THE WHITE HOUSE

FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government

APRIL 15, 2021 • STATEMENTS AND RELEASES

The Biden administration has been clear that the United States desires a relationship with Russia that is stable and predictable. We do not think that we need to continue on a negative trajectory. However, we have also been clear—publicly and privately—that we will defend our national interests and impose costs for Russian Government actions that seek to harm us.

Today the Biden administration is taking actions to impose costs on Russia for actions by its government and intelligence services against U.S. sovereignty and interests.

Executive Order Targeting the Harmful Foreign Activities of the Russian Government
Today, President Biden signed a new sanctions executive order that provides strengthened authorities to demonstrate the Administration's resolve in responding to and deterring the full scope of Russia's harmful foreign activities. This E.O. sends a signal that the United States will impose costs in a strategic and economically impactful manner on Russia if it continues or escalates its destabilizing international actions. This includes, in particular, efforts to undermine the conduct of free and fair democratic elections and democratic institutions in the United States and its allies and partners; engage in and facilitate malicious cyber activities against the United States and its allies and partners; foster and use transnational corruption to influence foreign governments; pursue extraterritorial activities targeting dissidents or journalists; undermine security in countries and regions important to United States national security; and violate well-established principles of international law, including respect for the territorial integrity of states.

The U.S. Department of the Treasury (Treasury) carried out the following actions pursuant to the new E.O.:

- Treasury issued a directive that prohibits U.S. financial institutions from participation in the primary market for ruble or non-ruble denominated bonds issued after June 14, 2021 by the Central Bank of the Russian Federation, the National Wealth Fund of the Russian Federation, or the Ministry of Finance of the Russian Federation; and lending ruble or non-ruble denominated funds to the Central Bank of the Russian Federation, the National Wealth Fund of the Russian Federation, or the Ministry of Finance of the Russian Federation. This directive provides authority for the U.S. government to expand sovereign debt sanctions on Russia as appropriate.

- Treasury designated six Russian technology companies that provide support to the Russian Intelligence Services' cyber program, ranging from providing expertise to developing tools and infrastructure to facilitating malicious cyber activities. These companies are being designated for operating in the technology sector of the Russian Federation economy. We will continue to hold Russia accountable for its malicious cyber activities, such as the SolarWinds incident, by using all available policy and authorities.

Imposing Additional Sanctions

Treasury sanctioned 32 entities and individuals carrying out Russian government-directed attempts to influence the 2020 U.S. presidential election, and other acts of disinformation and interference. This action seeks to disrupt the coordinated efforts of Russian officials, proxies, and intelligence agencies to delegitimize our electoral process. The U.S. government will continue to pursue those who engage in such activity.

Treasury, in partnership with the European Union, the United Kingdom, Australia, and Canada, sanctioned eight individuals and entities associated with Russia's ongoing occupation and repression in Crimea. The Transatlantic community stands united in supporting Ukraine against unilateral Russian provocations along the Line of Contact in eastern Ukraine, in occupied Crimea, and along Ukraine's borders, as well as agreeing on the need for Russia to immediately cease its military buildup and inflammatory rhetoric.

Reported Afghanistan Bounties

The Administration is responding to the reports that Russia encouraged Taliban attacks against U.S. and coalition personnel in Afghanistan based on the best assessments from the Intelligence Community (IC). Given the sensitivity of this matter, which involves the safety and well-being of our forces, it is being handled through diplomatic, military and intelligence channels. The safety and well-being of U.S. military personnel, and that of our allies and partners, is an absolute priority of the United States.

Expelling Diplomatic Personnel

The United States is expelling ten personnel from the Russian diplomatic mission in Washington, DC. The personnel include representatives of Russian intelligence services.

Further Responses to the SolarWinds Malicious Cyber Activity

Today the United States is formally naming the Russian Foreign Intelligence Service (SVR), also known as APT 29, Cozy Bear, and The Dukes, as the perpetrator of the broad-scope cyber espionage campaign that exploited the SolarWinds Orion platform and other information technology infrastructures. The U.S. Intelligence Community has high confidence in its assessment of attribution to the SVR.

The SVR's compromise of the SolarWinds software supply chain gave it the ability to spy on or potentially disrupt more than 16,000 computer systems worldwide. The scope of this compromise is a national security and public safety concern. Moreover, it places an undue burden on the mostly private sector victims who must bear the unusually high cost of mitigating this incident.

Today, the National Security Agency, the Cybersecurity & Infrastructure Security Agency, and the Federal Bureau of Investigation are jointly issuing a cybersecurity advisory, "Russian SVR Targets U.S. and Allied Networks," that provides specific details on software vulnerabilities that the SVR uses to gain access to victim devices and networks. The advisory also provides specific steps that network defenders can take to identify and defend against the SVR's malicious cyber activity.

Additionally, the SVR's compromise of SolarWinds and other companies highlights the risks

posed by Russia's efforts to target companies worldwide through supply chain exploitation. Those efforts should serve as a warning about the risks of using information and communications technology and services (ICTS) supplied by companies that operate or store user data in Russia or rely on software development or remote technical support by personnel in Russia. The U.S. government is evaluating whether to take action under Executive Order 13873 to better protect our ICTS supply chain from further exploitation by Russia.

Supporting a Global Cybersecurity Approach

The United States continues to strongly affirm the importance of an open, interoperable, secure, and reliable Internet. Russia's actions run counter to that goal, which is shared by many of our allies and partners. To strengthen our collective approach to bolstering cybersecurity, we are announcing two additional steps:

- First, the United States is bolstering its efforts to promote a framework of responsible state behavior in cyberspace and to cooperate with allies and partners to counter malign cyber activities. We are providing a first-of-its kind course for policymakers worldwide on the policy and technical aspects of publicly attributing cyber incidents, which will be inaugurated this year at the George C. Marshall Center in Garmisch, Germany. We are also bolstering our efforts through the Marshall Center to provide training to foreign ministry lawyers and policymakers on the applicability of international law to state behavior in cyberspace and the non-binding peacetime norms that were negotiated in the United Nations and endorsed by the UN General Assembly.

- Second, we are reinforcing our commitment to collective security in cyberspace. The Department of Defense is taking steps to incorporate additional allies, including the UK, France, Denmark, and Estonia, into the planning for CYBER FLAG 21-1, which is an exercise designed to improve our defensive capabilities and resiliency in cyberspace. CYBER FLAG 21-1 will build a community of defensive cyber operators and improve overall capability of the United States and allies to identify, synchronize, and respond in unison against simulated malicious cyberspace activities targeting our critical infrastructure and key resources.

The United States is committed to the security of our allies and partners; these efforts are intended to reinforce again our commitment to that bedrock principle.