

Treasury Escalates Sanctions Against the Russian Government's Attempts to Influence U.S. Elections

April 15, 2021

WASHINGTON — Today, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) took sweeping action against 16 entities and 16 individuals who attempted to influence the 2020 U.S. presidential election at the direction of the leadership of the Russian Government.

This announcement follows the Intelligence Community's (IC) "Assessment of Foreign Threats to the 2020 U.S. Federal Elections." The IC assessment addresses the intentions and efforts of key foreign actors, including Russia, to influence or interfere with the U.S. elections and undermine public confidence in the election process. Russia employed a system of government officials, disinformation outlets, and companies to covertly influence U.S. voters and spread misinformation about U.S. political candidates and U.S. election processes and institutions.

"Treasury will target Russian leaders, officials, intelligence services, and their proxies that attempt to interfere in the U.S. electoral process or subvert U.S. democracy," said Secretary Janet L. Yellen. "This is the start of a new U.S. campaign against Russian malign behavior."

Today's actions highlight how multiple Russian officials, proxies, and intelligence agencies coordinated to interfere with recent U.S. elections. Private and public sector corruption facilitated by President Vladimir Putin has enriched his network of confidants, who used their illicit business connections to advance Russia's campaign to undermine the 2020 U.S. presidential election—and to give Russia plausible deniability in its disinformation activities. Members of this network include First Deputy Chief of Staff of the Presidential Administration of Russia **Alexei Gromov** (Gromov), previously designated as a government official pursuant to Executive Order (E.O.) 13661. Gromov leads the Kremlin's use of its media apparatus that sought to exacerbate tensions in the United States by discrediting the 2020 U.S. election process. As a result, Treasury is designating Gromov pursuant to E.O. 13848 for having attempted to interfere in the 2020 U.S. presidential election.

TREASURY TARGETS DISINFORMATION OUTLETS CONTROLLED BY RUSSIAN INTELLIGENCE SERVICES

Russian Intelligence Services, namely the Federal Security Service (FSB), the Main Intelligence Directorate (GRU), and the Foreign Intelligence Service (SVR), play critical roles in propagating Russian disinformation online. The FSB, GRU, and SVR operate a network of websites that obscure their Russian origin to appeal to Western audiences. Outlets operated by Russian Intelligence Services focus on divisive issues in the United States, denigrate U.S. political candidates, and disseminate false and misleading information. The GRU and FSB were first designated in 2016.

The FSB directly operates disinformation outlets. **SouthFront** is an online disinformation site registered in Russia that receives taskings from the FSB. It attempts to appeal to military enthusiasts, veterans, and conspiracy theorists, all while going to great lengths to hide its connections to Russian intelligence. In the aftermath of the 2020 U.S. presidential election, SouthFront sought to promote perceptions of voter fraud by publishing content alleging that such activity took place during the 2020 U.S. presidential election cycle.





NewsFront is a Crimea-based disinformation and propaganda outlet that worked with FSB officers to coordinate a narrative that undermined the credibility of a news website advocating for human rights. Part of NewsFront's plan was to utilize Alexander Malkevich, who is also being re-designated in today's action, to further disseminate disinformation. NewsFront was also used to distribute false information about the COVID-19 vaccine, which further demonstrates the irresponsible and reckless conduct of Russian disinformation sites.

The **Strategic Culture Foundation** (SCF) is an online journal registered in Russia that is directed by the SVR and closely affiliated with the Russian Ministry of Foreign Affairs. SCF is controlled by the SVR's Directorate MS (Active Measures) and created false and unsubstantiated narratives concerning U.S. officials involved in the 2020 U.S. presidential election. It publishes conspiracy theorists, giving them a broader platform to spread disinformation, while trying to obscure the Russian origins of the journal so that readers may be more likely to trust the sourcing.

The GRU operates **InfoRos**. InfoRos calls itself a news agency but is primarily run by the GRU's 72nd Main Intelligence Information Center (GRITs). GRITs is a unit within Russia's Information Operations Troops, which is identified as Russia's military force for conducting cyber espionage, influence, and offensive cyber operations. InfoRos operates under two

organizations, “InfoRos, OOO” and “**IA InfoRos.**” InfoRos used a network of websites, including nominally independent websites, to spread false conspiracy narratives and disinformation promoted by GRU officials. **Denis Tyurin** (Tyurin) held a leadership role in InfoRos and had previously served in the GRU.

Russian Intelligence Service Disinformation Outlets

InfoRos	Strategic Culture Foundation	SouthFront	NewsFront
			
<p>InfoRos is covertly run by GRU 72nd Main Intelligence Information Center Officers. The GRU used InfoRos to exploit the worldwide health crisis to sow confusion and discord regarding the novel coronavirus.</p>	<p>The Strategic Culture Foundation is directed by Russia's SVR. It typically posts biased content while giving the misleading impression that is independent and unaffiliated with the SVR Directorate MS (Active Measures).</p>	<p>SouthFront is operated by the Russian FSB. It attempts to appeal to military enthusiasts, veterans, and conspiracy theorists, all while going to great lengths to hide its connections to Russia.</p>	<p>NewsFront is controlled by the Russian FSB. It is based in Crimea and partially focused on supporting Russia-backed forces in Ukraine. Its manipulative tactics led to a near total dismantling of its presence on social media in early 2020.</p>

Treasury designated SouthFront and the Strategic Culture Foundation pursuant to E.O. 13848 for having engaged in foreign interference in the U.S. 2020 presidential election. SouthFront was also designated pursuant to E.O. 13694, as amended, and E.O. 13382 for acting on behalf of the FSB. NewsFront was designated pursuant to the Countering America's Adversaries Through Sanctions Act (CAATSA), E.O. 13694, and E.O. 13382 for acting on behalf of the GRU.

Treasury also designated InfoRos, OOO, IA InfoRos, and Tyurin pursuant to CAATSA, E.O. 13694, and E.O. 13382 for acting on behalf of the GRU.

[More guidance specific to disinformation and election interference can be found on the website of the U.S. Cybersecurity and Infrastructure Security Agency.](#)

TREASURY FURTHER TARGETS YEVGENIY PRIGOZHIN'S NETWORK IN AFRICA

Yevgeniy Prigozhin (Prigozhin) is the Russian financier of the Internet Research Agency (IRA), the Russian troll farm that OFAC designated pursuant to E.O. 13848 in 2018 for interfering in

the 2016 presidential election. Prigozhin has been designated pursuant to E.O.s 13848, 13694, and 13661.

Russian national **Alexander Malkevich** (Malkevich) and his company, the **Foundation for National Values Protection** (FZNC), have facilitated Prigozhin's global influence operations since at least 2019. Malkevich, who was previously designated in 2018 pursuant to E.O. 13694 for directing USAREally, another designated Prigozhin-financed influence entity, has continued to support Prigozhin's disinformation operations. Malkevich runs the FZNC website. Malkevich utilized the FZNC website along with other Prigozhin operatives to spread messages on behalf of Prigozhin. Prigozhin has evolved from simply providing financial support to his global disinformation network to also writing content to denigrate the U.S. electoral process. Malkevich and the FZNC were designated pursuant to E.O.s 13848, 13694, and 13661 for supporting Prigozhin's global influence operations. FZNC was also designated pursuant to E.O. 13848 for being owned or controlled by Malkevich.

The **Association For Free Research And International Cooperation** (AFRIC), **International Anticrisis Center**, and Russian nationals **Petr Byschkov** (Byschkov), **Yulia Afanasyeva** (Afanasyeva), and **Taras Pribyshin** (Pribyshin) facilitate Prigozhin's malign operations in Africa and Europe while primarily operating from Russia. AFRIC has served as a front company for Prigozhin's influence operations in Africa, including by sponsoring phony election monitoring missions in Zimbabwe, Madagascar, the Democratic Republic of the Congo, South Africa, and Mozambique. Despite posing as an African-led initiative, AFRIC serves to disseminate Russia's preferred messaging, often related to disinformation. AFRIC works in coordination with other elements of the Prigozhin network, including FZNC and the International Anticrisis Center, a fraudulent think tank controlled by Prigozhin's operatives. Byschkov manages Prigozhin's "Africa Back Office," a team of political consultants tasked with devising strategies for manipulating African politics in support of Prigozhin's interests. Afanasyeva, an employee of the "Africa Back Office," ran AFRIC and the International Anticrisis Center. Pribyshin has conducted influence operations in Africa for the IRA in support of Prigozhin's objectives in the region since at least 2019.

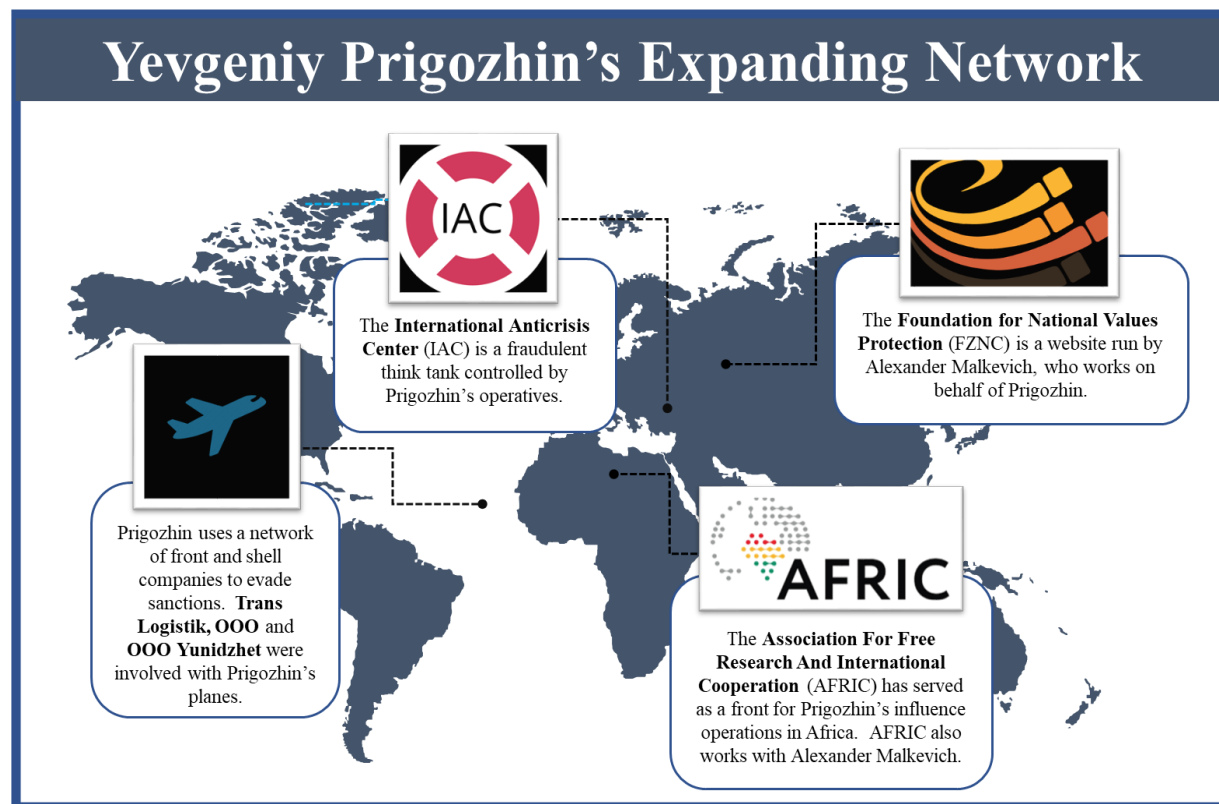
AFRIC, International Anticrisis Center, Byschkov, Afanasyeva, and Pribyshin were designated pursuant to E.O.s 13848, 13694, and 13661 for their roles in Prigozhin's operations.

TREASURY FURTHER TARGETS YEVGENIY PRIGOZHIN'S ATTEMPTS TO EVADE SANCTIONS

In addition, Prigozhin uses a complex network of shell and front companies to evade U.S. sanctions and to obscure his ownership in property. In 2019, two Russia-based companies, **Trans Logistik, OOO** (Trans Logistik) and **OOO Yunidzhet** (Yunidzhet), acted as covert procurement agents for Prigozhin to obtain aircraft related parts and maintenance. Trans Logistik obfuscated the ownership of Prigozhin's blocked property, including the previously identified aircraft that is blocked property, M-VITO, while Yunidzhet provided management services to another previously identified aircraft that is blocked property, M-SAAN. **Artem Stepanov** (Stepanov) is the Deputy General Director of Yunidzhet. **Maria Zueva** is the General Director of Yunidzhet. **Kirill Shcherbakov** is Yunidzhet's ultimate owner and also owns **OOO Alkon**, a company with close ties to Yunidzhet.

Trans Logistik and Yunidzhet were designated pursuant to E.O.s 13848, 13694 and 13661 for supporting Prigozhin. Stepanov, Zueva, and Shcherbakov were also designated pursuant to E.O.s 13848, 13694, and 13661 for acting on behalf of Yunidzhet. OOO Alkon was designated pursuant to E.O.s 13848, 13694, and 13661 for being owned by Stepanov.

The Federal Bureau of Investigation (FBI) is offering a reward of up to \$250,000 for information leading to the arrest of Prigozhin.



TREASURY TARGETS IRA ENABLER

Pakistan-based **Second Eye Solution** (SES), also known as Forwarderz, is an organization that specializes in creating and selling fraudulent identities and has assisted the IRA in concealing its identity to evade sanctions. Since at least 2012, SES engaged in a scheme to provide digital photographs of fake documents including passports, driver's licenses, bank statements, utility bills, and national identity documents. SES markets these fake documents for use to verify online accounts including money service business accounts and social media website accounts. In 2017, the IRA purchased 15 fraudulent U.S. driver licenses images from SES. The purchased licenses were used as supporting documents for online social media accounts opened by the IRA.

Pakistani Nationals **Mohsin Raza, Mujtaba Raza, Syed Hasnain, Muhammad Hayat, Syed Raza, and Shahzad Ahmed** are the owners and employees who were instrumental in processing payment for fraudulent identities. **Fresh Air Farm House, Like Wise, and MK Softtech** are four Pakistani front companies used to launder SES profits.

The fraudulent documents produced by SES are likely used at many online services to evade sanctions and anti-money laundering (AML) screening protocols beyond what OFAC has been able to identify. SES advertises that their fraudulent documents may be used on social media, freelancing job postings, and commerce platforms.

As part of today's listing of SES on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List), OFAC is also identifying digital currency addresses used by SES to fulfill customer orders in order to help assist financial institutions, and their third-party identity verification services, in identifying customers on their platforms who have purchased fraudulent identity documents. Known SES digital currency addresses have received over \$2.5 million in digital currencies over more than 26,900 transactions from 2013 to March 2021.

SES was designated pursuant to E.O.s 13848 and 13694, for acting on behalf of the IRA. Mohsin Raza, Mujtaba Raza, Seyed Hasnain, Muhammad Hayat, Syed Raza, and Shahzad Ahmed were designated pursuant to E.O.s 13848 and 13694, for acting for or on behalf of SES. Fresh Air Farm House, Like Wise, and MK Softtech were designated pursuant to E.O.s 13848 and 13694, for being owned or controlled by Mohsin Raza and Mujtaba Raza.

TREASURY TARGETS KNOWN RUSSIAN AGENT KONSTANTIN KILIMNIK

Konstantin Kilimnik (Kilimnik) is a Russian and Ukrainian political consultant and known Russian Intelligence Services agent implementing influence operations on their behalf. During the 2016 U.S. presidential election campaign, Kilimnik provided the Russian Intelligence Services with sensitive information on polling and campaign strategy. Additionally, Kilimnik sought to promote the narrative that Ukraine, not Russia, had interfered in the 2016 U.S. presidential election. In 2018, Kilimnik was indicted on charges of obstruction of justice and conspiracy to obstruct justice regarding unregistered lobbying work. Kilimnik has also sought to assist designated former President of Ukraine Viktor Yanukovich. At Yanukovich's direction, Kilimnik sought to institute a plan that would return Yanukovich to power in Ukraine.

Kilimnik was designated pursuant to E.O. 13848 for having engaged in foreign interference in the U.S. 2020 presidential election. Kilimnik was also designated pursuant to E.O. 13660 for acting for or on behalf of Yanukovich. Yanukovich, who is currently hiding in exile in Russia, was designated in 2014 pursuant to E.O. 13660 for his role in violating Ukrainian sovereignty.

[The FBI is offering a reward of up to \\$250,000 for information leading to the arrest of Kilimnik.](#)

SANCTIONS IMPLICATIONS

As a result of today's designations, all property and interests in property of these targets that are subject to U.S. jurisdiction are blocked, and U.S. persons are generally prohibited from engaging in transactions with them. Additionally, any entities 50 percent or more owned by one or more designated persons are also blocked. In addition, financial institutions and other persons that engage in certain transactions or activities with the sanctioned entities and individuals may expose themselves to secondary sanctions or be subject to an enforcement action.

[The Office of the Director of National Intelligence election interference report can be found on its website.](#)

[View more information on the persons designated today.](#)