SAMSUNG

February 12, 2018

Via counter_botnet@list.commerce.gov

Evelyn L. Remaley
Deputy Associate Administrator
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Washington, DC 20230

Subject: Promoting Stakeholder Action Against Botnets and Other Automated Threats

Dear Ms. Remaley:

Samsung Electronics America ("Samsung") appreciates this opportunity to comment on the Department of Commerce's Draft Report to the President on "Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats" (the "Draft Report").[1] Samsung has had a U.S. manufacturing presence for nearly 40 years and recently committed to increasing its investment in the U.S. for the development and deployment of Internet of Things ("IoT") technologies.[2] Investments like Samsung's will help unleash an IoT that will benefit consumers, grow the economy, and create jobs in the United States. In fact, McKinsey determined that by 2025, IoT will have a global economic impact up to $11 trillion a year.[3]

Earlier this year at the CES 2018 trade show, Samsung reaffirmed its commitment to accelerate IoT adoption for everyone and make all Samsung devices intelligent and internet-enabled by 2020.[4] While these advancements will help consumers further realize the benefits of a seamless and simple connected life, we recognize that security is also a critical aspect to this technological innovation. Furthermore, as a global leader in manufacturing connected products, we are committed to driving the marketplace to more secure innovations. That is why we are

[1] Promoting Stakeholder Action Against Botnets and Other Automated Threats, Federal Register, January 11, 2018. www.federalregister.gov/documents/2018/01/11/2018-00322/promoting-stakeholder-action-against-botnets-and-other-automated-threats

[2] "Samsung Shows Dedication to IoT with $1.2 Billion Investment and R&D," June 21, 2016, https://news.samsung.com/us/samsung-electronics-internet-of-things-planning-1-2-billion-for-u-s-research-and-development-of-iot/

[3] https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world

[4] In 2015, Samsung announced that all of our devices would be Internet-enabled by 2020, and as of January 2018, 90% of our TVs, appliances, smartphones, and tablets are now IoT-ready. https://news.samsung.com/us/tim-baxter-samsung-of-today-and-tomorrow-ces2018/

making three important investments to help protect consumers and the broader ecosystem: (1) enhancing the cybersecurity of the IoT products we manufacture; (2) offering third party IoT innovators an open and secure IoT platform to incorporate in their IoT products; and (3) requiring device security and interoperability in order for third party IoT products to connect fully to the Samsung SmartThings cloud. We are eager to work with you and other stakeholders to accelerate further advances in these areas throughout the global IoT market and internet economy.

(1) **KNOX connected products.** As Samsung announced at CES 2018, we are incorporating Samsung KNOX security technologies into Smart TVs and appliances in addition to mobile devices.[5] KNOX, our defense-grade security technology, includes a hardware root of trust and firmware to help ensure devices are protected end-to-end. Originally introduced in 2013 for our mobile phones and tablets, KNOX's fundamental underpinnings remain the same for our connected products of all kinds: securing devices through protections built in at the hardware level.

(2) ARTIK IoT platform. Beyond the security protections of our own IoT products, we have also developed a security solution available to all IoT innovators. Samsung's ARTIK, a hardware-based, open, and secure platform that delivers interoperability between IoT devices and apps, is a leading example of how openness and security can be combined to benefit the IoT ecosystem.[6] ARTIK enables secure device registration based on a hardware root of trust that supports a secure operating environment and securely connects devices to the cloud using TLS and certificates issued by a trusted certificate authority. Every device, app, and user interaction can be secured with open internet standards-based authentication and authorization, and ARTIK protects data with built-in identity and permissions managements. In fact, ARTIK's open technology allows all innovators in the IoT ecosystem to address significant challenges, like security, in a cost-sensitive and effective manner without hindering the deployment of the IoT.

(3) SmartThings Cloud. Finally, Samsung is proactively encouraging third parties to securely connect their devices to the SmartThings Cloud, the single cloud leveraged by both Samsung and third-party IoT products. This includes working to make various products from different manufacturers compatible and secure through promotion and adoption of the Open Connectivity Foundation ("OCF") standards and frameworks. Furthermore, Samsung has developed certain cybersecurity requirements that a third party device must meet before connecting to the Samsung SmartThings cloud. Thus, SmartThings Cloud helps drive the global market for all devices toward security.

Again, we are eager to engage with the Administration and other stakeholders to advance security innovations such as those Samsung is pioneering in the market. While static,

[5] https://news.samsung.com/us/samsung-vision-iot-experiences-ces2018-press-conference/
[6] https://www.artik.io

prescriptive government requirements tend to inhibit innovations as technology evolves over the long term, there is indeed an important role for the government to play in helping to accelerate dynamic market-driven security advances. The Administration should continue to expand the private sector-driven multi-stakeholder processes that the National Telecommunications and Information Administration, the National Institute of Standards and Technology ("NIST"), and the Department of Homeland Security have convened thus far. Samsung looks forward to actively participating in further initiatives convened by these agencies, pursuant to several of the Actions recommended in the Draft Report,[7] which challenge private sector stakeholders to move the market toward security.

Finally, given the substantial resources we are devoting to securing our IoT products and promoting security of the broader IoT marketplace, we agree with the Draft Report Action 2.3, which calls on the federal government to lead by example and create market incentives for IoT product vendors to adopt more secure products. With this in mind, Samsung recommends that the Administration and the Congress support – not conflict with or duplicate – important ongoing processes such as NIST's Cybersecurity for IoT Program's efforts with industry to develop guidance on IoT security for federal agencies. In particular, the final report to the President should recommend that:

- NIST work with industry to develop IoT security guidelines for federal procurement and management, including patchability, known vulnerabilities, hardcoded passwords, standard protocols, and other issues;
- Federal agencies use risk management principles to evaluate their threat posture, priority assets, and key mitigations over device lifecycles;
- Federal agencies implement these guidelines in procuring and managing IoT devices, for instance in contract language and Requests For Proposals; and
- NIST develop a mechanism to refresh the recommendations to keep pace with emerging technologies and security innovation.

We commend the Draft Report for acknowledging that botnets and other automated, distributed attacks are an ecosystem-wide challenge. Given that no single stakeholder community can address botnets in isolation, we look forward to continuing to collaborate with private sector partners, government stakeholders, and consumers on concrete actions to reduce botnet threats. Thank you for the opportunity to offer our views and please do not hesitate to contact the undersigned if you have any questions or need additional information.

[7] These include Action 1.1 regarding baseline security profiles for IoT devices; Action 1.3 regarding development and deployment of innovative technologies to prevent and mitigate distributed threats; Action 1.4 regarding government and industry collaboration to promote best practices; Action 3.2 regarding security for home IoT products; Action 5.1 regarding informational tools for home IoT devices; Action 5.2 regarding informational tools for critical infrastructure IoT applications; and Action 5.5 regarding a public awareness campaign promoting home IoT device security.

Sincerely,

John Godfrey
Senior Vice President, Public Policy
Samsung Electronics America, Inc.
john.godfrey@samsung.com
(202) 887-5667