders are aware of threats as they arise³. The Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC), as well as multi-state and sector-specific information sharing and analysis centers (ISACs) and information sharing and analysis organizations (ISAOs), are examples.

³ ["Information Sharing."](#) National Cybersecurity and Communications Information Center.

Prioritize Security Measures According to Potential Impact

Risk models differ substantially across the IoT ecosystem. For example, industrial consumers (such as nuclear reactor owners and operators) will have different considerations than a retail consumer. The consequences of a security failure across different customers will also vary significantly. Focusing on the potential consequences of disruption, breach, or malicious activity across the consumer spectrum is therefore critical in determining where particular security efforts should be directed, and who is best able to mitigate significant consequences.

Should IoT security measures focus on the IoT device?

Since the purpose of all IoT processes is to take in information at a physical point and motivate a decision based on that information (sometimes with physical consequences), security measures can focus on one or more parts of the IoT process. As noted earlier, the risks to IoT begin with the specific device, but are certainly not limited to it. Developers, manufacturers, and service providers should consider specific risks to the IoT device as well as process and service, and make decisions based on relative impact to all three as to where the most robust measures should be applied.

SUGGESTED PRACTICES:

Know a device's **intended use and environment**, where possible. This awareness helps developers and manufacturers consider the technical characteristics of the IoT device, how the device may operate, and the security measures that may be necessary.

Perform a “**red-teaming**” **exercise**, where developers actively try to bypass the security measures needed at the application, network, data, or physical layers. The resulting analysis and mitigation planning should help prioritize decisions on where and how to incorporate additional security measures.

Identify and authenticate the devices connected to the network, especially for industrial consumers and business networks. Applying authentication measures for known devices and services allows the industrial consumer to control those devices and services that are within their organizational frameworks.

Promote Transparency across IoT

Where possible, developers and manufacturers need to know their supply chain, namely, whether there are any associated vulnerabilities with the software and hardware components provided by vendors outside their organization. Reliance on the many low-cost, easily accessible software and hardware solutions used in IoT can make this challenging. Because developers and manufacturers rely on outside sources for low-cost, easily accessible software and hardware solutions, they may not be able to accurately assess the level of security built into component parts when developing and deploying network-connected devices. Furthermore, since many IoT devices leverage open source packages, developers and manufacturers may not be able to identify the sources of these component parts.

Increased awareness could help manufacturers and industrial consumers identify where and how to apply security measures or build in redundancies. Depending on the risk profile of the product in question, developers, manufacturers, and service providers will be better equipped to appropriately mitigate threats and vulnerabilities as expeditiously as possible, whether through patching, product recall, or consumer advisory.

SUGGESTED PRACTICES:

Conduct end-to-end risk assessments that account for both internal and **third party vendor risks**, where possible. Developers and manufacturers should include vendors and suppliers in the risk assessment process, which will create transparency and enable them to gain awareness of potential third-party vulnerabilities and promote trust and transparency. Security should be readdressed on an ongoing basis as the component in the supply chain is replaced, removed or upgraded.

Consider creating a **publicly disclosed mechanism for using vulnerability reports**. Bug Bounty programs, for example, rely on crowdsourcing methods to identify vulnerabilities that companies' own internal security teams may not catch.

Consider developing and employing a **software bill of materials** that can be used as a means of building shared trust among vendors and manufacturers. Developers and manufacturers should consider providing a list of known hardware and software components in the device package in a manner which is mindful of the need to protect intellectual property issues. A list can serve as a valuable tool for others in the IoT ecosystem to understand and manage their risk and patch any vulnerabilities immediately following any incident.

Connect Carefully and Deliberately

IoT consumers, particularly in the industrial context, should deliberately consider whether continuous connectivity is needed given the use of the IoT device and the risks associated with its disruption. IoT consumers can also help contain the potential threats posed by network connectivity by connecting carefully and deliberately, and weighing the risks of a potential breach or failure of an IoT device against the costs of limiting connectivity to the Internet.

In the current networked environment, it is likely that any given IoT device may be disrupted during its lifecycle. IoT developers, manufacturers, and consumers should consider how a disruption will impact the IoT device's primary function and business operations following the disruption.

Does every networked device need continuous, automated connection to the Internet?

In 2015, the Federal Trade Commission published a [guide](#) called "Start with Security: A Guide for Businesses" to help them determine this very question. While it may be convenient to have continuous network access, it may not be necessary for the purpose of the device – and systems; for example, nuclear reactors, where a continuous connection to the internet opens up the opportunity for an intrusion of potentially enormous consequences.

SUGGESTED PRACTICES:

Advise IoT consumers on the intended purpose of any network connections. Direct internet connections may not be needed to operate critical functions of an IoT device, particularly in the industrial setting. Information about the nature and purpose of connections can inform consumer decisions.

Make intentional connections. There are instances when it is in the consumer's interest not to connect directly to the Internet, but instead to a local network that can aggregate and evaluate any critical information. For example, Industrial Control Systems (ICS) should be protected through defense in depth principles as published by https://ics-cert.us-cert.gov/recommended_practices.

Build in controls to allow manufacturers, service providers, and consumers to disable network connections or specific ports when needed or desired to enable **selective connectivity**. Depending on the purpose of the IoT device, providing the consumers with guidance and control over the end implementation can be a sound practice.

CONCLUSION

Our nation cannot afford a generation of IoT devices deployed with little consideration for security. The consequences are too high given the potential for harm to our critical infrastructure, our personal privacy, and our economy.

As DHS issues these principles, we recognize the efforts underway by our colleagues at other federal agencies, and the work of private sector entities to advance architectures and institute practices to address the security of the IoT. This document is a first step to strengthen those efforts by articulating overarching security principles. But next steps will surely be required.

DHS identifies four lines of effort that should be undertaken across government and industry to fortify the security of the IoT.

FOUR LINES OF EFFORT:

1



Coordinate across federal departments and agencies to engage with IoT stakeholders and jointly explore ways to mitigate the risks posed by IoT.

DHS with its federal partners will continue to engage with industry partners to determine approaches that can further enhance IoT security, and to promote understanding of evolving technology trends that may address IoT risks. Future efforts will also focus on updating and applying these principles, as best practices and approaches are further refined and understood.

2



Build awareness of risks associated with IoT across stakeholders.

It is important that stakeholders are aware of IoT risks so that they can position themselves to address them. DHS will accelerate public awareness, education, and training initiatives, in partnership with other agencies, the private sector, and international partners. DHS, together with other agencies, will also undertake initiatives more directly tailored to particular sectors and individual consumers.

3



Identify and advance incentives for incorporating IoT security.

Policymakers, legislators, and stakeholders need to consider ways to better incentivize efforts to enhance the security of IoT. In the current environment, it is too often unclear who bears responsibility for the security of a given product or system. In addition, the costs of poor security are often not borne by those best positioned to increase security. DHS and all other stakeholders need to consider

how tort liability, cyber insurance, legislation, regulation, voluntary certification management, standards-settings initiatives, voluntary industry-level initiatives, and other mechanisms could improve security while still encouraging economic activity and groundbreaking innovation. Going forward, DHS will convene with partners to discuss these critical matters and solicit ideas and feedback.

4



Contribute to international standards development processes for IoT.

IoT is part of a global ecosystem, and other countries and international organizations are beginning to evaluate many of these same security considerations. It is important that IoT-related activities not splinter into inconsistent sets of standards or rules. As DHS becomes increasingly focused on IoT efforts, we must engage with our international partners and the private sector to support the development of international standards and ensure they align with our commitment to fostering innovation and promoting security.

DHS looks forward to these next collaborative steps. Together, we can, and must, address these complex challenges. By doing so, we will ensure that our network-connected future is not only innovative, but also secure and built to last.

APPENDIX: GUIDANCE AND ADDITIONAL RESOURCES

The principles in this document have been developed based on information gathered from industry reports, and through discussions with private industry, trade associations, non-governmental entities, and Federal partners, especially with NIST and NTIA.

Department of Homeland Security

- <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>

Other Federal Entities

- [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) Announcement for [Fostering the Advancement of the Internet of Things Workshop](#)
 5. Internet Policy Task Force [resource/review/cataloging](#) of the benefits, challenges, and potential roles for the government in fostering the advancement of the Internet of Things.
- NIST
 1. Cybersecurity [Framework](#)
 2. [Cyber-Physical Systems \(CPS\) Program](#)
 - a) CPS Public Working Group (PWG) [draft Cyber-Physical Systems \(CPS\) Framework Release 1.0](#)
 - [Comments accepted through 9/2/2015](#)

3. [Smart-Grid](#) Program
 4. International Technical Working Group on [IoT-Enabled Smart City Framework](#)
 5. NIST Special Publication (SP) [800-183](#), Network of Things, 7/28/2016.
 - a) NIST [news release](#)
- Federal Trade Commission
 1. FTC Staff Report, "Internet of Things: Privacy & Security in a Connected World," January 2015.
 - United States Congress
 1. Senate Committee on Commerce, Science, and Transportation committee hearing, "[The Connected World: Examining the Internet of Things](#)."
 2. Senate unanimously bipartisan resolution ([S. Res. 110](#)) calling for a national strategy to guide the development of the Internet of Things.
 3. House Energy and Commerce Committee's "[The Internet of Things: Exploring the Next Technology Frontier](#)"
 - Government Accounting Office
 1. [GAO engagement with DHS](#): GAO is currently engaged with DHS on IoT, code 100435 [January 15, 2016 notification letter available via this [link](#)]
 - a) Status/entry in the most recent, June 3, 2016 [List of Active GAO Engagements Related to DHS](#)

External Sources

The list of additional resources is provided solely as a reference and does not constitute an endorsement by the Department of Homeland Security (DHS). DHS does not endorse any commercial product, service, or enterprise.

- Atlantic Council
 1. Smart Homes and the Internet of Things – <http://www.atlanticcouncil.org/publications/issue-briefs/smart-homes-and-the-internet-of-things>
- I Am The Cavalry
 1. Five Star Automotive Cyber Safety Framework – <https://iamthecavalry.org/5star>
 2. Hippocratic Oath for Connected Medical Devices – <https://iamthecavalry.org/oath>
- Online Trust Alliance
 1. [Consumer Best Practices](#)
- Industrial Internet Consortium: <http://www.iiconsortium.org/IISF.htm>
- Open Web Application Security Project (OWASP)

1. Internet of Things Project
[https://www.owasp.org/index.php/OWASP Internet of Things Project](https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project)
 2. Internet of Things Security Guidance
[https://www.owasp.org/index.php/IoT Security Guidance](https://www.owasp.org/index.php/IoT_Security_Guidance)
- Safecode.org relevant industry best practices www.safecode.org
 - AT&T
 1. [Exploring IoT Security](#)
 - Symantec
 1. [An Internet of Things Reference Architecture](#)

