EIB World Trade Headlines

Evolutions In Business • www.eib.com • (978) 256-0438
Fax: (978) 250-4529 • P.O. Box 4008, Chelmsford, MA 01824

CELEBRATING OVER 30 YEARS

August 1, 2021 - Volume 13, Issue 14

Georgia company and owner admit guilt in scheme to evade U.S. national security trade sanctions

All defendants in custody have now entered guilty pleas

SAVANNAH, GA: A Georgia company and its owner have admitted guilt in a scheme to evade United States national security laws.

Dali Bagrou pled guilty in U.S. District Court to Conspiracy, while his company, World Mining and Oil Supply (WMO) of Dacula, Ga., pled guilty to Violation of the Export Control Reform Act, said David H. Estes, Acting U.S. Attorney for the Southern District of Georgia. The plea subjects Bagrou to a statutory sentence of up to five years in prison and substantial financial penalties, followed by up to three years of supervised release, while WMO is subject to a sentence of up to five years' probation, along with significant fines and financial restitution. As part of his plea, Bagrou also agreed to forfeit a home purchased with illicit proceeds; the Atlanta-area residence is valued at approximately $800,000.

"The conspirators in this case were attempting to enrich themselves by evading trade sanctions put in place to protect the national security of the United States," said Acting U.S. Attorney Estes. "Thanks to outstanding effort by our law enforcement partners, these defendants are now being held accountable for their violations of the law."

(*Continued On The Following Page)

As described in court documents and testimony in USA v. World Mining and Oil Supply et. al., the conspiracy began when an unnamed Russian government-controlled business began working with with Oleg Vladislavovich Nikitin, general director of KS Engineering (KSE), a St. Petersburg, Russia-based energy company, in 2016 to purchase a power turbine from a U.S.-based manufacturer for approximately $17.3 million. The Russian company intended to use the turbine on a Russian Arctic deepwater drilling platform, expressly prohibited by the U.S. Department of Commerce unless a license is first obtained.

Nikitin admitted that he and another KSE employee, Anton Cheremukhin, conspired with Gabrielle Villone, Villone's company GVA, and Villone's business partner Bruno Caparini, to obtain the turbine on their behalf. Villone, Caprini and GVA then employed the services of Bagrou and WMO to procure the turbine from a U.S.-based manufacturer and to have the turbine shipped overseas. The parties conspired to conceal the true end user of the turbine from both the U.S. manufacturer and the U.S. government by submitting false documentation that stated the turbine would be used by a U.S. company in and around Atlanta.

Nikitin, Villone, and Bagrou all were arrested in Savannah, Ga., in 2019 while attempting to complete the illegal transaction. Villone currently is serving a 28-month prison sentence after pleading guilty to Conspiracy, while the other named defendants await sentencing after pleading guilty.

"Special Agents of the Bureau of Industry and Security's Office of Export Enforcement (OEE) will aggressively enforce Russia sectoral sanctions violations and any attempt to procure U.S origin goods in violation of U.S. export laws," said Ariel Joshua Leinwand, Special Agent in Charge of OEE's Atlanta Office. "The substantial penalties from this guilty plea should serve as a deterrent to those seeking to engage in illegal export activities."

"The FBI and our partners will always make threats to our national security a top priority, and this conspiracy was a direct threat," said Chris Hacker, Special Agent in Charge of FBI Atlanta. "This was a methodical plan to undercut United States sanctions to put our goods in the hands of actors who are a direct threat to our national security."

"The illegal export of technology to other countries poses a significant threat to America's warfighters," said Special Agent in Charge, Cynthia A. Bruce, Department of Defense Office of Inspector General, Defense Criminal Investigative Service, (DCIS) Southeast Field Office. "DCIS and our investigative partners will aggressively pursue those who violate the trade sanctions that threaten the national security of the United States."

*(*Continued On The Following Column)*

The Department of Commerce, Bureau of Industry and Security, Office of Export Enforcement, as well as the Defense Criminal Investigative Service and the Federal Bureau of Investigation are investigating the case with assistance from U.S. Customs and Border Protection and the Georgia Department of Natural Resources. Assistant U.S. Attorneys Jennifer G. Solari and Steven H. Lee are prosecuting the case, with assistance from Assistant U.S. Attorney Xavier A. Cunningham, Section Chief of the Asset Forfeiture Recovery Unit.

DEPARTMENT OF COMMERCE

Bureau of Industry and Security RIN 0694–XC078

Publication of a Report on the Effect of Imports of Uranium on the National

Security: An Investigation Conducted Under Section 232 of the Trade Expansion Act of 1962, as Amended

AGENCY: Bureau of Industry and Security, Commerce.
ACTION: Publication of a report.

SUMMARY: The Bureau of Industry and Security (BIS) in this notice is publishing a report that summarizes the findings of an investigation conducted by the U.S. Department of Commerce (the ''Department'') pursuant to Section 232 of the Trade Expansion Act of 1962, as amended (''Section 232''), into the effect of imports of uranium on the national security of the United States. This report was completed on April 14, 2019 and posted on the BIS website in July 2021. BIS has not published the appendices to the report in this notification of report findings, but they are available online at the BIS website, along with the rest of the report (see the ADDRESSES section).

DATES: The report was completed on April 14, 2019. The report was posted on the BIS website in July 2021.

ADDRESSES: The full report, including the appendices to the report, are available online at https://bis.doc.gov/232.

FOR FURTHER INFORMATION CONTACT: For further information about this report contact Erika Maynard, Special Projects Manager, (202) 482–5572; and Leah Vidovich, Trade and Industry Analyst, (202) 482–1819. For more information about the Office of Technology Evaluation and the Section 232 Investigations, please visit: http://www.bis.doc.gov/232.

https://www.bis.doc.gov/index.php/documents/regulations-docs/federal-register-notices/federal-register-2021/2794-86-fr-41540/file

U.S. economy grew 6.5 percent in second quarter, marking full recovery from pandemic losses

Rising vaccination rates and stimulus spending fueled economic growth that surpassed the last pre-pandemic peak set in 2019 and erased losses caused by the coronavirus crisis, according to the Bureau of Economic Analysis. But new uncertainty lies ahead, as coronavirus cases rise in parts of the country.

Department of Commerce's NTIA to Begin Accepting Applications for $268 Million Connecting Minority Communities Pilot Program

WASHINGTON – The Department of Commerce's National Telecommunications and Information Administration (NTIA) today released a Notice of Funding Opportunity for the Connecting Minority Communities Pilot Program, which will direct $268 million for expanding broadband access and connectivity to eligible Historically Black Colleges or Universities (HBCUs), Tribal Colleges or Universities (TCUs), minority-serving institutions (MSIs), and consortia led by an HBCU, TCU, or MSI that also include a minority business enterprise or tax-exempt 501(c)(3) organization.

"Communities of color have faced systemic barriers to affordable broadband access since the beginning of the digital age," said U.S. Secretary of Commerce Gina M. Raimondo. "The investments we make as part of the Connecting Minority Communities Pilot Program will help communities that are struggling with access, adoption and connectivity, and will inform our path forward as we seek to finally close the digital divide across the country."

The Connecting Minority Communities Pilot Program was established by the Consolidated Appropriations Act, 2021. Grants will be distributed to help HBCUs, TCUs and MSIs purchase broadband service or equipment, hire IT personnel, operate a minority business enterprise or a tax-exempt 501(c)(3) organization, and facilitate educational instruction, including remote instruction.

*(*Continued On The Following Column)*

"NTIA knows how crucial colleges, universities and other community institutions can be when it comes to reaching vulnerable citizens and making a lasting impact," said Acting NTIA Administrator Evelyn Remaley. "We look forward to working with historically Black Colleges and Universities, Tribal Colleges or Universities, and minority-serving institutions to advance our shared goal of a fully connected nation."

The Notice of Funding Opportunity published today on grants.gov outlines the requirements for grant applications and other information about the program. Completed applications must be received by grants.gov no later than 11:59 p.m. EST on Dec. 1, 2021. In June, NTIA published the Final Rule for the program, which included programmatic scope, general guidelines, and described the agency's method to determine applicant eligibility and identify which eligible recipients have the greatest unmet financial needs.
NTIA is holding a series of webinars to further inform the public. The next Connecting Minority Communities webinars will be held on August 18 and 19.

Georgia company and owner admit guilt in scheme to evade U.S. national security trade sanctions

All defendants in custody have now entered guilty pleas

SAVANNAH, GA: A Georgia company and its owner have admitted guilt in a scheme to evade United States national security laws.

Dali Bagrou pled guilty in U.S. District Court to Conspiracy, while his company, World Mining and Oil Supply (WMO) of Dacula, Ga., pled guilty to Violation of the Export Control Reform Act, said David H. Estes, Acting U.S. Attorney for the Southern District of Georgia. The plea subjects Bagrou to a statutory sentence of up to five years in prison and substantial financial penalties, followed by up to three years of supervised release, while WMO is subject to a sentence of up to five years' probation, along with significant fines and financial restitution. As part of his plea, Bagrou also agreed to forfeit a home purchased with illicit proceeds; the Atlanta-area residence is valued at approximately $800,000.

"The conspirators in this case were attempting to enrich themselves by evading trade sanctions put in place to protect the national security of the United States," said Acting U.S. Attorney Estes. "Thanks to outstanding effort by our law enforcement partners, these defendants are now being held accountable for their violations of the law."

*(*Continued On The Following Page)*

As described in court documents and testimony in *USA v. World Mining and Oil Supply et. al*., the conspiracy began when an unnamed Russian government-controlled business began working with with **Oleg Vladislavovich Nikitin,** general director of **KS Engineering (KSE),** a St. Petersburg, Russia-based energy company, in 2016 to purchase a power turbine from a U.S.-based manufacturer for approximately $17.3 million. The Russian company intended to use the turbine on a Russian Arctic deepwater drilling platform, expressly prohibited by the U.S. Department of Commerce unless a license is first obtained.

Nikitin admitted that he and another KSE employee, **Anton Cheremukhin**, conspired with **Gabrielle Villone**, Villone's company **GVA**, and Villone's business partner **Bruno Caparini**, to obtain the turbine on their behalf. Villone, Caprini and GVA then employed the services of Bagrou and WMO to procure the turbine from a U.S.-based manufacturer and to have the turbine shipped overseas. The parties conspired to conceal the true end user of the turbine from both the U.S. manufacturer and the U.S. government by submitting false documentation that stated the turbine would be used by a U.S. company in and around Atlanta.

Nikitin, Villone, and Bagrou all were arrested in Savannah, Ga., in 2019 while attempting to complete the illegal transaction. Villone currently is serving a 28-month prison sentence after pleading guilty to Conspiracy, while the other named defendants await sentencing after pleading guilty.

"Special Agents of the Bureau of Industry and Security's Office of Export Enforcement (OEE) will aggressively enforce Russia sectoral sanctions violations and any attempt to procure U.S origin goods in violation of U.S. export laws," said Ariel Joshua Leinwand, Special Agent in Charge of OEE's Atlanta Office. "The substantial penalties from this guilty plea should serve as a deterrent to those seeking to engage in illegal export activities."

"The FBI and our partners will always make threats to our national security a top priority, and this conspiracy was a direct threat," said Chris Hacker, Special Agent in Charge of FBI Atlanta. "This was a methodical plan to undercut United States sanctions to put our goods in the hands of actors who are a direct threat to our national security."

"The illegal export of technology to other countries poses a significant threat to America's warfighters," said Special Agent in Charge, Cynthia A. Bruce, Department of Defense Office of Inspector General, Defense Criminal Investigative Service, (DCIS) Southeast Field Office. "DCIS and our investigative partners will aggressively pursue those who violate the trade sanctions that threaten the national security of the United States."

*(*Continued On The Following Column)*

The Department of Commerce, Bureau of Industry and Security, Office of Export Enforcement, as well as the Defense Criminal Investigative Service and the Federal Bureau of Investigation are investigating the case with assistance from U.S. Customs and Border Protection and the Georgia Department of Natural Resources. Assistant U.S. Attorneys Jennifer G. Solari and Steven H. Lee are prosecuting the case, with assistance from Assistant U.S. Attorney Xavier A. Cunningham, Section Chief of the Asset Forfeiture Recovery Unit.

Brussels Summit Communiqué

Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 14 June 2021

14 Jun. 2021 -

1. We, the Heads of State and Government of the 30 NATO Allies, have gathered in Brussels to reaffirm our unity, solidarity, and cohesion, and to open a new chapter in transatlantic relations, at a time when the security environment we face is increasingly complex. NATO remains the foundation of our collective defence and the essential forum for security consultations and decisions among Allies. NATO is a defensive Alliance and will continue to strive for peace, security, and stability in the whole of the Euro-Atlantic area. We remain firmly committed to NATO's founding Washington Treaty, including that an attack against one Ally shall be considered an attack against us all, as enshrined in Article 5. We will continue to pursue a 360-degree approach to protect and defend our indivisible security and to fulfil NATO's three core tasks of collective defence, crisis management, and cooperative security.

2. NATO is the strongest and most successful Alliance in history. It guarantees the security of our territory and our one billion citizens, our freedom, and the values we share, including individual liberty, human rights, democracy, and the rule of law. We are bound together by our common values, enshrined in the Washington Treaty, the bedrock of our unity, solidarity, and cohesion. We commit to fulfiling our responsibilities as Allies accordingly. We reaffirm our adherence to the purposes and principles of the United Nations (UN) Charter. We are committed to the rules-based international order. We commit to reinforce consultations when the security or stability of an Ally is threatened or when our fundamental values and principles are at risk.

*(*Continued On The Following Page)*

3. We face multifaceted threats, systemic competition from assertive and authoritarian powers, as well as growing security challenges to our countries and our citizens from all strategic directions. Russia's aggressive actions constitute a threat to Euro-Atlantic security; terrorism in all its forms and manifestations remains a persistent threat to us all. State and non-state actors challenge the rules-based international order and seek to undermine democracy across the globe. Instability beyond our borders is also contributing to irregular migration and human trafficking. China's growing influence and international policies can present challenges that we need to address together as an Alliance. We will engage China with a view to defending the security interests of the Alliance. We are increasingly confronted by cyber, hybrid, and other asymmetric threats, including disinformation campaigns, and by the malicious use of ever-more sophisticated emerging and disruptive technologies. Rapid advances in the space domain are affecting our security. The proliferation of weapons of mass destruction and the erosion of the arms control architecture also undermine our collective security. Climate change is a threat multiplier that impacts Alliance security. The greatest responsibility of the Alliance is to protect and defend our territories and our populations against attack, and we will address all threats and challenges which affect Euro-Atlantic security.

4. We gather at a time when the COVID-19 pandemic continues to test our nations and our resilience. NATO and Allied militaries have supported the civilian response to the pandemic, while ensuring our collective defence and the effectiveness of our operations. We have also provided critical assistance to a number of partners through the delivery of vital medical supplies. We pay tribute to all those who combat this pandemic in our countries and around the world.

5. At our December 2019 meeting in London, we asked the Secretary General to carry out a forward-looking reflection process to further strengthen NATO's political dimension, including consultations. We recognise the important contribution of the independent group appointed by the Secretary General to support NATO 2030. As a result, today we agree NATO 2030 – a transatlantic agenda for the future. Throughout its history, NATO has continuously adapted to a changing security environment. The NATO 2030 agenda complements and builds on our ongoing political and military adaptation, strengthens our ability to deliver on the three core tasks and contributes to making our strong Alliance even stronger and ready for the future.

(*Continued On The Following Column)

6. To that end we agree to:

- Reaffirm that NATO is the unique, essential and indispensable transatlantic forum for consultations and joint action on all matters related to our individual and collective security. We pledge to strengthen and broaden our consultations and to ensure that NATO remains flexible and effective to conduct military operations in support of our common security. We reaffirm the Alliance's shared democratic principles as well as our commitment to the spirit and the letter of the North Atlantic Treaty. We commit to reinforcing consultations when the security or stability of an Ally is threatened or when our fundamental values and principles are at risk.
- Strengthen NATO as the organising framework for the collective defence of the Euro-Atlantic area, against all threats, from all directions. We reiterate our commitment to maintaining an appropriate mix of nuclear, conventional and missile defence capabilities for deterrence and defence, and to the 2014 Defence Investment Pledge, in its entirety. We commit to the full and speedy implementation of ongoing work to further strengthen our deterrence and defence posture, and we pledge to continue to improve the readiness of our forces and to strengthen and modernise the NATO Force Structure to meet current and future defence needs.
- Enhance our resilience. Noting that resilience remains a national responsibility, we will adopt a more integrated and better coordinated approach, consistent with our collective commitment under Article 3 of the North Atlantic Treaty, to reduce vulnerabilities and ensure our militaries can effectively operate in peace, crisis and conflict. Allies will develop a proposal to establish, assess, review and monitor resilience objectives to guide nationally-developed resilience goals and implementation plans. It will be up to each individual Ally to determine how to establish and meet national resilience goals and implementation plans, allowing them to do so in a manner that is compatible with respective national competences, structures, processes and obligations, and where applicable those of the EU.
- Foster technological cooperation among Allies in NATO, promote interoperability and encourage the development and adoption of technological solutions to address our military needs. For this purpose we will launch a civil-military Defence Innovation Accelerator for the North Atlantic. We also agree to establish a NATO Innovation Fund, where Allies who so wish can support start-ups working on dual-use emerging and disruptive technologies in areas key to Allied security.

(*Continued On The Following Page)

- Enhance NATO's ability to contribute to preserve and shape the rules-based international order in areas that are important to Allied security. We will increase our dialogue and practical cooperation with existing partners, including with the European Union, aspirant countries and our partners in the Asia Pacific, and strengthen our engagement with key global actors and other new interlocutors beyond the Euro-Atlantic area, including from Africa, Asia and Latin America.
- Substantially strengthen NATO's ability to provide training and capacity building support to partners, recognising that conflict, other security developments and pervasive instability in NATO's neighbourhood directly impact Allied security.
- Aim for NATO to become the leading international organisation when it comes to understanding and adapting to the impact of climate change on security. We agree to significantly reduce greenhouse gas emissions from military activities and installations without impairing personnel safety, operational effectiveness and our deterrence and defence posture. We invite the Secretary General to formulate a realistic, ambitious and concrete target for the reduction of greenhouse gas emissions by the NATO political and military structures and facilities and assess the feasibility of reaching net zero emissions by 2050. We will also initiate a regular high-level climate and security dialogue to exchange views and coordinate further action.
- Invite the Secretary General to lead the process to develop the next Strategic Concept. The Concept will be negotiated and agreed by the Council in Permanent Session and endorsed by NATO Leaders at the next Summit.

7. The NATO 2030 agenda sets a higher level of ambition for NATO. It provides clear guidelines for further adaptation to address existing, new and future threats and challenges, building on the ongoing political and military adaptation of the Alliance. Delivering on the NATO 2030 agenda, the three core tasks and the next Strategic Concept requires adequate resourcing through national defence expenditure and common funding. Based on requirements, we agree to increase such resourcing, including as necessary NATO common funding starting in 2023, taking into account sustainability, affordability and accountability. When we meet in 2022, we will agree, alongside the Strategic Concept, the specific requirements for additional funding up to 2030 and the resource implications across the NATO Military Budget, the NATO Security Investment Programme and the Civil Budget, as well as identify potential efficiency measures.

*(*Continued On The Following Column)*

8. NATO's fundamental and enduring purpose is to safeguard the freedom and security of all its members by political and military means. The evolving security environment increasingly requires us to address threats and challenges through the use of military and non-military tools in a deliberate, coherent, and sustained manner. NATO will take a tailored and structured approach. NATO uses a variety of non-military tools which support the Alliance's three core tasks. It also serves as a platform for enhancing the coherent use of these tools by Allies, under their own authority and control, and alongside other international actors. We will continue to strengthen effective, clear, and convincing strategic communication as an essential element to support all three of NATO's core tasks.

9. For more than twenty-five years, NATO has worked to build a partnership with Russia, including through the NATO-Russia Council (NRC). While NATO stands by its international commitments, Russia continues to breach the values, principles, trust, and commitments outlined in agreed documents that underpin the NATO-Russia relationship. We reaffirm our decisions towards Russia agreed at the 2014 Wales Summit and all our subsequent NATO meetings. We have suspended all practical civilian and military cooperation with Russia, while remaining open to political dialogue. Until Russia demonstrates compliance with international law and its international obligations and responsibilities, there can be no return to "business as usual". We will continue to respond to the deteriorating security environment by enhancing our deterrence and defence posture, including by a forward presence in the eastern part of the Alliance. NATO does not seek confrontation and poses no threat to Russia. Decisions we have taken are fully consistent with our international commitments, and therefore cannot be regarded by anyone as contradicting the NATO-Russia Founding Act.

10. We call on Russia to rescind the designation of the Czech Republic and the United States as "unfriendly countries" and to refrain from taking any other steps inconsistent with the Vienna Convention on Diplomatic Relations.

11. Russia's growing multi-domain military build-up, more assertive posture, novel military capabilities, and provocative activities, including near NATO borders, as well as its large-scale no-notice and snap exercises, the continued military build-up in Crimea, the deployment of modern dual-capable missiles in Kaliningrad, military integration with Belarus, and repeated violations of NATO Allied airspace, increasingly threaten the security of the Euro-Atlantic area and contribute to instability along NATO borders and beyond.

*(*Continued On The Following Page)*

12. In addition to its military activities, Russia has also intensified its hybrid actions against NATO Allies and partners, including through proxies. This includes attempted interference in Allied elections and democratic processes; political and economic pressure and intimidation; widespread disinformation campaigns; malicious cyber activities; and turning a blind eye to cyber criminals operating from its territory, including those who target and disrupt critical infrastructure in NATO countries. It also includes illegal and destructive activities by Russian Intelligence Services on Allied territory, some of which have claimed lives of citizens and caused widespread material damage. We stand in full solidarity with the Czech Republic and other Allies that have been affected in this way.

13. Russia has continued to diversify its nuclear arsenal, including by deploying a suite of short- and intermediate-range missile systems that are intended to coerce NATO. Russia has recapitalised roughly 80 percent of its strategic nuclear forces, and it is expanding its nuclear capabilities by pursuing novel and destabilising weapons and a diverse array of dual-capable systems. Russia continues to use aggressive and irresponsible nuclear rhetoric and has increased its ongoing emphasis on destabilising conventional exercises that include dual-capable systems. Russia's nuclear strategy and comprehensive nuclear weapon systems modernisation, diversification, and expansion, including the qualitative and quantitative increase of Russian non-strategic nuclear weapons, increasingly support a more aggressive posture of strategic intimidation. We will continue to work closely together to address all the threats and challenges posed by Russia.

14. We reiterate our support for the territorial integrity and sovereignty of Ukraine, Georgia, and the Republic of Moldova within their internationally recognised borders. In accordance with its international commitments, we call on Russia to withdraw the forces it has stationed in all three countries without their consent. We strongly condemn and will not recognise Russia's illegal and illegitimate annexation of Crimea, and denounce its temporary occupation. The human rights abuses and violations against the Crimean Tatars and members of other local communities must end. Russia's recent massive military build-up and destabilising activities in and around Ukraine have further escalated tensions and undermined security. We call on Russia to reverse its military build-up and stop restricting navigation in parts of the Black Sea. We also call on Russia to stop impeding access to the Sea of Azov and Ukrainian ports. We commend Ukraine's posture of restraint and diplomatic approach in this context. We seek to contribute to de-escalation. We are also stepping up our support to Ukraine. We call for the full implementation of the Minsk Agreements by all sides, and support the efforts of the Normandy format and the Trilateral Contact Group.
supporting the Republic of Moldova's democratic reforms and

(*Continued On The Following Column)

Russia, as a signatory of the Minsk Agreements, bears significant responsibility in this regard. We call on Russia to stop fuelling the conflict by providing financial and military support to the armed formations it backs in eastern Ukraine. We reiterate our full support to the Organization for Security and Cooperation in Europe (OSCE) Special Monitoring Mission to Ukraine. We stress the importance of ensuring its safety and full and unhindered access throughout the entire territory of Ukraine, including Crimea and the Russia-Ukraine border, in accordance with its mandate. We further call on Russia to reverse its recognition of the Abkhazia and South Ossetia regions of Georgia as independent states; to implement the EU-mediated 2008 ceasefire agreement; to end its militarisation of these regions and attempts to forcibly separate them from the rest of Georgia through the continued construction of border-like obstacles; and to cease the human rights violations, arbitrary detentions, and harassments of Georgian citizens. We reiterate our firm support to the Geneva International Discussions. We also call on Russia to engage constructively in the Transnistria Settlement Process. We are committed to supporting the Republic of Moldova's democratic reforms and providing assistance through our Defence and Related Security Capacity Building Initiative.

15. We remain open to a periodic, focused, and meaningful dialogue with a Russia willing to engage on the basis of reciprocity in the NRC, with a view to avoiding misunderstanding, miscalculation, and unintended escalation, and to increase transparency and predictability. NRC meetings have helped us communicate clearly our positions, and we are ready for the next meeting of the NRC. We will continue to focus our dialogue with Russia on the critical issues we face. The conflict in and around Ukraine is, in current circumstances, the first topic on our agenda. NATO remains committed to making good use of the existing military lines of communication between both sides to promote predictability and transparency, and to reduce risks, and calls on Russia to do so as well. We continue to aspire to a constructive relationship with Russia when its actions make that possible.

16. Terrorism, in all its forms and manifestations, continues to pose a direct threat to the security of our populations, and to international stability and prosperity. We categorically reject and condemn terrorism in the strongest possible terms. Allies will continue to fight this threat with determination, resolve, and in solidarity. While nations retain the primary responsibility for their domestic security and their own resilience, the fight against terrorism demands a coherent, long-term effort by the international community as a whole, involving a wide range of instruments and actors. NATO's role in the fight against terrorism contributes to all three core tasks of the Alliance, and is an integral part of the Alliance's 360-degree approach to deterrence and defence. Cooperation in NATO adds value to Allies' national efforts and capacity to prevent, mitigate, respond to, and be resilient against acts of terrorism.

(*Continued On The Following Page)

We also recognise the need to address the conditions conducive to the spread of terrorism. Our approach to terrorism, and its causes, is in accordance with international law and the purposes and principles of the UN Charter, and upholds all relevant United Nations Security Council Resolutions (UNSCRs) on the fight against terrorism.

17. We remain fully committed to NATO's enhanced role in the international community's fight against terrorism, including through awareness and analysis, preparedness and responsiveness, capabilities, capacity building and partnerships, and operations. We continue to implement our 2019 Action Plan and will update it by the end of this year, to take account of the evolving terrorist threats. We are determined to meet our commitments under UNSCR 2396, including through NATO's new Battlefield Evidence Policy, supported by improved information and data collection, preservation, sharing, and analysis, within NATO's mandate. We will continue our work to defend against improvised explosive devices and chemical, biological, radiological, and nuclear (CBRN) threats. We are developing capabilities to protect our forces against terrorist misuse of technology, while capitalising on emerging technologies to help us in the fight against terrorism. We are also stepping up support to partner countries to fight terrorism themselves and deny terrorists safe haven, which in turn strengthens NATO's own security. NATO will also continue to engage, as appropriate, with partner countries and other international actors to ensure added value and complementarity. NATO continues to play its part in the Global Coalition to Defeat ISIS/Da'esh, including through our Airborne Warning & Control System (AWACS) surveillance flights and staff-to-staff support.

18. After almost 20 years, NATO's military operations in Afghanistan are coming to an end. We have denied terrorists a safe haven from which to plot attacks against us, helped Afghanistan to build its security institutions, and trained, advised, and assisted the Afghan National Defence and Security Forces; they are now taking on full responsibility for security in their country. We pay tribute to those who have lost their lives or have been wounded, and express our deep appreciation to all the men and women who have served under the NATO flag, and to their families.

19. Withdrawing our troops does not mean ending our relationship with Afghanistan. We will now open a new chapter. We affirm our commitment to continue to stand with Afghanistan, its people, and its institutions in promoting security and upholding the hard-won gains of the last 20 years. Recalling our previous commitments, NATO will continue to provide training and financial support to the Afghan National Defence and Security Forces, including through the Afghan National Army Trust Fund. NATO will retain a Senior Civilian Representative's Office in Kabul to continue diplomatic engagement and enhance our partnership with Afghanistan.

Continue Here

Sentencing of Canadian Citizen Michael Spavor

08/11/2021 08:18 AM EDT

Antony J. Blinken, Secretary of State

We stand with the international community in calling for the People's Republic of China (PRC) to release, immediately and unconditionally, Canadian citizens Michael Spavor and Michael Kovrig. We continue to condemn these arbitrary detentions as well as the sentence imposed against Mr. Spavor on August 10. Mr. Spavor and Mr. Kovrig have not received the minimal procedural protections during their more than two-and-a-half-year arbitrary detention, and we stand with more than 60 countries who endorsed the recent Declaration Against Arbitrary Detention in State-to-State Relations. In my discussions with PRC officials, I have raised several cases of both U.S. and Canadian citizens subject to arbitrary detentions and exit bans in China, and I strongly support the immediate and unconditional release of all those whom the People's Republic of China has arbitrarily detained. The practice of arbitrarily detaining individuals to exercise leverage over foreign governments is completely unacceptable. People should never be used as bargaining chips.

The United States also remains deeply troubled by the lack of transparency surrounding these legal proceedings and joins Canada in calling for full consular access to Mr. Spavor and Mr. Kovrig, in accordance with the Vienna Convention on Consular Relations and the China-Canada Consular Agreement. We call upon PRC authorities to grant the requests of Canadian officials and other foreign diplomats to attend their proceedings.

The U.S. economy added 943,000 jobs in July as the labor market recovery boomed

The jobless rate in July was 5.4 percent. The data comes as Congress works on an infrastructure package that supporters say will add even more jobs.

NSO's Pegasus spyware: here's what we know

The Pegasus Project reports that journalists, activists, and heads of state could have been infiltrated

By Mitchell Clark Jul 23, 2021, 5:11pm EDT
Throughout the past week, we've seen story after story about a company called NSO Group, and a piece of spyware called Pegasus. Some of the stories have been shocking, with allegations that fully updated smartphones can be hacked with a single text message, and reports that two women close to murdered journalist Jamal Khashoggi were among those targeted by a government agency using the spy tool. A coalition of news outlets, including The Washington Post, Le Monde, and The Guardian is behind the reporting, and they're calling it the Pegasus Project. The project was led by Forbidden Stories, an organization of journalists that works on stories after the original reporters have been silenced in some way. Amnesty International ran detailed forensics on 67 smartphones to look for evidence that they were targeted by Pegasus spyware — and 37 of those phones tested positive. But many crucial details still aren't clear.

Here's what we know about the NSO Group and Pegasus so far.

What is Pegasus, and who or what is NSO Group?

Pegasus is spyware developed by a private contractor for use by government agencies. The program infects a target's phone and sends back data, including photos, messages, and audio / video recordings. Pegasus' developer, an Israeli company called NSO Group, says that the software can't be traced back to the government using it — a crucial feature for clandestine operations.

In short, NSO Group makes products that let governments spy on citizens. The company describes the role of its products on its website as helping "government intelligence and law-enforcement agencies use technology to meet the challenges of encryption" during terrorism and criminal investigations. But as you might imagine, civil liberties groups aren't happy about the spyware-for-hire business, and restricting the business to government clients does little to quiet their concerns.

The company told The Washington Post that it works only with government agencies, and that it will cut off an agency's access to Pegasus if it finds evidence of abuse. In its transparency report released at the end of June, the company claimed it has done that before. Still, an Amnesty International statement raised concerns that the company is providing spyware to oppressive governments, where government agencies can't be trusted to do right by their citizens.

(*Continued On The Following Column)

The Forbidden Stories organization, which helped lead the Pegasus Project's efforts, has a write-up of the company's exploits and controversies over the past decade, some of which have inspired lawsuits from journalists and activists arguing that NSO's software has been used improperly. The Washington Post also has an interview that covers the company's own story about how it was founded and how it got started in the surveillance industry.

Who was being spied on?

We don't know for sure. However, much of the reporting centers around a list containing 50,000 phone numbers, the purpose of which is unclear. The Pegasus Project analyzed the numbers on the list and linked over 1,000 of them to their owners. When it did so, it found people who should've been off-limits to governmental spying (based on the standards NSO says it holds its clients to): hundreds of politicians and government workers — including three presidents, 10 prime ministers, and a king — plus 189 journalists, and 85 human rights activists.

Wait, who made this list?

At this point, that's clear as mud. NSO says the list has nothing to do with its business, and claims it's from a simple database of cellular numbers that's a feature of the global cellular network. A statement from an Amnesty International spokesperson, posted to Twitter by cybersecurity journalist Kim Zetter, says that the list indicates numbers that were marked as "of interest" to NSO's various clients. The Washington Post says that the list is from 2016.

Settled Allegations

2021 Keysight Technologies, Inc. settled allegations that it violated the International Traffic in Arms Regulations (ITAR) in connection with unauthorized exports of technical data, to include software, to various countries, including a proscribed destination.

https://www.pmddtc.state.gov/sys_attachment.do?sysparm_referring_url=tear_off&view=true&sys_id=98ebc0e51b35b0d0c6c3866ae54bcb80

2021 Honeywell International, Inc. Honeywell International, Inc. settled allegations that it violated the International Traffic in Arms Regulations (ITAR) in connection with unauthorized exports and retransfers of technical data resulting from the failure to exercise appropriate internal controls.

https://www.pmddtc.state.gov/sys_attachment.do?sysparm_referring_url=tear_off&view=true&sys_id=113eab0b1bb764902dc36311f54bcb42

DEPARTMENT OF THE TREASURY and DEPARTMENT OF COMMERCE

Fact Sheet: Supporting the Cuban People's Right to Seek, Receive, and Impart Information through Safe and Secure Access to the Internet

August 11, 2021

Overview
The United States stands with the Cuban people in their quest for democracy, human rights, and fundamental freedoms. In July 2021, tens of thousands of Cubans took to the streets to make these demands of their government. In response to these protests, the Cuban regime reacted with violence and repression, including by implementing measures to curb the flow of information over the internet in Cuba.1 These actions continue a decades-long history of oppression by the regime, and a track record of failing to respect the basic universal rights of the Cuban population.

1 As outlined by the White House on July 22, 2021, the United States calls on Cuba's leaders to reinstate and to maintain access to all internet and telecommunications services for all people within Cuba's borders. Please see the White House Fact Sheet on Biden-Harris Administration Measures on Cuba here: https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/22/fact-sheet-biden-harris-administration-measures-on-cuba/.

2 This Fact Sheet is informational, does not have the force of law, and does not supersede any relevant statutes, Executive Orders, or regulations, including the legal provisions cited. The information herein is current and operative as of the date of publication of this Fact Sheet, unless or until modified.

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) and the U.S. Department of Commerce's Bureau of Industry and Security (BIS) administer a comprehensive economic embargo on Cuba, consistent with applicable legislation. While most transactions between persons subject to U.S. jurisdiction and Cuba continue to be prohibited under the embargo, the U.S. government allows for certain activities to support the Cuban people's access to information on the internet. The relevant OFAC regulations can be found in the Cuban Assets Control Regulations, 31 C.F.R. part 515 (CACR), which are available here. The relevant BIS regulations can be found in the Export Administration Regulations (EAR), 15 C.F.R. parts 730- 774, which are available here.

*(*Continued On The Following Column)*

Accordingly, and in view of recent events, OFAC and BIS are issuing this fact sheet to emphasize the U.S. government's commitment to promoting the ability of the Cuban people to seek, receive, and impart information, by highlighting the most relevant exemptions and authorizations pertinent to supporting the Cuban people through the provision of certain internet and related telecommunications services.2 In the event that individuals, entities, or governments face sanctions-related challenges in providing such assistance, have questions regarding the application of the exemptions or authorizations, or believe additional authorizations are needed, OFAC and BIS stand ready to engage with those stakeholders to provide guidance and respond to applications for specific licenses. 2

Provisions That Support Internet Freedom in Cuba
OFAC General Licenses

OFAC maintains the following general licenses (GLs), exemptions, and frequently asked questions (FAQs) related to the provision of internet-based services in Cuba; these may support the Cuban people's right to seek, receive, and impart information through safe and secure access to the internet.3 OFAC encourages those interested in providing such assistance to the Cuban people to avail themselves of these exemptions and authorizations to the extent applicable.
3 The Commerce Department regulates exports or reexports to Cuba of commodities, software, and technology that are subject to the EAR; exports and reexports that are licensed or otherwise authorized by the Commerce Department are, subject to certain requirements, also authorized by the Treasury Department under an existing OFAC general license (see EAR provisions outlined below; see §§ 515.533 of the CACR).

 Software and services for Cuban internet users: The CACR authorize the provision of certain services incident to the exchange of communications over the internet and services related to the exportation and reexportation of certain communications-related items. These authorizations cover the provision of certain fee-based internet communications services such as e-mail or other messaging platforms, social networking, VOIP, web hosting, and domain-name registration, among other services. These authorizations also cover services related to many kinds of software (including applications) used on personal computers, cell phones, and other personal communications devices. The CACR authorize the provision of services, including software design, business consulting, and IT management and support (including cloud storage), related to certain communications-related items or to install, repair, or replace such items or provide related training. These communications-related items include hardware and software exported or reexported to Cuba pursuant to BIS' License Exception Consumer Communications Device (CCD), License Exception Support for the Cuban People (SCP), or an individual license from BIS, as well as certain items that are not subject to the EAR. (CACR § 515.578 and §515.533; see also FAQs 785 and 787)

*(*Continued On The Following Page)*

Provision of telecommunications services and establishment of telecommunications facilities: The CACR authorize transactions, including payments, incident to the provision of telecommunications services related to the transmission or the receipt of telecommunications involving Cuba. The CACR also authorize certain transactions relating to the establishment of facilities to provide telecommunications services linking the United States or third countries and Cuba, including facilities to provide telecommunications services in Cuba. The CACR define telecommunications services to include internet connectivity, data, telephone, telegraph, radio, television, news wire feeds, and similar services, regardless of medium of transmission, including transmission by satellite. These authorizations are intended to improve access to telecommunications services for Cubans and increase international connections with the Cuban people, both with the United States and with third countries around the world. (CACR § 515.542; see also FAQ 784)

 In-country presence of internet and telecommunications providers: The CACR authorize providers of certain telecommunications or internet-based services to engage in transactions necessary to establish and maintain a physical presence (including leasing of physical premises such as an office, warehouse, classroom, or retail outlet space), or a business presence in Cuba to engage in transactions authorized by or exempt from the CACR. Transactions necessary to establish or maintain a business presence may include establishing and maintaining subsidiaries, branches, offices, joint ventures, franchises, or agency or other business relationships with any Cuban individual or entity (including ETECSA, the Cuban state-owned telecommunications provider), subject to certain limitations. (CACR § 515.573; see also FAQs 765 and 788)

 Internet-based distance learning and educational training: The CACR authorize the provision of certain internet-based courses, including distance learning and Massive Open Online Courses, to Cuban nationals, wherever located, provided that the course content is at the undergraduate level or below. (CACR §§ 515.565; see also FAQ 702)

(*Continued On The Following Column)

"The source of knowledge is experience."

BIS regulates the export and reexport to Cuba of commodities, software, and technology. Although nearly all U.S. items require a license for export or reexport to Cuba, there are several license exceptions that may be used to authorize such transactions in lieu of a license. Certain telecommunications and internet-related items may be exported and reexported to Cuba under a license exception issued by BIS if the items are intended to improve the free flow of information to, from, and among the Cuban people. License Exceptions Consumer Communications Devices (CCD) and Support for the Cuban People (SCP) authorize the export and reexport to Cuba of items intended to improve telecommunications and internet infrastructure and certain consumer communications items for use by eligible recipients. Both license exceptions specify the eligible items by description and Export Control Classification Number (ECCN) on the Commerce Control List (CCL).

Additional Information

For additional information, including the latest updates related to the Cuba sanctions program administered by OFAC, please refer to the Treasury Department's Cuba sanctions webpage available here. If you have additional questions regarding the scope of requirements under the OFAC-administered Cuba sanctions program, or the applicability or scope of any related OFAC authorizations, please contact OFAC's Sanctions Compliance and Evaluation Division at (800) 540-6322 or (202) 622-2490, or by email at OFAC_Feedback@treasury.gov .

For additional information concerning export controls related to Cuba, please refer to BIS' webpage available here. If you have questions regarding export control requirements for Cuba, please contact the BIS Foreign Policy Division at (202) 482-4254, or by email at foreign.policy@bis.doc.gov.