Statement on Third-Party Internet Reputation and Hygiene Reporting Providers

To whom it may concern,

McAfee has been a pioneer and leader in protecting consumers, enterprises, and governments from cyberattacks for more than 30 years with integrated security, privacy, and trust solutions. We built our platform through a deep, rich history of innovation and have established a leading global brand. Whether we are securing the digital experience of a consumer who is increasingly living life online or defending many of the world’s largest enterprises and governments from sophisticated attacks and nation-state threats, McAfee is singularly committed to one mission: to protect all things that matter through leading-edge cybersecurity.

McAfee’s Internet footprint reflects the breadth of security services we provide to customers. In some cases, the types of activities we undertake affect the ratings generated by third-party Internet reputation and hygiene reporting providers. Some of these activities and their effect on third-party Internet reputation and hygiene reporting providers are common to software companies, while others are unique to McAfee. A selection of such activities are described below:

Internet reputation and hygiene reporting related to malware and spam:

- Internet reputation and hygiene providers use public and private data sources to determine whether an Internet Address is likely to exhibit malicious behavior or be infected with malware. McAfee provides Web Gateway services to our customers using on-premise and public cloud-based web proxies. Traffic entering the Internet from these systems is traffic that originates with service customers. This traffic does not originate with McAfee and does not reflect any potential or actual malware issue affecting McAfee’s systems.

- As part of our analysis of malware samples identified by our tools and/or submitted to us by our customers, McAfee performs disassembly and controlled detonation of malware. To the extent detonated malware connects to the Internet via one of our public Internet gateways, such detonation may be detectable by public information services that gather data from DNS sink-holing and similar methods. Public information services that use data derived from such malware detonations to compose an Internet hygiene score are not accurately attributing their data to their cause, which in this case is controlled malware detonations that have the side effect of generating Internet traffic.

- We employ malware researchers and threat researchers whose activities may affect the scores of third-party Internet reputation and hygiene reporting services.

- We may or may not employ deceptive technologies as part of our business. If we deploy deceptive technologies within IP address space registered to us, such technologies are likely to contribute to lower scores by third-party Internet reputation and hygiene reporting companies.
Internet reputation and hygiene reporting related to SSL protocol version support and related issues:

- Our Enterprise business develops and supports products for enterprises worldwide. Some of our customers use versions of our products that were created prior to the most recent rounds of standards and algorithms for transport encryption and transport layer security. As a result, systems in our IP address space providing support for such product versions must use older versions of transport security standards, protocols, and algorithms. The following link contains details on our Enterprise products end-of-life policy: [https://www.mcafee.com/enterprise/en-us/assets/misc/support-policy-product-support-eol.pdf](https://www.mcafee.com/enterprise/en-us/assets/misc/support-policy-product-support-eol.pdf)

- Similarly, our Consumer business supports a wide range of desktop operating systems, some of which are only compatible with older versions of transport encryption and transport layer security. As a result, systems in our IP address space providing support for such product versions must use older versions of transport security standards, protocols, and algorithms.

- The need to support legacy transport layer security protocols and algorithms may constrain the versions of other supporting software, including web server versions.