[redacted]

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
DIRECTOR OF THE NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER
WASHINGTON, DC 20511

Counterintelligence Risk Assessment – WeChat

[redacted] WeChat, a social media company owned by Chinese parent company, Tencent Holdings Ltd., operates a mobile app also called WeChat. [redacted]

(U) WeChat was initially launched in 2011 as a messaging application. Over time WeChat has evolved into an ecosystem of apps that include sharing images and videos, making payments and transferring money, ride hailing, using geolocation data to find friends, playing games, and delivering advertisements to targeted users or broadcasting to the entire user base, among other mini-applications.

(U) In 2018 the National Counterintelligence and Security Center published the *Foreign Economic Espionage in Cyberspace*, stating that "Foreign intelligence services—and threat actors working on their behalf—continue to represent the most persistent and pervasive cyber intelligence threat. China, Russia, and Iran stand out as three of the most capable and active cyber actors tied to economic espionage and the potential theft of U.S. trade secrets and proprietary information."[1] The year 2017 was called out as a representing "a watershed in the reporting of software supply chain operations."[2] Furthermore, in "Breaking Trust: Shades of Crisis Across an Insecure Software Supply Chain" the Atlantic Council observed, after

[1] (U) *See Foreign Economic Espionage in Cyberspace*, page 5. National Counterintelligence and Security Center (2018).
[2] (U) *See* Id. page 12.

*(U[redacted]) **NOTE**: This CI assessment was prepared under the auspices of the National Counterintelligence and Security Center, Supply Chain and Cyber Directorate. It was coordinated with CI and Cyber officials at CIA, FBI, and NSA. The information is provided for intelligence purposes only. No information contained in this assessment, nor any information derived therefrom, may be used in any proceeding (whether criminal or civil), to include any trial, hearing, or other proceeding before any court, department, agency, regulatory body, or other authority of the United States without the advance approval of the agency or department that originated the information contained herein. Any reproduction, dissemination, or communication (including, but not limited to, oral briefings) of this information must be accompanied by a statement of these restrictions. Questions about this assessment or requests for copies can be directed to the Assistant Director for Supply Chain and Cyber Directorate on secure [redacted] or unsecure [redacted].*

[redacted]

[redacted]

[redacted]

National Intelligence Council (NIC) Threat Assessment:

[redacted]

reviewing a decade of supply chain attacks, that, "Software supply chain attacks are popular, they are impactful, and are used to great effect by states, especially China and Russia."[3]

(U) Chinese Intelligence and Security Services (PRCISS) have already demonstrated a willingness to use the supply chain as a platform for malicious cyber operations. As an example, in December 2018 the Department of Justice announced that two Chinese hackers associated with the Ministry of State Security had been indicted for illegal computer intrusions into Managed Service Providers (MSP), targeting more than 45 U.S. technology companies and U.S. Government agencies.[4]

(U) The legitimate functionality within the WeChat ecosystem presents inherent vulnerabilities. For example, mobile devices store and share device geolocation data by design and many apps—including WeChat—request permission for location and other resources that are not needed for the function of the app. Additionally, WeChat only uses client-to-server encryption, vice end-to-end encryption, which allows the service provider, Tencent, to sit between the sender and the receiver and have full access to message content and related data. The broad suite of data the app garners, including location data, phone usage data, captured image metadata, and network connectivity data, are accessible to PRCISS if that data transits China or is stored within its borders.

[redacted]

[3] (U) *See Breaking Trust: Shades of Crisis Across an Insecure Software Supply Chain*, The Atlantic Council (July 2020).

[4] (U) *See* U.S. v. Zhu Hua and Zhang Shilong, 18 C.F.R 00891, Department of Justice Indictment, United States District Court, Southern District of New York (Dec. 17, 2018).

[redacted]