U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

July 10, 2020

The Honorable Stephen F. Lynch
Chairman
Subcommittee on National Security
Committee on Oversight and Reform
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairman Lynch:

On behalf of the Federal Bureau of Investigation (FBI), this responds to your letter, dated February 26, 2020, to the FBI and the Office of the Director of National Intelligence (ODNI) regarding potential foreign interference in mobile applications and protection of personal data. This letter supplements the ODNI's comprehensive response submitted to the Subcommittee on May 18, 2020.

Pursuant to Executive Order 13636 §4, the Intelligence Community (IC) "ensures the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity" and the Attorney General and Secretary of Homeland Security thereafter ensure such targeted entities are notified so they can take corrective action. If the IC were to identify a compromised mobile application or digital marketplace, the FBI and the Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, would take steps to notify the affected entity so that it can protect itself and its customers. Affected companies will typically secure their customers by regularly releasing software security updates and disclosing security incidents, when warranted.

Engaging the private sector through enduring partnerships is a key component of the FBI's mission. The FBI routinely shares information with industry across all sectors by disseminating threat notifications, hosting unclassified and classified briefings, and presenting at conferences and workshops. The FBI also maintains direct liaison with companies through its 56 Field Offices and its cyber task forces.

The FBI uses Private Industry Notifications (PIN), FBI Liaison Alert System (FLASH) reports, and Public Service Announcements (PSAs) to communicate more broadly with the public and private sector regarding cyber threats. These reports are coordinated with interagency partners and provide actionable information that can be ingested into private industry systems. Nearly 250 of these communications have been disseminated since 2013.

Finally, the FBI encourages consumers to make themselves aware of potential risks and vulnerabilities that mobile applications and social media mechanisms can pose, including risks to exposing sensitive or personal information. Users should be vigilant with their personal information. It is important to note that if users voluntarily provide information to a mobile application that is based in a foreign country or that stores information in a foreign country, the information is subject to the respective foreign country's laws, which may allow its acquisition by that country's government. This would not constitute a "compromise" per se as a company is expected to comply with host country legal process.

Thank you for your support of the FBI, its mission, and its people.

Sincerely,

Jill C. Tyson
Assistant Director
Office of Congressional Affairs

cc: The Honorable Jody B. Hice, Ranking Member
Subcommittee on National Security

The Honorable Adam Schiff, Chairman
Permanent Select Committee on Intelligence

The Honorable Devin Nunes, Ranking Member
Permanent Select Committee on Intelligence

The Honorable John Ratcliffe, Director
Office of the Director of National Intelligence