

Before the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
DEPARTMENT OF COMMERCE
Washington, D.C. 20230

In the Matter of

The Benefits, Challenges, and
Potential Roles for Government in
Fostering the Advancement of the
Internet of Things

Docket No. 170105023–7023–01
RIN 0660–XC033

COMMENTS OF CISCO SYSTEMS, INC.

Cisco Systems, Inc. (“Cisco”) welcomes the opportunity to provide further input¹ to the Department of Commerce on issues raised by the National Telecommunications and Information Administration’s (“NTIA”) request for comments (“Supplemental Request”) regarding “the benefits, challenges, and potential roles for the government in fostering the advancement of the Internet of Things” (“IoT”).²

I. INTRODUCTION

The NTIA Green Paper called out a number of policy issues relating to the development of the IoT, as well as a series of core principles that government should advance or assist in advancing.³

¹ These comments supplement comments previously provided by Cisco Systems, Inc. in response to a prior request for public comment by the National Telecommunications and Information Administration date June 2, 2016 (Original Request).

[https://www.ntia.doc.gov/files/ntia/publications/cisco - ntia iot comments 6-2-2016-c1.pdf](https://www.ntia.doc.gov/files/ntia/publications/cisco_-_ntia_iot_comments_6-2-2016-c1.pdf)

² National Telecommunications and Information Administration, RIN 0660–XC033, “The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things: Notice, Request for Public Comment” (January 13, 2017) (Supplemental Request). <https://www.ntia.doc.gov/federal-register-notice/2017/request-comments-benefits-challenges-and-potential-roles-government>. The Supplemental Request was developed to solicit feedback on the findings of the NTIA “Green Paper” also issued January 2017.

<https://www.ntia.doc.gov/other-publication/2017/green-paper-fostering-advancement-internet-things>.

³ Green Paper at 2-3, 15.

The Green Paper also presents a view on the next steps that the federal government should take to support the continued growth of the IoT. The policy analysis presented in the Green Paper covers a wide range of issues, but in this round of comments, Cisco will focus our attention on a core area of our interest and expertise—cybersecurity.

In doing so, we thank the Department of Commerce, including NTIA and the National Institute for Standards and Technology (NIST), for its continued focus on improving cybersecurity through the development of not only the NIST Cybersecurity Framework, but also by spotlighting areas that required specific focus and attention. IoT is such an area because of the unprecedented growth in scale of the network. Every day we develop and bring online increasing numbers of connected devices. We also continue to add connectivity to devices originally designed without such capabilities.⁴

The growth of IOT and our increasing reliance on connected “things” throughout our daily lives requires more attention be paid to the principles of Security by Design and Privacy by Design. However, even if dramatic changes could instantly be made to the quality of connected devices on a going-forward basis, there are already tens of millions—if not hundreds of millions—of previously manufactured devices that are now or may yet be connected to the Internet. This underscores the increasing importance of utilizing the network as both a sensor and a tool to manage risk from: a) devices that cannot effectively protect themselves in a dynamic threat environment; and b) from devices becoming weapons in an attack on other devices or systems.

⁴ For example, IOT technologies make it possible to transform dangerous mining jobs by allowing trucks that drive into blast sites to operate via remote control instead of risking the life of a human driver. http://www.cisco.com/c/m/en_us/never-better/digital-business.html

In this comment, Cisco will discuss how growth in the IoT market is impacting how market participants, including the government, must address cybersecurity. We will then discuss Security and Privacy by Design principles before turning to the important role networks can play in managing cybersecurity risk. Finally, we will discuss government's role in assisting industry in developing a skilled workforce and the need for more focused research on IoT cybersecurity.

II. GROWTH IN THE IOT MARKET

Cisco's Visual Networking Index (VNI) provides global IP traffic forecasts and analysis regarding the dynamic factors that facilitate network growth. The following statistics from the recent report, "The Zettabyte Era—Trends and Analysis," demonstrate the staggering scale of IP network growth:²

- Annual global IP traffic will pass the zettabyte (ZB) threshold by the end of 2016 and reach 2.3 ZB per year by 2020. (A zettabyte is 1000 exabytes, or 1 billion terabytes.) That represents a threefold increase in global IP traffic in the next 5 years.
- Traffic from wireless and mobile devices will account for two-thirds (66 percent) of total IP traffic by 2020. Wired devices will account for only 34 percent.
- From 2015 to 2020, average broadband speeds will nearly double.
- By 2020, 82 percent of all consumer Internet traffic globally will be IP video traffic, up from 70 percent in 2015.

The challenge of securing networks growing at that pace and operating at such scales are almost beyond human comprehension—and certainly beyond human capabilities. Our experience indicates that without automation, security becomes very challenging when the ratio of managed devices to IT professionals exceeds 200:1. Cisco's 2017 Annual Cybersecurity Report (Cisco

ACR) shows that almost half of IT professionals surveyed already face upwards of 5,000 alerts per day.⁵

The 2017 Cisco ACR goes on to note that almost half of those alerts go uninvestigated: Perhaps due to several factors—such as the lack of an integrated defense system or the lack of staff time—organizations are able to investigate a little more than half the security alerts they receive in a given day. As shown in Figure 52, 56 percent of alerts are investigated, and 44 percent are not investigated; of those alerts that are investigated, 28 percent are deemed legitimate alerts. Forty-six percent of legitimate alerts are then remediated.

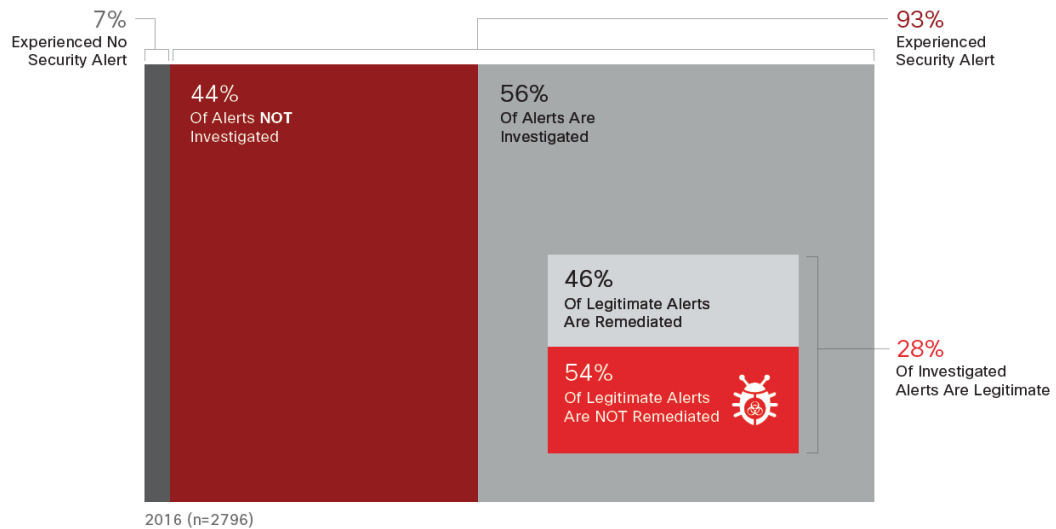
To put the problem into more concrete terms, if an organization records 5000 alerts per day, this means:

- 2800 alerts (56 percent) are investigated, while 2200 (44 percent) are not
- Of those investigated, 784 alerts (28 percent) are legitimate, while 2016 (72 percent) are not
- Of the legitimate alerts, 360 (46 percent) are remediated, while 424 (54 percent) are not remediated⁶

⁵ <http://blogs.cisco.com/security/announcing-the-cisco-2017-annual-cybersecurity-report>.

⁶ 2017 Cisco ACR p. 54.

Figure 52 Percentages of Security Alerts That Are Not Investigated or Remediated



Source: Cisco 2017 Security Capabilities Benchmark Study

The key to improving risk management decision-making in an environment growing this quickly is automation. We must clean up the “signal to noise” ratio by assigning those security tasks capable of being automated to machines. This will allow humans to focus on the problems that require their focused attention and creativity.

III. SECURITY AND PRIVACY BY DESIGN

Security by Design and Privacy by Design are important concepts that will help improve the quality of devices and services—brought to market. Given that the IoT market is relatively new, it will take time to sort out what the norms are with regard to privacy and security. However, we propose that the problem space relating to the development of privacy and security norms could be viewed as having three layers.

In the top layer, there are existing regulated spaces where IoT technologies may prove a useful adjunct to existing computing systems used to operate critical infrastructure. Before being allowed to operate in those regulated environments, we should expect that the IoT devices will be subject to rigorous testing and certification so that their capabilities and limitations can be carefully

ascertained and verified. Such assessments may very well test whether and to what extent IoT devices properly manage security risk but also what their fault tolerances are. This data will help us understand how resilient these devices are against failure that could impact availability or reliability of critical functions, and, therefore, cause unacceptable risk of harm to public safety.

In exchange for this increased level of scrutiny, we should reasonably expect that IoT devices appropriate for use in critical systems will be more expensive than the rest of the market—and that associated innovation will be slower. When attempting to classify IoT devices, it is, therefore, important to consider the establishing classes or categories of devices based on factors such as risk and cyber resilience that align to matching controls, protection, and privacy regulations. For example, a consumer device such as a connected doorbell needs fewer security controls than an implantable medical device or a device that operates a critical infrastructure system—e.g., water filtration or power distribution.

In the bottom layer, there will be technology development practices sufficiently unreasonable from a societal standpoint that they will yield devices unacceptable for sale in the marketplace by the legal system regardless of the level of criticality for its expected use. The Federal Trade Commission (FTC) has been actively defining this space through its consumer protection enforcement actions. We should anticipate that the FTC will continue to challenge security practices it concludes are well outside the mainstream—e.g., hard-coded usernames and passwords in Internet-connected consumer appliances. The FTC has also done important work educating developers of technology and the institutions that fund their development via its "Start with Security" training program and related online guidance distilled from its casework on security.⁷

⁷ <https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business>

In the middle, the rest of the market will be defined with reference to standards and best practices that allow technology buyers to decide what level of risk they are willing to accept given the environment where they seek to deploy IoT technologies. Existing principles for privacy and data protection will remain very relevant to the development of the IoT market—e.g., the Fair Information Practice Principles (FIPPs) and the related OECD Guidelines. Consumers will still expect notice, choice, access, security, and enforcement in an IoT world. It will, however, take time to understand how to translate some of those concepts to an environment where devices may lack screens to display notice or keyboards to allow for user input.

By the same token, our understanding of what level of security can reasonably be expected from inexpensive, low-power IoT devices may evolve over time as well. We do not yet know what security responsibilities consumers and end-users should reasonably expect to assume. It is also not yet apparent how much security buyers will be willing to pay for even when they understand the risks of connected technologies.

As we gain greater experience managing the risks and benefits of these technologies, governments should continue to forbear from developing regulatory approaches to the IoT marketplace. In exchange, industry must endeavor to avoid security and privacy practices that are likely to shock or cause unreasonable surprise. It is incumbent on developers of technology to demonstrate trustworthiness. With this in mind, we note that the NTIA Green Paper references the notion of trustworthiness, but does not seek to define it.⁸ At Cisco, Trustworthiness is one of our Trust Principles, which also include Transparency and Accountability. We demonstrate trustworthiness through the following commitments:

⁸ Green Paper at 6 and 19.

- We take active measures to safeguard the security and reliability of the network.
- We are committed to securing and protecting our customers and their data.
- We adhere to a Secure Development Lifecycle (SDL) in the development of our products and services.
- We protect the security of our value chain.⁹

IV. **ROLE OF THE NETWORK IN MANAGING IOT**

Even as significant improvements are made to device security, the network must play an important role in defending devices that cannot protect themselves—and in protecting devices from being used to attack devices and systems. At Cisco, we are exploring the development of standards and new technologies that can better instrument the network and enable automation of security challenges. For example, there may be useful information capable of facilitating better network management that could be derived from standardized manufacturer declarations regarding IP traffic that would be considered either within the range of expectations or, alternatively, anomalous.¹⁰

Along these lines, there has been some discussion about the need to develop “lightweight” cryptography given the need for secure communication between connected devices and the likelihood that many such devices may not be capable of supporting state of the art standards—e.g., Advanced Encryption Standard (AES), Elliptic curve Diffie-Hellman (ECDH), or Elliptic

⁹ <https://www.cisco.com/c/en/us/about/trust-transparency-center/principles.html>

¹⁰ See IETF draft standard on Manufacturer Usage Descriptions. <https://tools.ietf.org/html/draft-ietf-opsawg-mud-02>. Also see, IETF work on automated networking, “which refers to the self-managing characteristics (configuration, protection, healing, and optimization) of distributed network elements, adapting to unpredictable changes while hiding intrinsic complexity from operators and users.” <https://datatracker.ietf.org/wg/anima/about/>

Curve Digital Signature Algorithm (ECDSA). However, we are somewhat skeptical about the need to prioritize the development of IOT-specific “lightweight” algorithms for two reasons. First, most IoT devices built with Internet connectivity should be capable of handling standard Internet cryptography. Second, crypto-security is essentially all or nothing—a device is going to be either capable of running widely accepted encryption suites or it is not.¹¹ Certain minimum compute capabilities are required to ensure proper implementation of encryption. Devices that lack those capabilities are unlikely to be secure absent some further assistance from the network.

V. SKILLS AND WORKFORCE DEVELOPMENT

Cisco agrees that there is a major area of need around fostering the skills to securely develop and operate connected technologies. To help close this security skills gap, Cisco is introducing the Global Cybersecurity Scholarship program. Cisco has committed to invest \$10 million in this program to increase the pool of talent with critical cybersecurity proficiency.¹² The government should also make targeted investments in this area—particularly in the context of networking IoT devices with limited computing capabilities. This might involve incentivizing state colleges and universities to adopt degree or certificate programs around cybersecurity and privacy—both at undergrad and graduate levels. Today, there are very few such programs.

One possible starting point would be an existing NIST program called the National Initiative for Cybersecurity Education (NICE).¹³ Within the context of that initiative, it may be possible to develop a program focused on the IoT market. In addition to skills development for students,

¹¹ See <http://csrc.nist.gov/groups/ST/lwc-workshop2015/papers/session8-mcgrew-paper.pdf>

¹² <https://mkto.cisco.com/security-scholarship>

¹³ <http://csrc.nist.gov/nice>

workforce development for existing workers is an area of continuing interest for leaders in the technology industry to partner with the government.

VI. Consumer Education and Research and Development

We also believe that two other areas require significant investment by the government: 1) consumer education; and 2) research and development. Cisco believes that it is vital for our society to both educate consumers and users of technologies about their shared responsibility for managing cyber-risks. As a result, Cisco is committed to partnering with the National Cybersecurity Alliance and serves as a board member for the organization.¹⁴ Finally, in addition to these workforce and consumer security initiatives, more work on advancing the state of the art for IOT security research is required. This is a key area of focus for the Cisco Research Center.¹⁵

VII. CONCLUSION

We look forward to working with NTIA to foster the development of industry-led standards and best practices to advance the state of IoT security. We firmly believe that current efforts to translate the concepts of Security by Design and Privacy by Design in to the IoT market are evolving in a meaningful way. We thank the Department of Commerce for serving as a convener of all interested stakeholders, which has significantly accelerated this process.

As the Department of Commerce acknowledges, the government should continue to proceed cautiously with regard to the promulgation of IoT-specific regulations or we will not see the full potential of this technology come to fruition. In exchange for this opportunity to advance exciting new connected technologies, industry must focus on developing devices with trustworthiness in

¹⁴ <https://staysafeonline.org/about-us/board-members>

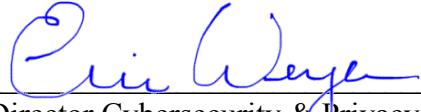
¹⁵ <https://research.cisco.com/research>

mind. It is also likely that even as the level of security improves in IoT devices, they will be operating in a dynamic threat environment where threat actors are learning and changing their tactics.

As a result, it is very likely the case that the network will assume a central role in protecting devices against attack and in guarding against scenarios where IoT devices themselves are turned into offensive instrumentalities. We look forward to continuing our engagement on these important issues.

Respectfully submitted,

Cisco Systems

By: 
Director Cybersecurity & Privacy Policy
Cisco Global Government Affairs

Cisco Systems, Inc.
601 Pennsylvania Ave., NW
North Bldg., Suite 900
Washington, DC 20004

March 13, 2017