KIRKLAND **ALERT**

March 21, 2018

Treasury Department Sanctions Russian Entities and Individuals for Cyberattacks and Election Interference, Indicating Additional Measures May be Forthcoming

On March 15, 2018, the U.S. Department of the Treasury Office of Foreign Assets Control ("OFAC") designated five entities and 19 individuals in response to Russian cyberattacks and Russia's attempted interference in the 2016 U.S. presidential election. The sanctions represent the most assertive action to date by the Trump Administration against Russia in response to its apparent interference in the 2016 election. Though the measures are narrowly tailored, the administration has indicated that there will be more sanctions forthcoming.

The sanctions represent the most assertive action to date by the Trump Administration against Russia in response to its apparent interference in the 2016 election.

The View from Washington

President Trump has been under pressure to impose sanctions on Russia since the summer of 2017, when Congress overwhelmingly passed the Countering America's Adversaries Through Sanctions Act ("CAATSA"), which set time limits by which the President had to take certain actions. Pressure increased over the last month as Treasury had yet to sanction the entities and individuals identified in its January 29, 2018, report on Russian oligarchs, senior political figures and parastatal entities, a report which was required under CAATSA. It became more acute last week, when British Prime Minister Theresa May accused Russia of being behind the poisoning of a former Russian spy and his daughter outside London. The U.S. joined the U.K., France and Germany in condemning the attack and "a pattern of earlier irresponsible Russian behavior," prompting the question of whether the Trump Administration would retaliate.[1]

In announcing the new sanctions just days before Russia's own presidential election, Treasury Secretary Steven Mnuchin characterized the measures as "targeted," given that they only add certain Russian entities and individuals to U.S. government restricted party lists rather than constitute wider sanctions on Russia more broadly.[2] However, he added that Treasury "intends to impose additional CAATSA sanctions … to hold Russian government officials and oligarchs accountable for their destabilizing activities by severing their access to the U.S. financial system."[3] It remains to be seen what ultimately occurs, but it is possible this is the first in a series of Russia-related sanctions.

Summary of Sanctions Imposed

It remains to be seen what ultimately occurs, but it is possible this is the first in a series of Russia-related sanctions.

The March 15th announcement consists of related cyber sanctions on two types of parties:

Malicious Cyber Actors

Treasury designated three entities and 13 individuals under Executive Order ("EO") 13694, which predated CAATSA but was codified by Section 222 of the statute, and is directed generally at persons outside the U.S. determined to be engaging in "significant malicious cyber-enabled activities."[4] Those designated include the Internet Research Agency LLC ("IRA"), which on February 16, 2018, was indicted by special counsel Robert Mueller in connection with the probe into Russia's attempted election interference.[5] Treasury stated, e.g., that the IRA "tampered with or altered information in order to interfere with the 2016 U.S. election."[6]

Parties designated under the sanctions orders are added to OFAC's List of Specially Designated Nationals and Blocked Persons ("SDN List"). This means their assets in the U.S. are blocked, their access to the U.S. financial system is cut off, and that U.S. persons are generally prohibited from engaging in transactions with them. As a practical matter, non-U.S. persons, such as EU-based global financial institutions, likely also will refrain from dealing with SDNs in order to preserve their own access to U.S. dollars. Some of the parties designated under EO 13694 were already subject to blocking sanctions for other reasons, but now are designated on the SDN List for an additional reason.

Cyber Actors Operating on Behalf of the Russian Government

Treasury also designated two entities and six individuals under section 224 of CAATSA itself, which "targets cyber actors operating on behalf of the Russian government."[7] These designations include Russia's Federal Security Service, (*Federalnaya Sluzhba Bezopasnosti*) ("FSB"), a Russian intelligence organization considered the successor to the Soviet Union's KGB. In December 2016, OFAC had previously designated the FSB under EO 13694, and therefore it was already on the SDN List.

In announcing the sanctions, OFAC also amended and re-issued a General License ("General License 1A") ("GL 1A") it had previously issued authorizing certain transactions with the FSB.[8] OFAC stated that GL 1A "only authorizes certain transactions with the FSB acting in its administrative and law enforcement capacities."[9] These include those that are necessary and ordinarily incident to:

- requesting, receiving, utilizing, paying for, or dealing in certain licenses and authorizations for the importation, distribution, or use of certain information technology products in the Russian Federation;
- compliance with rules and regulations administered by, and certain actions or investigations involving, the FSB; and

- travel to or from Russia, including those transactions required to enter into and exit the country (i.e., complying with Russian border control requirements).[10]

GL 1A acknowledges the comprehensive role the FSB plays in Russia's economy. For example, as identified above, companies seeking to import into Russia products that implement encryption first must obtain authorization from the FSB.[11] Treasury sought to stop short of imposing sanctions that, in penalizing the FSB, could also hurt the interests of U.S. companies. In issuing GL 1A, Treasury stated it "was issued in order to ensure that U.S. persons engaging in certain business activities in Russia that are not otherwise prohibited are not unduly impacted."[12]

Treasury sought to stop short of imposing sanctions that, in penalizing the FSB, could also hurt the interests of U.S. companies.

Key Takeaways

- Russia-related business carries increasingly heightened risk. Investors and companies contemplating business with a Russia nexus should conduct a careful assessment of all potential counterparties, including their beneficial owners.
- U.S. companies engaging in transactions with the FSB should carefully check those activities against the terms of GL 1A, to ensure they remain in compliance with the limits of what it authorizes.
- Additional Russia-related measures may be forthcoming in the near future, requiring ongoing diligence and reevaluation of potential vectors of risk.

* * *

Anchored in Washington, D.C., Kirkland & Ellis's International Trade and National Security Practice, in coordination with the Firm's global offices and related practice areas, serves as a trusted adviser to companies, private equity sponsors and financial institutions to identify, assess and mitigate the complex international risks of operating and investing across national borders.

We focus on U.S. and EU economic sanctions (OFAC, EU), export controls (ITAR, EAR), anti-money laundering (AML), national security investment reviews (CFIUS) and related areas. We regularly work with our clients on a global basis on transactional, regulatory counseling, and investigative and enforcement matters, providing seasoned, holistic and sound advice.

If this publication was forwarded to you and you would like to receive similar future client alerts directly, please subscribe here.

---

[1] Press Release, Salisbury attack: Joint statement from the leaders of France, Germany, the United States and the United Kingdom (Mar. 15, 2018), https://www.gov.uk/government/news/salisbury-attack-joint-statement-from-the-leaders-of-france-germany-the-united-states-and-the-united-kingdom.

[2] Press Release, Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks (Mar. 15, 2018), https://home.treasury.gov/news/press-releases/sm0312 (hereinafter "Treasury Press Release").

[3] *Id.*

[4] Exec. Order No. 13694, 80 Fed. Reg. 63 (Apr. 2, 2015) (amended Dec. 29, 2016).

[5] Indictment, *United States v. Internet Research Agency LLC*, Case 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).

[6] Treasury Press Release.

[7] 22 USC § 9524 (2017).

[8] General License No. 1A Authorizing Certain Transactions with the Federal Security Service (Mar. 15, 2018), *available at* https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber_gl1a.pdf.

[9] FAQ No. 502, Office of Foreign Assets Control (Mar. 15, 2018), https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#501 ("FAQ No. 502").

[10] FAQs No. 501-04, Office of Foreign Assets Control (Mar. 15, 2018), https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#501.

[11] Under GL 1A, corresponding payments to the FSB under such procedures could not exceed $5,000 in any calendar year, and exports of encryption software still separately would require an export license from the U.S. Department of Commerce Bureau of Industry and Security.

[12] FAQ No. 502.

If you have any questions about the matters addressed in this *Kirkland Alert*, please contact the following Kirkland authors or your regular Kirkland contact.

Mario Mancuso, P.C.
Kirkland & Ellis LLP
655 Fifteenth Street, N.W.
Washington, D.C. 20005
www.kirkland.com/mmancuso
+1 202 879 5070

Zachary S. Brez, P.C.
Kirkland & Ellis LLP
601 Lexington Avenue
New York, NY 10022
www.kirkland.com/zbrez
+1 212 446 4720

Sanjay J. Mullick
Kirkland & Ellis LLP
655 Fifteenth Street, N.W.
Washington, D.C. 20005
www.kirkland.com/smullick
+1 202 879 5111

Joanna M. Ritcey-Donohue
Kirkland & Ellis LLP
655 Fifteenth Street, N.W.
Washington, D.C. 20005
www.kirkland.com/jritcey-donohue
+1 202 879 5980

Michael S. Casey
Kirkland & Ellis International LLP
30 St Mary Axe
London EC3A 8AF
www.kirkland.com/mcasey
+44 20 7459 2255

Ariel V. Lieberman
Kirkland & Ellis LLP
655 Fifteenth Street, N.W.
Washington, D.C. 20005
www.kirkland.com/alieberman
+1 202 879 5215