From: **Michael Nelson**
Date: Mon, Apr 10, 2017 at 5:07 PM
Subject: Cloudflare comments on Draft 1.1
To: cyberframework@nist.gov
Cc: Adam Sedgewick, NIST

Comments on the January 10, 2017, version of Draft 1.1 of the NIST "Framework for Improving Critical Infrastructure Cybersecurity"

The NIST Cybersecurity Framework has been an invaluable guide for thousands of organizations trying to reduce their exposure to cyberthreats. The ongoing revision process will make the Framework even more useful as new threats arise. Cloudflare welcomes this opportunity to provide input on how the 2014 version of the Framework can be improved.

In particular, we welcome the new language in Draft 1.1 that highlights the need to consider all three parts of the CIA (Confidentiality, Integrity and Availability) triad. Until last year, almost all media reporting on cybersecurity focused on the theft of data. The original Framework did not devote enough attention to challenges in ensuring the integrity and availability of data and systems. Thus, we believe that the new language on CIA under the section on "Measuring and Demonstrating Cybersecurity" is helpful.

The original version of the Framework also put much more focus on data at rest than on the security of networks. Since it was published, there has been an explosive growth of Distributed Denial of Service (DDoS) attacks by malicious hackers, organized crime groups, and some governments, who use them to disrupt and extort businesses and organizations. The massive Mirai botnet attacks in October 2016 showed how Internet of Things devices could be leveraged for DDoS attacks, some of which were able to bring down key parts of the Domain Name System ecosystem.

Yet, the latest draft of the Cybersecurity Framework does not explicitly mention either DDoS attacks or the Internet of Things. We recommend adding text describing the new network-based threats (and how the IoT complicates the picture) within the main text of Draft 1.1. It is also essential that new entries be added to Table 3 ("Framework Core") that would help users of the Framework address DDoS attacks. The current draft mentions the need for more system capacity to deal with attacks but does not dwell on the tools and services that can detect and deflect DDoS attacks. It is important to realize that often the best and most cost-effective solutions will be third-party, cloud-based services rather than hardware and software installed on-premise.

Please let us know if you have any questions about our comments. We look forward to participating in the May, 2017, workshop at NIST and to continuing to support the NIST Cybersecurity Framework process.

Michael R. Nelson
Public Policy
Cloudflare
Washington, DC