Crowell

CLIENT ALERT

Biden Administration Considers Imposing Sanctions on Kaspersky Labs

April 6, 2022

As the U.S. government continues to ratchet up sanctions in response to the Russian invasion of Ukraine, public reporting suggests there may be a new target in the sites of U.S. sanctions authorities: Kaspersky Labs (Kaspersky), the popular Russian cybersecurity and antivirus company. Any sanctions imposed by the Department of Treasury's Office of Foreign Assets Control (OFAC) would come on the heels of other recent government action against Kaspersky. On March 25, 2022, the Federal Communications Commission (FCC) added Kaspersky to its list of communications equipment and services that are deemed to pose an unacceptable risk to the national security of the United States, as well as the safety and security of the American people. Kaspersky, which is headquartered in Moscow, is the first non-Chinese company added to the list that includes Shenzhen-based Huawei Technologies Company and ZTE Corporation, among others. Kaspersky has publicly disagreed with the decision.

Last week, several news outlets reported that the U.S. government has been privately warning some critical infrastructure companies that Russia could manipulate software designed by Kaspersky to gain remote access to customer information systems. Similarly the United Kingdom's National Cyber Security Centre (NCSC) has pointed out that the risk calculus has "materially changed," and the NCSC further notes that "Russian law already contains legal obligations on companies to assist the Russian Federal Security Service (FSB), and the pressure to do so may increase in a time of war." Because many of Kaspersky's most popular products relate to antivirus, endpoint protection, and cloud security, the chief concern is that such software may have privileged access to sensitive data or locations that could be exploited for Russia's strategic advantage.

These actions, and the looming possibility of sanctions, are the latest in a multi-year campaign by the federal government to reduce the risks it has identified as associated with Kaspersky's products and services. On September 13, 2017, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) issued Binding Operational Directive 17-01, *Removal of Kaspersky-Branded Products*, requiring federal agencies to remove and discontinue use of all Kaspersky antivirus software because of the inherent vulnerability that Russian government threat actors could potentially exploit the software's system access. The following year, the National Defense Authorization Act for Fiscal Year 2018 prohibited the federal government from using hardware, software, or services developed, in whole or in part, by Kaspersky. A corresponding addition to the Federal Acquisition Regulation (FAR)—FAR 52.204-23—prohibited government contractors from providing or using such hardware, software, and services in performance of a federal contract or subcontract. In conjunction with these actions, several U.S. government officials warned of the risks to the private sector.

While the U.S. government considers sanctions against Kaspersky, there are several actions companies can undertake now to mitigate potential business disruptions and further secure their information and information systems:

- **Identify Kaspersky Products and Services** – Companies should first consider whether they use any of Kaspersky's cybersecurity offerings, from antivirus and endpoint protection offerings; to cloud security; to professional services such as Kaspersky's security awareness training, security architecture design, or vulnerability and patch management

programs. Because Kaspersky's software is often packaged with or renamed by other computer security products and services, this could require additional time and resources.

- **Assess Supply Chain Implications** –Companies may also wish to examine whether their vendors and suppliers use Kaspersky's products, as sanctions can and often do come with unanticipated supply chain issues.
- **Source or Develop Alternative Solutions** – Companies that currently utilize Kaspersky should consider developing contingency plans to mitigate potential business disruptions. If alternatives are not already in place, now is the time to line up backup products, especially for antivirus and endpoint protection. Installing new antivirus and endpoint protection across an organization's estate can be time-consuming, fraught with configuration difficulties, and (in nearly all cases) first requires the removal of any previous antivirus or endpoint protection systems for the new solution to operate effectively.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Caroline E. Brown
Partner – Washington, D.C.
Phone: +1.202.624.2509
Email: cbrown@crowell.com

Robert Holleyman
Partner and C&M International President & CEO – Washington, D.C.
Phone: +1.202.624.2505
Email: rholleyman@crowell.com

Jeffrey L. Snyder
Partner – Washington, D.C.
Phone: +1.202.624.2790
Email: jsnyder@crowell.com

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1.202.624.2615
Email: ewolff@crowell.com

Alexander Urbelis
Senior Counsel – New York
Phone: +1.212.895.4254
Email: aurbelis@crowell.com

Paul C. Mathis
Associate – Washington, D.C.
Phone: +1.202.688.3432
Email: pmathis@crowell.com