Response to Request for Public Comment

[RIN 0660–XC033]

[Docket No. 170105023–7023–01]

National Telecommunications and Information Administration (NTIA)

Department of Commerce

Attention: IOT RFC
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Ave. NW
Washington, DC 20230

Katherine Gronberg
Vice President, Government Affairs

Timothy Jones | CISSP, CISM, CCSK, FSCA
Systems Engineer - Public Sector
ForeScout Technologies, Inc.
408.213.3191
info@forescout.com

ForeScout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134
866.377.8771

ForeScout Technologies, Inc.

Response to the National Telecommunications and Information Administration's (NTIA) Request for Public Comment on its Green Paper: "Fostering the Advancement of the Internet of Things"

February 27, 2017

ForeScout Technologies is pleased to provide comments in response to the NTIA's green paper, ''Fostering the Advancement of the Internet of Things." We commend the NTIA on its efforts to understand and explain the opportunities and challenges presented by the Internet of Things (IoT). This report represents an extremely thoughtful and comprehensive effort.

1) Is our discussion of IoT presented in the green paper regarding the challenges, benefits, and potential role of government accurate and/or complete? Are there issues that we missed, or that we need to reconsider?

With respect to section B(i) ("Cybersecurity"), we believe this section warranted a more thorough discussion of the challenge of visibility when it comes to IoT in a network environment. A basic tenet of cybersecurity is: "You can't protect what you can't see." Hardware and software asset management are the top two security controls in both the National Institute for Standards and Technology (NIST) cybersecurity framework and the SANS Top 20 Controls[1]. Put simply, "hardware management" and "software management" mean: you should know what's on your networks and know what software those devices are running. It can be difficult enough for companies and government agencies to have an accurate and current picture of devices running traditional operating systems in their enterprises. Yet "domain awareness" is vastly more difficult with respect to IoT devices because they typically cannot be "seen" by traditional cybersecurity tools.

IoT devices are quite different from traditional information technology devices, meaning, laptops, desktops and servers. They differ mainly in the sense that they have minimal hardware, non-standard operating systems and very limited processing capabilities. In general, agents cannot be installed on most types of IOT devices. An "agent" is a small piece of software that resides on a device. Agents can have various functions and, among other things, can allow a device to be scanned for malware and vulnerabilities. Such agents usually connect back to a server, which has a list of new malware to check for (and remediate) or new patches that must be installed on the device's OS or firmware. Because IoT devices generally do not run security agents, they are difficult for most existing vulnerability scanning tools to see on the network: they only see that something is "there" and cannot tell what it is, what it's running or how it's behaving. From a security

[1]NIST Framework https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf and SANS Critical Security Controls: https://www.sans.org/media/critical-security-controls/Poster_Fall_2014_CSCs_WEB.PDF

standpoint, the endpoint is invisible. Hence, to protect IoT devices, solutions that do not require agents are needed.

Although IoT devices are invisible to most existing cybersecurity tools, it's important to realize how prevalent they already are in the enterprise. According to leading analysts (Gartner and IDC), the number of connected devices is anticipated to grow from five billion now to 30 billion by 2020.[2] Federal agencies are already beginning to address the problem of IoT on their networks through two large-scale programs, the Continuous Diagnostics and Mitigation Program (CDM) for civilian agencies and Comply to Connect (C2C) for the Department of Defense (DoD). What is groundbreaking about these programs is that they will give the agencies *continuous* domain awareness—knowledge of a device's presence on the network the instant it connects to the network, versus a periodic scan— and they will allow agencies to discover and account for devices, including non-traditional IoT and operational technology (OT) devices. We support Booz Allen Hamilton's comments to the NTIA, "Organizations should include IoT devices in their continuous monitoring strategy to maintain ongoing awareness of security threats and vulnerabilities."[3]

How consumers implement these strategies at home is a slightly different matter. While there is a long way to go in terms of offering consumers affordable and user-friendly tools to monitor the devices on their home network, ForeScout is encouraged by the debut of several such tools at this year's Consumer Electronic Show. Further, IoT "platforms" intended for home-use (for example, Google Home or Amazon Echo), while not explicitly security tools, could eventually be configured to provide more security benefits such as notifying users when devices exhibit abnormal behavior.

2) Is the approach for Departmental action to advance the Internet of Things comprehensive in the areas of engagement? Where does the approach need improvement?

ForeScout believes the NTIA Green Paper could have placed a stronger emphasis on the increased attack surface that IoT creates. In its response to the original NTIA Request for Comments, the American Bar Association's Science and Technology section pointed out, "The highly networked nature of IoT creates a large number of attack surfaces that can be exploited."[4] This reality cannot be overstated. We define attack surface (or threat surface) as our exposure to known or unknown threats with their associated exploitable vulnerabilities. The estimated 30 billion devices predicted by 2020 represents a 30-fold increase from 2009.[5] It is critical to understand that this explosive growth in the amount of IoT on networks translates proportionally into explosive growth of the attack/threat surface that can be exploited by hackers.

---

[2] http://www.idc.com/infographics/IoT
[3] Response to Request for Comment, Booz Allen Hamilton, Inc., June 2, 2016, p. 12
[4] Response to Request for Comment, ABA Section of Science & Technology Law, June 2, 2016, p. 11
[5] http://www.gartner.com/newsroom/id/2636073

Vulnerable devices, no matter what their flavor (i.e. consumer, operational or industrial), serve as a possible entry point for attackers to move laterally within the organization's networks to higher value assets (HVAs) such as customer data, intellectual property or data that is sensitive from a physical security standpoint. They also open the door to disruption of operations across the organization, potentially leading to partial or full system downtime—or even outright failure. Finally, vulnerable IoT devices on a widespread scale can be conscripted by attackers to conduct large-scale denial of service attacks, against one's own infrastructure or someone else's.

The Green Paper states: "…The ubiquity of and dependence on IoT magnifies the security risk on each domain, whether it is the power grid, our automobiles, or children's toys. The distributed denial of service (DDOS) attack in October 2016 on a Domain Name Service (DNS) provider's lookup service that used an army of IoT devices protected only by factory-default passwords is an example of how Internet-connected devices have changed the cybersecurity environment." Here, the report is citing a report by Brian Krebs about the Mirai botnet attack which occurred in the fall of 2016, in which hundreds of thousands of compromised IoT devices were exploited to take down web hosting services that caused disruption to websites and web services, causing real business loss. Mr. Krebs' subsequent research into the Mirai malware is extremely eye-opening.[6] Mirai's most worrisome attribute is that it recruits new devices at an unprecedented speed, constantly scanning for Internet-facing devices with insecure factory default credentials. Mirai thus propagates itself and creates botnets that include hundreds of thousands, maybe millions, of devices – orders of magnitude larger than what we have previously seen.

The Mirai botnet was the most visible and far-reaching example of the potential IoT risks that must be mitigated, and on a global scale. Incident management in cases such as these will require enhanced coordination by the private sector, government and individual consumers. We will likely see more events like this in 2017 and beyond, and for most private enterprises as well as government agencies, even knowing that these assets are present in their environments will be a significant challenge. The inherited risk of IoT from years past will need to be addressed as we look to strengthen, centralize and prioritize IoT security going forward. The challenge of securing IoT should not prevent it from delivering its enormous potential benefits to society, so we believe the question of security in particular deserves to be elevated in this discussion.

3) Are there specific tasks that the Department should engage in that are not covered by the approach?

While it is very important to pursue measures which will lead to better security of devices themselves, we believe this area has been too great a focus of U.S. government efforts thus far. In the Green Paper, NTIA devotes a section to the concept of "Security by Design," [Section B(i)(2)]. ForeScout is inherently skeptical of the concept of "inherently secure" devices. Even when

[6] https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/?utm_source=Passcode+Subscribers&utm_campaign=e5b6c985e1-EMAIL_CAMPAIGN_2017_01_19&utm_medium=email&utm_term=0_e61b9fede0-e5b6c985e1-260729597&mc_cid=e5b6c985e1&mc_eid=6891c92e33

manufacturers are incentivized or required to create better hardware and software for these devices, there can and will be vulnerabilities – just as there are in the hardware and software applications we use in and on our desktops, laptops and servers today.

ForeScout is pleased to participate in NTIA's multistakeholder process on patching and upgradeability. This is an important effort, as IoT devices that can be truly password protected and updated to help fix vulnerabilities will go a long way toward reducing the numbers of devices worldwide that can be conscripted into botnet attacks. However, patching and upgradability have their limitations. Even if *all* device manufacturers can be persuaded, either through incentives or requirements, to produce devices that can be patched and to create secure, user-friendly patching methods, we will still face the problem, perhaps on a significant scale, of unknown vulnerabilities and/or patches that aren't delivered in time.

ForeScout advocates for a defense-in-depth approach to securing IoT, in accordance with the NIST Framework and SANS Security Controls.[7] This is not a novel idea, but we think it is worthwhile to explain how these fundamental concepts can and should be applied to securing the Internet of Things. Defense in depth, or layered defense, teaches us that we must consider security throughout the layers of the network, not only within the hardware of or software that resides on a device. A more granular approach to defense in depth leads users of IoT devices to ask more than just: "What bad things (i.e. vulnerabilities or malware) are on my device?" It requires them to also ask, "How is this device behaving?" and "What bad things are happening on my network?" If the answers to either of these questions is problematic, then a remedial action should be taken. In some cases, a remedial action could be disconnecting the device. In some cases, it could mean quarantining the device or restricting the actions it can take, such as preventing it from sending or receiving data packets. Such actions can prevent a compromised device from communicating with its command and control (C&C) server, which would prevent the device from participating in a botnet. It would also prevent a device from engaging in harmful behavior directed at its own network (such as scanning and mapping, compromising additional devices and exfiltrating data).

4) What should the next steps be for the Department in fostering the advancement of IoT?

Better authentication, encryption and patching for devices, if implemented worldwide in a reliable and accepted way, will over time help alleviate some of the threat from massive botnets, but they do not by themselves solve the problem that insecure devices presently pose to consumer and

[7] ForeScout notes that there has been criticism of the defense-in-depth approach, specifically, that it is a military concept that doesn't translate perfectly into network security. The aspects of defense in depth that are useful here are: 1) there is no "magic bullet," no single security approach or solution, to protect IT networks from attackers and multiple security mechanisms must be employed to minimize the impact of a failure in any one mechanism, and 2) it is critical to consider all layers of the Open Systems Interconnect (OSI) model in in network security design and planning, not just the physical (device) level. The OSI model is a hierarchical model of how different devices, protocols and applications can interoperate to provide a network.

enterprise networks. In the meantime and beyond, we have to rely on methodologies that allow us to protect networks and prevent rogue behavior by devices in ways that do not rely solely on processes that take place in or on the device itself.

There are a few basic policies, practices and tools that can overcome the considerable security challenges that IoT presents and allow society to realize IoT's vast potential. Agencies like NTIA, NIST and the Department of Homeland Security (and Department of Defense for the Defense Industrial Base community) can help coordinate and guide and the creation of IoT security best practices and encourage their adoption. In our opinion, these are the most important:

- **Agentless visibility.** It is essential to be able to see the devices that connect to a network and to gauge their "suitability" to be allowed to connect, without depending on an agent to know if devices exist or to profile devices. Agents cannot be deployed on all devices (such as printers, HVAC, wearables, smart TVs, security cameras and more), therefore a gap in visibility exists if we rely on agent-based visibility solutions.
- **Automation.** Automation refers to a state in which enterprises allow their security tools to respond to threats automatically, without human intervention, according to previously established policies. Automation is key to monitoring and managing a large number of diverse devices and mitigating potential threats. Automation greatly reduces the reliance on the human facilitation of patching or removing malware which can be time-consuming and prone to human error. The importance of automation in solving the IoT security problem cannot be over-emphasized.
- **Integration/Orchestration.** The ability to have an enterprise's cybersecurity tools work together to achieve instantaneous and automated mitigation is not a panacea: it exists today. It is often called "integration." ForeScout calls it "orchestration." Put simply, by providing the ability to share contextual insights and automate workflows and security processes between third-party security products, orchestration makes participating products smarter and greatly improves system-wide security effectiveness. Today, silos exist because cybersecurity vendors, often competitors, are neither required nor incentivized to create products that interoperate, demanding that humans connect the various outputs—totally defeating the concept of automation (above). The U.S. government can play a role in breaking down these silos, and should leverage its considerable buying power to influence vendors' behavior in this regard.
- **Stronger Device Security**. As outlined in this document, stronger security measures built into devices is, by itself, an incomplete solution to the IoT security problem, but it is part of the solution. All will benefit from more security-conscious device design and manufacture, and a supervised supply chain, particularly in key sectors like healthcare and critical infrastructure. This is one area where government can and must play an important coordinating and incentivizing role.
- **Certificate-Based Authentication, Encryption and Virtual Private Networks**. Capturing data is the primary activity of many, if not most, IoT devices (for example, in preventive maintenance and health-related use cases). However, devices are not equipped with, or cannot understand, basic authentication standards. If they do have authentication

guidelines, they are typically proprietary. Certificate-based authentication, coupled with encryption and Virtual Private Networks (VPNs), or encryption tunnels, will be essential. Certificate based authentication means a trusted party, called a certificate authority (CA), acts as the root of trust that authenticates the identity of individuals, computers and other entities in order to access or make changes to a device's OS or firmware. Encryption is a process that converts data into ciphertext, which renders them unreadable by humans. Authentication and encryption will need to be leveraged to protect data in transit and at rest. Virtual Private Networks (VPN) should be the transport vehicle for data to flow from client (sensor) to server (database) communication when traversing the Internet with critical/sensitive data.

About ForeScout

ForeScout Technologies is transforming security through visibility, providing Global 2000 enterprises and government agencies with agentless visibility and control of traditional and IoT devices the instant they connect to the network. Our technology continuously assesses, remediates and monitors devices and works with disparate security tools to help accelerate incident response, break down silos, automate workflows and optimize existing investments. As of September 30, 2016 more than 2,200 customers in over 60 countries improve their network security and compliance posture with ForeScout solutions. See devices. Control them. Orchestrate multivendor response. Learn how at www.forescout.com.