607 14th St. NW, Suite 660
Washington, DC 20005

February 12, 2018

VIA EMAIL: *counter_botnet@list.commerce.gov*

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, N.W., Room 4725

Attn:
Evelyn L. Remaley
Deputy Associate Administrator
Washington, D.C. 20230

Re: CA Technologies Comments on Draft Report to the President on Promoting Stakeholder Action Against Botnets and Other Automated Threats

CA Technologies appreciates the opportunity to provide comments on the Draft Report to the President on Enhancing the Resilience of the Internet and Communications Technology (ICT) Ecosystem Against Botnets and Other Automated, Distributed Threats (Report). Since our founding in 1976, CA Technologies has continued to serve as a global leader in software solutions enabling customers to plan, develop, manage and secure applications and enterprise IT environments across distributed, cloud, mobile and mainframe platforms. A majority of the Global Fortune 500, as well as many government agencies around the world, rely on CA to help manage their increasingly dynamic and complex IT infrastructures.

CA Technologies welcomes the draft Report, as it lays out key themes, goals, and action items for addressing the distinct business, security and privacy challenges facing governments, enterprises, organizations and consumers associated with botnets and other automated threats.

CA is focusing its response on specific Action items outlined in several of the Report's goals, with a particular focus on federal efforts to promote secure software development practices, and efforts to promote IoT device authentication and the use of secure gateways.

Secure Software Development Processes and Practices

CA Technologies applauds the draft Report for recommending the promotion of secure development processes and practices to minimize vulnerabilities in the software code that underpins devices, networks and applications.

The Report properly recognizes the challenge that insecure software poses to the ICT ecosystem. Under the Technical Domains subsection, the Report cites studies, which find that common software development techniques result in, optimistically, a flaw for every 2,000 lines of code. CA Veracode's *2017 State of Software Security* report also highlights the pervasive risk of software security. For example, the widespread use of software components in application development means a vulnerability in a single component can reach thousands of applications – so a hacker must only create one virus or program to breach thousands of applications and potentially millions of companies. Examination by CA Veracode demonstrated that 77 percent of applications had at least one vulnerability on initial scan.[1]

CA strongly supports 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 Action correctly notes that it is possible to develop code with very small numbers of errors, where the importance of the mission merits the reduction in productivity. However, CA believes that secure software development tools and practices have developed sufficiently such that minimizing errors in code need not impede productivity in a significant way. Rather, if secure development tools, practices and processes are embedded in an agile code development process, organizations can develop more quality code while maintaining strong productivity and efficiency. As an example, the CA Veracode Greenlight solution gives customers the ability to scan code within an integrated development environment, providing instant insights to developers on line of code where a flaw is located, the type of flaw, severity of the flaw, and the associated common weakness enumeration.

CA Technologies agrees that the federal government should support industry adoption of secure development tools through efforts that improve return on investment or create market incentives for lagging sectors or industry groups. We also agree that the federal government should work with industry to develop strategies that make it easier and cheaper to adopt secure development approaches.

CA Veracode's experience with thousands of customers over the past 12 years has allowed us to identify best practices within high-performing application testing programs. The government should continue to encourage adoption of best practices through standards such as the NIST Framework for Improving Critical Infrastructure Cybersecurity (CSF), Payment Card Industry Data Security Standard (PCI DSS), HIPAA, and other regulatory and voluntary frameworks.

CA Technologies also agrees that many of the software components, libraries, and modules used in modern products may be outdated or vulnerable. Therefore, we support the Report's recommendation for the NTIA to engage with diverse stakeholders in examining the role of transparency tools and practices in improving manufacturers and purchasers understanding of what goes into IoT products. However, we believe it is critical that NTIA engage a broad range of stakeholders through this process to ensure that any outcomes reflect consensus best practices. We also believe it is important that

[1] https://www.veracode.com/sites/default/files/pdf/resources/ipapers/soss-2017/index.html

stakeholders both understand and express the notion that software security is a holistic process, and that software component transparency represents a single, but very important facet of this process. Ultimately, organizations should continue to prioritize the dedication of resources and budget towards the activities and tools that provide the strongest overall outcomes.

CA Technologies supports 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*.

CA Technologies is a member of the Coalition for Cybersecurity Policy and Law. The Coalition has developed a CSF profile for DDoS prevention and mitigation and is updating this profile to align with the goals of the Report. This profile will provide strong value to organizations looking to utilize the CSF to address the challenge of botnets.

A key component of this profile is scanning for vulnerabilities, which is also included as a subcategory of the CSF Core[2]. The CSF also included new language in Section 3 of Draft 2, Version 1.1 on utilizing the CSF in the life cycle phases of design, build/buy, deploy, operate and decommission. CA believes the CSF should continue to evolve to examine secure software development practices, especially as all industry segments are increasingly building/leveraging software applications.

CA Technologies recommends that NIST add secure development processes and practices to the CSF Roadmap of key issues that merit increased attention in the future. These practices include a mix of developer education, threat modeling, architectural risk assessment, code scanning and analysis, penetration testing, and continuous tracking of known vulnerabilities and attack vectors.

CA also recommends that NIST, working through the National Cybersecurity Center of Excellence (NCCoE), launch a work stream to engage with industry stakeholders, and leading software assurance organizations, such as the Software Assurance Forum for Excellence in Code (SAFECode[3]), to develop risk-based, scalable guidance on effective secure software development processes and practices. CA Technologies is a charter member of SAFECode and would be greatly interested in participating in this proposed work stream.

CA Veracode's analysis of millions of application scans, covering 6 trillion lines of code, has helped us identify four major principles that are common in application security testing programs that see significant results in reducing the prevalence of software vulnerabilities and lowering application risk:

1. **Test throughout the software development lifecycle with multiple technologies.** Different kinds of application security testing — static, dynamic, and manual penetration testing — find different types of vulnerabilities. The most effective and mature Application Security (AppSec) programs use all three kinds of testing to find and fix vulnerabilities during development and once an application is live in production. Not all vulnerabilities are created equal, so effective programs also need to complement testing technologies with policies that describe what types of vulnerabilities make an application "fail" and require fixing.
2. **Start small and build the program over time to secure the entire application landscape.** Organizations just starting out with security testing shouldn't try to fix every vulnerability in every application. Security teams need to triage the most critical applications and fix the most

[2] NIST Cybersecurity Framework Core: DE.CM-8
[3] https://safecode.org

severe vulnerabilities first. As an AppSec program scales up into a more mature program, organizations will assess all of their software, not only applications developed internally, but also those purchased from third parties and those assembled with open source components.

3. **Use metrics to improve performance over time.**
   Advanced AppSec programs measure results through a set of metrics and key performance indicators (KPIs), such as compliance with policy (internal policy, OWASP policy, and industry regulations). Metrics allow organizations to quantify their risk. Metrics also enable AppSec managers to communicate areas for improvement to the security and development teams.
4. **Train developers to code securely and enable them with the right tools.**
   As DevOps practices (combining the disciplines of development and operations in an agile development environment) continue to take hold in IT departments today, security teams are increasingly filling the role of expert consultants and partners, rather than testers and compliance babysitters. This means developers are shouldering more responsibilities both during security testing and remediation. We call this practice DevSecOps. CA Veracode data shows that supporting developers with resources such as eLearning and remediation coaching by security experts can have a tremendous impact on the efficacy of developer teams in fixing security bugs.

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

CA agrees that the federal government can lead by example and establish market incentives by evaluating and implementing effective ways to mandate the use of software development tools and processes that significantly reduce the incidence of security vulnerabilities in all federal software procurements, such as through certification requirements.

CA Technologies welcomes the new initiative in the DHS Continuous Diagnostics and Mitigation program, which inquires whether suppliers use a secure software development life cycle process in the development of their solutions.

CA also believes that certification programs can play an important role in strengthening the cybersecurity landscape, if developed effectively. They can set minimum security standards for suppliers and increase market confidence for customers, including both enterprises and consumers. However, in order for a software certification process to be successful, it must take into account modern development practices.

First, the certification scheme should focus on development processes, rather than on end products. A lengthy, resource-intensive certification regime focused on testing products after their development may take months or years to complete. With modern agile development methods and cloud delivery, software products are continuously updated. Software development organizations that prioritize security integrate security into their development process, as described above. A certification regime that confirms the application of secure development processes in the delivery of code will enable continued innovation while also producing more secure software. The risk profile of the application being developed can dictate the level of security rigor that the development process requires.

Second, the federal government should promote international alignment of government certification regimes, ideally based on international, consensus driven standards. This is particularly important as

many national and regional governments are implementing or considering certification regimes for ICT products and services. The ISO 27034 standard, currently under development, can provide a foundation for certification against secure development processes. As stated above, while ISO focuses on more mature development organizations, CA believes the NCCoE could engage stakeholders to develop best practice guidelines for organizations with less mature development processes.

Third, the federal government should leverage the burgeoning private sector certification ecosystem in software assurance. The CA Veracode Verafied service certifies that customers are: assessing their code with static analysis testing; remediating high severity flaws; educating developers on secure coding; avoiding using known vulnerable open source components; and integrating testing for continuous scanning in the SDL. This certification service is continuing to evolve, reflecting industry trends towards continuous delivery and DevOps practices.

Finally, it is important to remember that certification represents a point in time measurement and should not be misunderstood as guaranteeing complete security indefinitely, as attacks continue to evolve and new vulnerabilities are discovered.

CA Technologies supports Action item 5.3: *Government should encourage the academic and training sectors to fully integrate secure coding practices into computer science and related programs*.

Integrating secure software development practices in engineering and computer science education represents a more foundational approach to strengthening software security, which can significantly improve security outcomes over the long term.

The vast majority of software developers enter the workplace without formal software security training. Developers need better training in cybersecurity principles and secure coding. Because security training is not a part of most computer science courses, we could see great improvements in the security skills of developers, simply by encouraging and incentivizing more schools and universities to teach secure development practices as part of their computer science curricula.

We agree that the National Initiative for Cybersecurity Education should engage with academia and the private sector to incorporate security-by-design principles and supporting tools at every step in the course of study.

Device Authentication and Application Security

CA Technologies supports 3.1: *The networking industry should expand current product development and standardization efforts for effective and secure traffic management in home and enterprise environments*.

As the Internet of Things continues to expand at an exponential pace, securely authenticating the people, devices, applications and data involved in the IoT ecosystem will be critical to ensuring trust. Application Programming Interfaces (APIs) manage the connections between applications, data and devices. Broadly speaking, APIs make it possible for organizations to open their backend data and functionality for reuse in new application services. Organizations and governments that leverage open APIs can realize significant data-driven value creation. However, these APIs also represent significant attack vectors for malicious actors. Therefore, API management and security are key components of IoT and application security.

This need for strong security can conflict with a basic goal of API design—a well-designed API makes it easy for developers to create apps that provide seamless access to enterprise resources. Strong security is likely to impact this ease of access. Deploying security in a centralized API architecture (rather than in the API implementation) through an API Gateway will help mitigate this impact, as will enabling the use of flexible access management technologies like OAuth[4] and OpenID Connect.[5] And more broadly, throughout the process of designing, deploying and managing an interface, program managers and API architects must closely communicate and collaborate to ensure they agree on their core strategic goals, what they will do to achieve these goals and how they will evaluate the outcomes of their efforts.

Automated client registration and secure channel creation requires no specific implementation of security protocols by the app developer but results in an end-to-end protocol and data-level security posture. API management solutions can be configured to provide end-to-end security between the client and secure data (including dynamic secure data storage on mobile clients), as well as protecting against many web-based threats and OWASP vulnerabilities.

Strong authorization control is essential for protecting APIs against attack and misuse. OAuth has emerged as the leading authorization technology for API security. One of the great benefits of OAuth (especially OAuth 2.0) is its flexibility. A user can leverage OAuth to create a solution tailored to her specific needs and requirements.

However, it is important to remember that OAuth is not inherently secure or insecure, and that OAuth-based authorization will only be one element of a complete API security solution.

An OAuth authorization server should be integrated with strong, multi-factor authentication, wherever this is applicable. Ideally, a user's API Gateway should have templates that will simplify the process of designing token governance policies and OAuth patterns appropriate to the use case. The Gateway technology should also include a runtime policy enforcement layer that will make it easier to enforce and manage the policies and patterns for multiple APIs.

Conclusion

CA Technologies welcomes the opportunity to partner with the federal government, industry, and other stakeholders in addressing the significant challenges posed by botnets and other automated, distributed threats. CA appreciates the Report's strong focus on secure software development practices, processes and tools in its goals and action items. Further, CA supports efforts to enhance security in the interfaces between devices, applications, and back-end databases. We recognize that this initiative will require significant effort and resources from the full range of stakeholders, and we look forward to contributing on the implementation of the Report's recommendations.

[4] https://oauth.net/
[5] http://openid.net/connect/