(b)(3) [redacted]

NIC | NATIONAL INTELLIGENCE COUNCIL

NATIONAL INTELLIGENCE COUNCIL MEMORANDUM

(U) THIS IS AN IC-COORDINATED MEMORANDUM.

28 September 2017

NICM 2017-110 REL NATO

(b)(3) [redacted] Kaspersky Laboratory Products Puts Networks and Data at Risk of Exploitation by Russian Intelligence Services

(b)(3) [redacted] **We assess that the use of Kaspersky Laboratory (KL) anti-virus products risks exposing government and commercial networks on which it is used to the Russian intelligence services, despite it being consistently ranked as one of the top personal antivirus products in the world.** All anti-virus software, by its nature, has persistent, invasive access to all data on customer computers, a characteristic which is not exclusive to Kaspersky Lab. However, as a Russian entity, the company would be required by Russian law to cooperate with requests for data from the Russian Intelligence services.

- (U) As with most antivirus products, KL antivirus software sends information from customer networks to a cloud-based network for storage and analysis, after which users' computers are scanned against identified cyber threats, such as malware, viruses, vulnerabilities, and bad or suspicious Internet Protocol addresses.

(b)(3) [redacted] KL products operate on hundreds of millions of systems globally, and KL antivirus software is embedded in (b)(1), (b)(3) [redacted] software and hardware products. (b)(1), (b)(3) [redacted]

(b)(1), (b)(3) [redacted]

(U//~~REL TO USA, NATO~~) This Sense of the Community Memorandum was prepared for the National Intelligence Council under the auspices of the National Intelligence Officer for Cyber Issues. (b)(3) [redacted]

(b)(3) [redacted] *Questions about this memorandum may be directed to the NIO on* (b)(3) [redacted]

(b)(3) [redacted]

(b)(1), (b)(3) [redacted]

(U) **Kaspersky Lab has also been accused of its own unethical business practices, according to international media.** For example, in 2015 the company was accused of sabotaging competitor software, by flagging benign files as malicious files so that its competitors' anti-virus software would mark the files as dangerous. These "false-positive" hits resulted in some Kaspersky Lab competitors' customer computers not working properly as some of the falsely flagged files were essential to the operating system.