Kaspersky Lab response clarifying the inaccurate statements published in a Bloomberg Businessweek article on July 11, 2017:

“Regardless of how the facts are misconstrued to fit in with a hypothetical, false theory, Kaspersky Lab, and its executives, do not have inappropriate ties with any government. The company does regularly work with governments and law enforcement agencies around the world with the sole purpose of fighting cybercrime.

“In the internal communications referenced within the recent article, the facts are once again either being misinterpreted or manipulated to fit the agenda of certain individuals desperately wanting there to be inappropriate ties between the company, its CEO and the Russian government, but no matter what communication they claim to have, the facts clearly remain there is no evidence because no such inappropriate ties exist.”

Below, the false allegations and inaccurate representations included in the article are addressed, point by point:

1. “The huge reach of Kaspersky’s technology is partly the result of licensing agreements that allow customers to quietly embed the software in everything from firewalls to sensitive telecommunications equipment—none of which carry the Kaspersky name.”

Kaspersky Lab has technology licensing agreements with more than 120 technology providers. The licensing agreements permit these partners to embed Kaspersky Lab’s unparalleled anti-malware engine into their own solutions, and once Kaspersky Lab products are included, these vendors are responsible for publicly communicating all the external products used in their comprehensive offering. It is also important to note that less than four percent of the company’s revenue comes from licensing deals.

Examples of our partners providing the full information about security solutions they are using in their offerings are included in their technical documents and/or on their websites: examples -ZyXEL and Juniper Networks.

2. “While the U.S. government hasn’t disclosed any evidence of the ties, internal company emails obtained by Bloomberg Businessweek show that Kaspersky Lab has maintained a much closer working relationship with Russia’s main intelligence agency, the FSB, than it has publicly admitted.”

Actually, the reported emails show no such link, as the communication was misinterpreted or manipulated to try to make the media outlet's narrative work. Kaspersky Lab is very public about the fact that it assists law enforcement agencies around the world with fighting cyberthreats, including those in Russia, by providing cybersecurity expertise on malware and cyberattacks.

Kaspersky Lab regularly cooperates with law enforcement agencies, industry peers and victims of cybercrime. For example, in the past, we have assisted law enforcement efforts to arrest the Lurk gang, which stole $45 million from banks and other financial institutions. Similarly, Kaspersky Lab assisted the Dutch police in identifying and catching the authors of the CoinVault ransomware. The majority of the CoinVault victims have been registered in the Netherlands, Germany, U.S., France and the UK. The company's goal is very simple - protect users from cyberthreats and make the internet safer for everyone.

Other examples of Kaspersky Lab cooperation with international law enforcement agencies are:

- Simda botnet disruption: https://www.interpol.int/News-and-media/News/2015/N2015-038
- Shylock financial botnet disruption: https://www.europol.europa.eu/newsroom/news/europol-and-kaspersky-lab-expand-cooperation-in-combating-cybercrime

3. "It has developed security technology at the spy agency's behest and worked on joint projects the CEO knew would be embarrassing if made public."

It's important to be clear, the company never received a request from the Russian government, or any affiliated organization, to create or participate in ANY secret projects, including one for anti-DDoS protection. In the mid-to-late 2000s, Kaspersky Lab was already working to put together an anti-DDoS offering as well as asking customers, prospects and channel partners about this type of solution, and the Russian anti-cybercrime unit told the company that they considered DDoS attacks an emerging and serious threat. Since there was a strong market need, Kaspersky Lab invested in the R&D required to finish fully developing the solution, which is what Eugene Kaspersky indicated in the internal communications referenced by the publication. To clarify, the FSB is not currently, and never was, a Kaspersky Lab DDoS Protection client. Also, while developing the anti-DDoS product, Eugene Kaspersky made it clear in his internal communications that he did not want any possible leaks, as attackers could learn how to bypass the technology measures if public, and he didn't want competitors to copy it before it could be launched.

4. "The software also regularly communicates with the maker to receive updates, which security experts say could theoretically provide access to sensitive users such as government agencies, banks, and internet companies."

Kaspersky Lab was one of the first companies in the industry to introduce hourly updates to provide the most recent detection for threats against our users. The product updates are thoroughly verified and designed exclusively to improve the detection of malware, and all the

updates are encrypted and digitally signed, making them very hard to forge and almost impossible to alter by any third party. Kaspersky Lab does not provide access to these updates to any third party outside of the company, and Kaspersky Lab would never assist any entity in its efforts to spy on users. With a 20-year history in the IT security business as one of the most trusted security providers, the company's reputation speaks for itself.

5. "Kaspersky Lab confirmed the emails are authentic."

Kaspersky Lab never confirmed the emails the media outlet claims to have are authentic, as the media outlet refused to share them with the company for validation to protect an anonymous source; however, the archives were thoroughly searched for any document they might be referring to, and an internal email that contains routine business chatter regarding product development may be the document the publication is referencing.

6. "Kaspersky Lab would also cooperate with internet hosting companies to locate bad actors and block their attacks."

Kaspersky Lab does not cooperate with hosting companies to locate bad actors, and cooperation with hosting providers in an anti-DDoS context means working with a hosting provider to block an attack on their level, before malicious traffic reaches the attacked web resource. This happens when the company experts understand that potential sources of the attack are located in particular data centers.

7. "Active countermeasures" is a term of art among security professionals, often referring to hacking the hackers, or shutting down their computers with malware or other tricks."

The article inaccurately attributes the countermeasures referenced to be for the government, when the information being discussed was actually referencing the types of active measures needed for strong DDoS-protection for customers, such as the DDoS intelligence system, which alerts that there is an emerging DDoS-attack against a customer through monitoring the activity of DDoS botnets.

Hacking back is illegal, and Kaspersky Lab has never been involved in such activities; and instead we are actively participating in joint shut-down of botnets led by law enforcements of several countries where the company provides technical knowledge (for example:https://www.interpol.int/News-and-media/News/2015/N2015-038).

8. "The second part is more unusual: Kaspersky provides the FSB with real-time intelligence on the hackers' location and sends experts to accompany the FSB and Russian police when they conduct raids."

Kaspersky Lab assists law enforcement agencies around the world with fighting cyberthreats, including those in Russia, by providing cybersecurity expertise on malware and cyberattacks. When assisting in official Russian cybercrime investigations, in accordance with Russian law, we only provide technical expertise throughout the investigation to help them catch cybercriminals. Concerning raids and physically catching cybercriminals, Kaspersky Lab might ride along to examine any digital evidence found, but that is the extent of our participation, as we do not track hackers' locations. Kaspersky Lab doesn't provide any government agencies, nor other parties, with information on location of people and doesn't gather "identifying data from customers' computers" because it is technically impossible.

9. The project lead was Kaspersky Lab's chief legal officer, Igor Chekunov, a former policeman and KGB officer.

Reporting it this way is misleading, as Mr. Chekunov worked for the Border Service in the Soviet Union - serving obligatory military service for two years. At that time, the Border Service was a part of KGB structure. For example, in the U.S., this would be the same as working for customs and border protection (CBP), which is under the Department of Homeland Security (DHS). In addition, Mr. Chekunov did not lead the product development for the company's anti-DDoS solution.

-- Attributable to Kaspersky Lab