February 12, 2018

VIA EMAIL: 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

Re: McAfee's comments in response to the Departments of Commerce and Homeland Security on "Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats"

McAfee LLC appreciates the opportunity to respond to the request for comments on the *"Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats"* posted on January 5, 2018. McAfee has been an active participant in related efforts at NSTAC, NTIA and NIST that have contributed to the development of this report to the President. We hope our comments are useful.

McAfee, an independent cybersecurity company, is focused on accelerating ubiquitous protection against security risks for people, businesses and governments worldwide. We are responding today to comment on the proposed report to the President. McAfee is totally committed to improving the global security ecosystem and has been demonstrating that support by working with governments, law enforcement and industry partners to takedown automated attack tools and infrastructure. McAfee has long shared the sentiment with governments worldwide that we cannot delay in collectively addressing the evolving cybersecurity threats facing us all. McAfee continues to lead efforts to improve cybersecurity at home, on the go and in enterprise environments.

Before beginning our comments, we want to express how extremely pleased we are to see the totality and variety of input that has gone into this report. The NSATC, NIST and NTIA efforts, focused on gathering industry thoughts and developing Presidential recommendations, are only going to make this report better. We truly appreciate the fact that government is going to these lengths to assure they are listening to and partnering with industry to address this increasingly serious threat to the digital realm.

Our Comments

As we read the report, it is apparent discussions in the report are not focused on any specific timeframe. Some of the items listed will take ten years or more to put in place. Where does this leave us in that period of transition to a solution? The report does not seem to prioritize the goals and actions and it is apparent some of the items should be started immediately. As you are reviewing the comments from the private sector, it would be beneficial if there were some prioritization indicated in the final report. This will help by focusing the private sector and the federal government on what is needed from each and when.

One of the interesting and unique approaches taken in the NSTAC Report to the President on Internet and Communications Resilience was that they developed and presented recommendations for each part of the described ecosystem. They also targeted areas specifying actions for both government and the private sector. These are the type of directions that are needed for us to move forward. A goal without a plan is simply a wish. While this report has some excellent goals, it is obvious that there is great deal of additional work needed to turn these into actions.

What follows are comments on the various Goals and Actions specified in the report. We did not supply comments to every Action, only those where appropriate.

Goal 1: Identify a clear pathway toward an adaptable, sustainable, and secure technology marketplace

Action 1.1 Establish broadly accepted baseline security profiles for IoT devices in home and industrial applications and promote international adoption through bilateral arrangements and the use of international standards. The federal government should accelerate this process by adopting baseline security profiles for IoT devices in U.S. government environments.

The text describing this Action seems focused on working through standards efforts such as the IETF, JTC1 and other international standards organizations. That is not where the majority of IoT development is occurring today. As shown by the NTIA's multi-stakeholder process on IoT Security Upgradability and Patching, the majority of IoT standards development is happening in consortia, vendor focused consensus efforts and pay-to-play groups. This is a very diverse set of organizations, all wanting to assure their standards take the market place by storm. This is not a conducive environment for developing broadly accepted, baseline security profiles for home-based devices in any reasonable timeframe.

We do however, have an example of a successful public-private partnership where real outcomes occurred that has been rapidly embraced by the private sector and is having a global impact. The focus of the Cybersecurity Framework on reviewing, understanding and improving organizational cybersecurity protection programs was a positive change from where organizational efforts had been in the past. The highly transparent and collaborative process NIST led in developing the Framework has served as a model not only for other

U.S. government agencies but also for governments worldwide looking to address cybersecurity-related issues in a collaborative fashion.

While far from perfect, with absolutely much more work needed, industrial applications have done a better job at incorporating security capabilities than home-related applications and devices. There are security standards for various aspects of industrial IoT devices. There are however, little to nothing addressing the Home environment. We need to prioritize efforts in areas where we can have the most impact relating to protecting against automated attack mechanisms. Consumer devices in the home have shown to be a serious emerging attack vector for launching large scale attacks.

Recommendation: NIST should be directed to convene a public-private effort to develop a home cybersecurity management architecture for consumer devices that addresses assuring devices have the means to be patched using trusted connections from the authorized device manufacturer, while defining mechanisms that would prevent devices from being used for other than their manufacture’s intended purposes.

Action 1.2 Software development tools and processes to significantly reduce the incidence of security vulnerabilities in commercial-off-the-shelf software must be more widely adopted by industry. The federal government should collaborate with industry to encourage further enhancement and application of these practices and to improve marketplace adoption and accountability.

The government has had efforts such as these for years with some success, but not to the level needed to radically change the landscape. It is well known in the security vendor and other mature product development communities what needs to be done and it is being done. Companies have actively incorporated secure development principles and secure coding practices into their software development lifecycles. While not perfect, these companies are working hard to reduce software flaws before the products are shipped.

The problem is many developers have never been taught or have realized that security and privacy engineering principles are critical to a successful, supportable and profitable product line. Sadly, many college and university computer science graduates have never taken a cybersecurity course on secure coding. Many educational institutions don’t even offer such a course, let alone make it a requirement.

It should be noted that the economics of IoT product development can itself be a problem. For example, if you are building a $7 device, are you going to put a $15 security investment into each of those devices? Chances are the answer is no. This type of situation then changes the producer’s support approach to the product. At that price point, the product becomes a throwaway. The manufacture can sell you another newer, updated version, instead of adding the expense of integrating a secure means to update the previous product. This is the reality we are now dealing with. In this case it is not that the staff lacks the understanding of secure coding principles; an organizational decision was made to not worry about it as a part of that product's development and deployment lifecycle. And as we have seen repeatedly, devices and software have a tendency to continue to be used long after they should have been upgraded or replaced.

Recommendation: The National Initiative for Cybersecurity Education (NICE) in conjunction with the Department of Education, should work with states to assure all accredited computer science and engineering related degree programs require courses in cybersecurity, secure software development and secure coding as a requirement for successfully completing the degree program. They should also work with community colleges to encourage incorporating cybersecurity and secure coding classes into their software development curriculum.

Goal 2: Promote innovation in the infrastructure for dynamic adaptation to evolving threats

Action 2.1 Internet service providers and their peering partners should expand current information sharing to achieve more timely and effective sharing of actionable threat information both domestically and globally.

This Action appears short sighted as it gives the impression ISPs have all the critical information to share. The security vendor community seems to have been completely left out of this holistic view of the ecosystem. Today there are innovative information sharing organizations turning cyber threat data into active and actionable intelligence. Organizations such as the Cyber Threat Alliance, comprised of cybersecurity product vendors, are sharing threat information so its members can rapidly deploy actionable intelligence and threat mitigations to their customers in near-real time.

Recommendation: This section needs to be expanded to include a wider set of those communities and organizations that are actively capturing, analyzing and enriching cyber threat intelligence daily.

Action 2.2 Stakeholders and subject matter experts, in consultation with NIST, should lead the development of a CSF Profile for Enterprise DDoS Prevention and Mitigation.

McAfee applauds the intent of this action. Much of this work, however, has already been created by the Coalition of Cybersecurity Policy and Law. McAfee is a member of the Coalition. The Coalition has developed the "*Cybersecurity Framework DDoS and Botnet Prevention and Mitigation Profile*". The profile is being contributed as a part of the Coalition's response to this report.

Recommendation: We support Coalition’s profile development effort and believe NIST should use this as the basis for a focused public development of such a profile and in the end, assure it is properly incorporated into a near-term version of the Framework.

Action 2.3 The federal government should lead by example and demonstrate practicality of technologies, creating market incentives for early adopters.

Recommendation: The federal government should actively use the power of the purse to incentivize the market. IoT goods and services should meet certain required security capabilities in order to be purchased. This includes both the industrial and the home aspects. For example, nothing would be purchased for military housing without meeting the home cybersecurity management architecture and associated device security capabilities.

Action 2.4 Industry and government should collaborate with the full range of stakeholders to continue to enhance and standardize information-sharing protocols.

While a laudable goal, automated processing and response as described will require a great deal more than simply updating sharing protocols such as STIX and TAXII. It will require real trust. Today STIX and TAXII are industry recognized standards for information sharing and are in active development in the OASIS standards development organization’s Cyber Threat Intelligence TC. If the intent of this Action was to provide a means to allow external information, crossing organizational boundaries to drive automated responses inside the receiving organization, we need to create the means to trust that information. We are already seeing organizations reluctant to join the DHS Automated Indicator Sharing program and that is a simple exchange of threat indicators and defensive mechanisms. Without a means to trust both the actions the exchanged data is requesting and the organization sending that data, it is unlikely automated responses will be allowed to occur by the receiving organization. This is not a technical problem but a cultural one. While enhancing standardized information sharing protocols, for this to be effective we will also have to develop the capability to convey trust in a secure and meaningful way. But before that is deployable, trust must be established between the sharing parties.

Goal 3: Promote innovation at the edge of the network to prevent, detect, and mitigate bad behavior

Action 3.1 The networking industry should expand current product development and standardization efforts for effective and secure traffic

management in home and enterprise environments.

Action 3.1's description seems to be looking to create new solutions and standards, while using new technologies to solve problems in both the home and enterprise. But are we overlooking capabilities we already have? IPV6 is just now reached 10% deployment, 20 years after it was first deployed. IPV6 can run end-to-end encryption thus making 3rd party man-in-the-middle attacks a great deal more difficult. Currently when malicious activity is occurring from within a standard home environment, network service providers can only see it is coming from the home network. They cannot determine which device is causing the problem within the home networks. With IPV6, each individual device in the home could be identified so network service providers could identify the offending device, take appropriate actions and potentially notify the home owner as to what recommended actions they should take. There are other security related advantages to IPV6. For example, for network infrastructure components such as DNS can be better secured with IPV6 rendering name-based attacks, such as Address Resolution Protocol poisoning much more difficult.

Recommendation: Create a national plan, working with network service providers, network application vendors, security vendors, government and other appropriate communities to develop a means to rapidly accelerate IPV6 deployment, while establishing a hard date to discontinue IPV4 usage.

Goal 4: Build coalitions between the security, infrastructure, and operational technology communities domestically and around the world

Action 4.2 The federal government should promote international adoption of best practices and relevant tools through bilateral and multilateral international engagement efforts.

The description of this action correctly identifies a problem that exists in standards development. Unlike some countries, the United States does not coordinate strategy well when participating in international standards bodies. Additionally, the United States participation in international standards development has been seemingly waning while China has seen a sharp increase in their participation. Without more coordination and active participation, the US may find ourselves following rather than leading.

Goal 5: Increase awareness and education across the ecosystem

Action 5.1 The private sector should establish and administer voluntary informational tools for home IoT devices, supported by a scalable and cost-effective assessment process, that consumers will intuitively trust and understand.

Labeling schemes need to be designed to convey the appropriate capabilities instead of a point in time evaluation by a third-party testing / assessment lab. Products need to list the security capabilities they provide, remote upgradability, vulnerability patching, secure communications, the types of privacy related-information captured, geo-location, health data, etc. Trying to make an attestation that this device is secure will fail because invariably vulnerabilities will be discovered, and the product is then no longer secure. Focusing on the capabilities built into the product shows that security and protection of the consumer’s privacy is important to the manufacturer.

Recommendation: Any labeling scheme developed, whether it is for consumer use or for use in critical infrastructure, should target the security capabilities built in to support secure use and support the overall secure lifecycle of the product.

Action 5.5 The federal government should establish a public awareness campaign to support recognition and adoption of the home IoT device security profile and branding.

This is not a new idea. It has been discussed as a part of the President’s Commission on Enhancing National Cybersecurity. The problem to date is, efforts such as ‘Stop.Think.Connect’ are not leveraging PSAs. At least outside the DC area, the program is not resonating with those that need it the most. “Only you can prevent forest fires.” “This is your brain, this is your brain on drugs“. The messages of ‘Stop.Think.Connect’ need to be broadcast widely. They are not getting out to the masses. Just having a website with lots of great resources is not enough. Targeting a small section of the population is also not enough.

Any sort of public awareness campaign should not be limited to just IOT devices. It needs to be addressing cybersecurity and its value in general. If the goal is to influence consumers to see the value of cybersecurity, you must first explain why it is important to them. You need to address the basics before you can influence their purchasing decisions. Technology has advanced so much in the past 20 years and most people have just not been able to keep up. That lack of basic knowledge needs to be addressed in a manner the public will see and be able to benefit from.

Summary

There are items that need to be addressed which this report did not. Dealing with devices and attacks beyond our borders; orphaned devices; products whose maintainers have stopped supporting that version, but the product is still in wide use in various sectors of our economy, for example. The NSTAC report called for a Cybersecurity Moonshot study to provide private industry advice on how the government could most effectively coordinate a national effort for securing the digital foundation for our lives. Nearly everything addressed in this report fits into a concept such as the proposed Cybersecurity Moonshot. It is obvious that we as a nation need to find the will and resources to address this core threat to our digital economy.

Thank you again for allowing us the opportunity to provide comments on the Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats. We are happy to see the breadth of input this effort has incorporated into this report. We are pleased to have been an active part of the multiple areas discussed and described in the report, from the NIST Botnet Workshop, the NTIA's multi-stakeholder process on IoT Security Upgradability and Patching, to the NSTAC report to the President on Internet and Communications Resilience. McAfee is proud to have been a part of these efforts and looks forward to partnering with the federal government and global community to continue working to secure our digital economy.