# EIB World Trade Headlines

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

July 15, 2021 - Volume 13, Issue 13


## Five Charged in Scheme to Export Thermal Imaging Scopes and Night Vision Goggles to Russia, in Violation of Arms Export Control Act

A federal grand jury in Los Angeles unsealed an indictment Thursday that accuses five defendants of conspiring to unlawfully export defense articles to Russia. Specifically, the defendants allegedly exported thermal imaging riflescopes and night-vision goggles without a license, in violation of the Arms Export Control Act.

According to court documents, Elena Shifrin, 59, of Mundelein, Illinois, and Vladimir Pridacha, 55, of Volo, Illinois, were arrested June 17 for their roles in a nearly four-year scheme in which the defendants purchased dozens of thermal imaging devices, most of which cost between $5,000 and $10,000 and are controlled by the International Traffic in Arms Regulations, from sellers across the United States. The other three defendants named in the indictment are: Boris Polosin, 45, of Russia; Vladimir Gohman, 52, of Israel; and Igor Panchernikov, 39, an Israeli national who, during much of the scheme, resided in Corona, California.

As outlined in the indictment, the defendants allegedly obtained many of the items using aliases, falsely assuring the sellers that they would not export the items from the United States. The thermal imaging devices were then exported to co-conspirators in Russia using aliases and false addresses to conceal their activities.

*(*Continued On The Following Page)*

*NEWSLETTER NOTES*

As alleged, the defendants hid the thermal imaging devices among other non-export-controlled items when exporting them to Russia, and they falsely stated on export declarations that the contents of their exports were non-export-controlled items with values of less than $2,500. In no case did any of the defendants obtain the required export licenses to export defense articles to Russia.

All five defendants are charged with conspiring to violate the Arms Export Control Act and face up to 20 years in federal prison if convicted. The indictment also accuses all five defendants of conspiring to smuggle thermal imaging devices from the United States and file false export information to conceal their activities, which carries a statutory maximum penalty of five years in prison. A federal district court judge will determine any sentence after considering the U.S. Sentencing Guidelines and other statutory factors.

Acting U.S. Attorney Tracy Wilkison of the Central District of California and Assistant Attorney General John C. Demers of the Justice Department's National Security Division made the announcement. The FBI's Los Angeles and Chicago Field Offices are investigating the case, with valuable assistance provided by the U.S. Postal Inspection Service and Homeland Security Investigations.

Assistant U.S. Attorneys David T. Ryan and Wilson Park of the Central District of California and Trial Attorney Matthew Chang of the National Security Division's Counterintelligence and Export Control Section are prosecuting the case.

An indictment is merely an allegation, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

## At 100, China's Ruling Party Faces Headwinds

On July 1, the Communist Party of China will observe the 100th anniversary of its founding with a "grand ceremony" and "[l]arge-scale exhibitions … display the glorious course, great achievements and valuable experience of the CPC over the past 100 years," as the party-affiliated Global Times put it.

But despite China's meteoric rise in recent decades, outside assessments point to difficulties ahead.

In a Foreign Affairs issue dedicated to the question of whether China can "keep rising," Jude Blanchette writes that the ambitious President Xi Jinping may prove to be an obstacle to the country's future success, as he courts risk by abandoning the measured, domestically focused strategies of his predecessors.

*(*Continued On The Following Column)*

China has multiplied its share of global GDP several times over since the 1990s, but Daniel H. Rosen argues in the same Foreign Affairs issue that China's economic growth may have reached a limit under its current, heavily state-regulated paradigm—and that the liberalization needed for further expansion could entail a rough ride. In the current issue of Washington Quarterly, Scott Rozelle and Matthew Boswell write that China has a big economic problem on its hands: Its hundreds of millions of rural citizens—who comprise roughly 7% of all humanity—suffer from underemployment, a lack of education, and little opportunity to either participate in or contribute to the country's middle-class boom. The problem, they suggest, could be knotty enough to prevent China from entering the ranks of high-income countries anytime soon.

## IMPOSES ADMINISTRATIVE PENALTY ONVIRGINIA COMPANY FORE XPORTS TO RUSSIAN MILITARY END USER WASHINGTON

–On June 28,2021,Kevin J. Kurland, Acting Assistant Secretary for Export Enforcement, Bureau of Industry and Security (BIS) of the U.S. Department of Commerce, announced an administrative settlement of $200,000 with Patriot 3, Inc. of Fredericksburg, Virginia. The BIS orderresolved allegations that Patriot 3, Inc.,on or about October 16, 2014, sold and/or transferred maritime jet bootswith underwater propulsion systems ("JetBoots"), items subject to the Export Administration Regulations(EAR), for export to military end users in Russia with knowledge that a violation of the EAR had occurred or was about or intended to occur in connection with the items. The items are classified under Export Control Classification Number ("ECCN") 8A992 and controlled in connection with exports to military end users or for military end uses in Russia as set forth in Section 744.21 of the EAR. The boots were valued at approximately $329,760and Patriot 3 sold and transferred the items for export to Russia knowing that they were destined for the Russian Government's Federal Guard Service (also known by the acronym "FSO") without the appropriate licenses required."Today's administrative settlement demonstrates Export Enforcement's commitment to combating violations of export laws and regulations with all of our enforcement tools, especially when it involves exports to military end users in Russia," said Acting Assistant Secretary Kurland. BIS's mission is to advance U.S. national security and foreign policy objectives by ensuring an effective export control and treaty compliance system and promoting continued U.S. strategic technology leadership. Among its enforcement efforts, BIS is committed to preventing U.S.-origin items from supporting Weapons of Mass Destruction (WMD) projects,facilitating terrorist activities, or destabilizing military modernization programs. For more information, please visitwww.bis.doc.gov.

## U.S. Secretary of Commerce Gina M. Raimondo Statement on Bipartisan Infrastructure Framework

WASHINGTON – Following President Joe Biden's announcement of the $1.2 trillion Bipartisan Infrastructure Framework, U.S. Secretary of Commerce Gina M. Raimondo released the following statement:

"Today represents a historic accomplishment that will transform our economy, create millions of good-paying jobs, rebuild our country's infrastructure, and position the United States to outcompete on the global stage. This framework is a momentous step forward in delivering for the American people and will benefit millions of American workers, businesses and communities.

"This framework provides long overdue investments in some of our most critical sectors that drive our economy, such as a historic $65 billion investment in broadband infrastructure to connect every American to reliable high-speed internet. The pandemic exposed how essential access to affordable, reliable broadband is to our everyday lives. Too many rural, tribal and minority communities do not have the access needed to go to school or work remotely, or access critical services like telemedicine. This bipartisan plan will bridge the digital divide and ensure no community is left behind.

"As the President has said – we've spent too much time competing with one another, and not nearly enough competing with the rest of the world to win the 21st century. We have a moment to show the world that democracies can succeed in tackling our biggest challenges and that America can lead by example. Today's Bipartisan Infrastructure Framework is our opportunity to do that. We are demonstrating that you can work across the aisle to deliver a big, bold plan with bipartisan support.

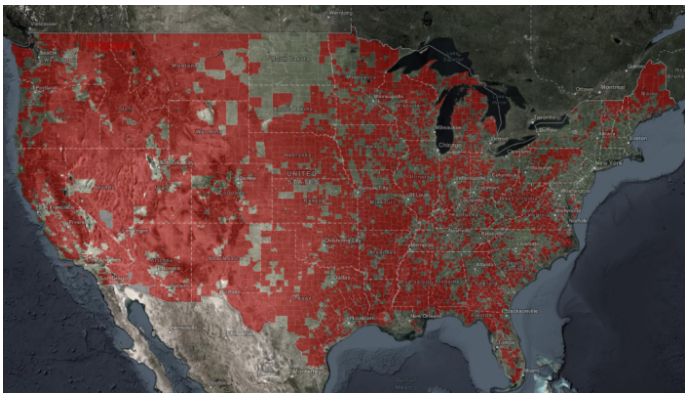
"Our work is not done. President Biden himself outlined critical priorities, such as investing in the Care Economy, that are not included in this package but remain critical components of our economic recovery and need to be included in the accompanying reconciliation package. I look forward to working with members of Congress to pass and implement the Bipartisan Infrastructure Framework as part of President Biden's Build Back Better Agenda."

## NTIA Creates First Interactive Map to Help Public See the Digital Divide Across the Country

NTIA map links poverty usage and broadband access by compiling data sets to show where high-poverty communities are located with relation to internet usage patterns and access to computers and related equipment
Infrastructure

Today, the U.S. Department of Commerce's National Telecommunications and Information Administration (NTIA) released a new publicly available digital map that displays key indicators of broadband needs across the country. This is the first interactive, public map that allows users to explore different datasets about where people do not have quality Internet access.

The public "Indicators of Broadband Need" tool released today puts on one map, for the first time, data from both public and private sources. It contains data aggregated at the county, census tract, and census block level from the U.S. Census Bureau, the Federal Communications Commission (FCC), M-Lab, Ookla and Microsoft. Speed-test data provided by M-Lab and Ookla help to illustrate the reality that communities experience when going online, with many parts of the country reporting speeds that fall below the FCC's current benchmark for fixed broadband service of 25 Mbps download, 3 Mbps upload. This is the first map that allows users to graphically compare and contrast these different data sources.



*(*Continued On The Following Page)*

"As we release this important data to the public, it paints a sobering view of the challenges facing far too many Americans as they try to connect to high-speed broadband and participate in our modern economy," said U.S. Secretary of Commerce Gina M. Raimondo. "In his American Jobs Plan, President Biden has proposed a once-in-a-lifetime investment that would finally connect one hundred percent of the country to reliable and affordable high-speed broadband."

The map also puts poverty and lack of broadband access on the same page. The dataset allows you to see where high-poverty communities are located and how that relates to internet usage patterns, as well as to a lack of computers and related equipment. The map also shows usage patterns in tribal communities, which have historically suffered from lack of internet access. Users can toggle the separate data sets on and off to compare information, and search for specific locations, including Tribal lands and minority-serving institutions, to gain a better understanding of where broadband needs are greatest.

"Any effort to close the digital divide starts with solid data, and NTIA continues to help policymakers make more informed decisions on expanding broadband access," said Acting NTIA Administrator Evelyn Remaley. "Now, the public can benefit from our platform to see which areas of the country still don't have broadband at speeds needed to participate in the modern economy."

"Broadband is no longer nice to have. It's need to have. To ensure that every household has the internet access necessary for success in the digital age, we need better ways to accurately measure where high-speed service has reached Americans and where it has not," said FCC Acting Chairwoman Jessica Rosenworcel. "The latest mapping effort by NTIA is a welcome new tool that provides valuable insight into the state of broadband across the country. Kudos to Secretary Raimondo and Acting Assistant Secretary Remaley for their leadership. The FCC looks forward to continuing our close collaboration with the Commerce Department and other federal partners to fulfill the goal of connecting 100 percent of Americans."

NTIA also offers to state governments and federal partners a geographic information system (GIS) platform called the National Broadband Availability Map (NBAM) that provides more complex tools for analyzing broadband access, such as the ability to upload GIS files to compare proposed projects. Earlier this month, NTIA announced that Arizona, Idaho, Kansas, Maryland, Mississippi, and South Dakota have joined the growing roster of state participants in the NBAM, bringing the total number of participating states to 36. The mapping platform allows these states and others to better inform broadband projects and funding decisions.

For more information about the NBAM, please visit NTIA's BroadbandUSA website or email nbam@ntia.gov .

## Commerce Department Adds Five Chinese Entities to the Entity List for Participating in China's Campaign of Forced Labor Against Muslims in Xinjiang

WASHINGTON – The Department of Commerce's Bureau of Industry and Security (BIS) added five Chinese entities to the Entity List for accepting or utilizing forced labor in the implementation of the People's Republic of China's campaign of repression against Muslim minority groups in the Xinjiang Uyghur Autonomous Region (XUAR). This action targets these entities' ability to access commodities, software, and technology subject to the Export Administration Regulations (EAR), and is part of a U.S. Government-wide effort to take strong action against China's ongoing campaign of repression against Muslim minority groups in the XUAR.

The entities to be added to the Entity List in connection with participating in the practice of, accepting, or utilizing forced labor involving Uyghurs and other Muslim minority groups in the XUAR are:

- Hoshine Silicon Industry (Shanshan) Co., Ltd.
- Xinjiang Daqo New Energy Co., Ltd.
- Xinjiang East Hope Nonferrous Metals Co., Ltd.
- Xinjiang GCL New Energy Material Technology Co., Ltd.
- Xinjiang Production and Construction Corps (XPCC)

This Entity List rule supplements other Entity List designations in October 2019, June 2020, and July 2020. Including the rule announced today, these actions have added 53 parties specifically implicated in human rights abuses of ethnic minorities from Xinjiang, and 15 of these which were implicated in human rights abuses related to forced labor of ethnic minorities from Xinjiang.

"As we made clear during this month's G7 summit, the United States is committed to employing all of its tools, including export controls, to ensure that global supply chains are free from the use of forced labor and technology is not misused to abuse human rights," said Secretary of Commerce Gina Raimondo. "The Commerce Department will continue to take firm, decisive action to hold China and other perpetrators of human rights abuses accountable."

*(*Continued On The Following Page)*

The Entity List is a tool utilized by BIS to restrict the export, reexport, and transfer (in-country) of items subject to the EAR to persons (individuals, organizations, companies) reasonably believed to be involved, or to pose a significant risk of becoming involved, in activities contrary to the national security or foreign policy interests of the United States. Additional license requirements apply to exports, re-exports, and transfers (in-country) of items subject to the EAR to listed entities, and the availability of most license exceptions is limited.

For more information, visit www.bis.doc.gov .

## Lisa Wang, Nominee for Assistant Secretary for Enforcement and Compliance, Department of Commerce

Ms. Wang has been a partner with Picard, Kentz and Rowe LLP since 2016. She specializes in international trade law matters, including antidumping and countervailing duty litigation and trade policy issues. Previously, Ms. Wang was a Senior Attorney in the Office of the Chief Counsel for Trade Enforcement and Compliance at the U.S. Department of Commerce, and an Assistant General Counsel in the Office of the U.S. Trade Representative. Before that, she spent three years as the Senior Import Administration Officer for the U.S. Embassy in Beijing, China, and was an associate with Dewey Ballantine LLP. She earned her JD from the Georgetown University Law Center, and her BS from Cornell University. Ms. Wang is married to Timothy Kovacs, where they reside in Washington, D.C. with their two young daughters.

## State Trade Expansion Program (STEP)

### Information for small businesses

The STEP grant program has helped thousands of small businesses obtain grants and find customers in the international marketplace since 2011. Through awards to U.S. states and territories, STEP helps small businesses overcome obstacles to exporting by providing grants to cover costs associated with entering and expanding into international markets.
STEP financial support helps U.S. small businesses:

- Learn to export
- Participate in foreign trade missions
- Design international marketing products and campaigns
- Support website globalization and e-commerce capabilities
- Pay for subscriptions to services provided by the U.S. Department of Commerce and other federal agencies
- Participate in export trade show exhibits and training workshops

Check out the Grants for U.S. Small Business to Sell Overseas webinar to learn more about the STEP program.
Review the following blog posts to learn how small businesses have successfully used STEP to help them export:

- Small Town Business STEPs into the Global Marketplace with a Little Help from SBA
- State Trade Expansion Program: 10 Years of Success

Contact a STEP awardee in your state to find out how they can help you start or expand your business to reach global customers: Find STEP awardees.

### Information for state entities

STEP provides financial awards to state and territory governments to assist small businesses with export development.
Find information on how eligible state entities can apply for STEP awards to be used to increase small business exporters and their sales in their state:

- STEP Grant Application Instructions
- STEP Grant Application Materials
- STEP Director's Memo - STEP 9 FY21 Funding and FAQs
- FY20 Funding Opportunity Announcement and FAQ

STEP awards are managed and provided at the local level by state government organizations. The program is managed at the national level by the SBA's Office of International Trade.

## Commerce Department Adds 34 Entities to the Entity List to Target Enablers of China's Human Rights Abuses and Military Modernization, and Unauthorized Iranian and Russian Procurement

FOR IMMEDIATE RELEASE Friday, July 9, 2021

publicaffairs@doc.gov

The Department of Commerce's Bureau of Industry and Security (BIS) added 34 entities to the Entity List for their involvement in, or risk of becoming involved in, activities contrary to the foreign policy and national security interests of the United States. Of these 34 entities, 14 are based in the People's Republic of China (PRC) and have enabled Beijing's campaign of repression, mass detention, and high-technology surveillance against Uyghurs, Kazakhs, and members of other Muslim minority groups in the Xinjiang Uyghur Autonomous Regions of China (XUAR), where the PRC continues to commit genocide and crimes against humanity. Commerce added another five entities directly supporting PRC's military modernization programs related to lasers and C4ISR programs to the Entity List.

Secretary of Commerce Gina Raimondo issued the following statement:

"The Department of Commerce remains firmly committed to taking strong, decisive action to target entities that are enabling human rights abuses in Xinjiang or that use U.S. technology to fuel China's destabilizing military modernization efforts. We will continue to aggressively use export controls to hold governments, companies, and individuals accountable for attempting to access U.S.-origin items for subversive activities in countries like China, Iran, and Russia that threaten U.S. national security interests and are inconsistent with our values."

As part of this package, Commerce added eight entities for facilitating the export of U.S. items to Iran in violation of the Export Administration Regulations (EAR) or to entities on the U.S. Department of the Treasury's Office of Foreign Assets Control Specially-Designated Nationals List. Commerce added another six entities for their involvement in the procurement of U.S.-origin electronic components, likely in furtherance of Russian military programs. Additionally, Commerce added one entity to the Military End-User List under the destination of Russia. Finally, Commerce removed one entity from the Unverified List, as a conforming change to this same entity being added to the Entity List for being involved in proliferation to unsafeguarded nuclear activities.

*(*Continued On The Following Column)*

The Entity List is a tool utilized by BIS to restrict the export, reexport, and transfer (in-country) of items subject to the EAR to persons (individuals, organizations, companies) reasonably believed to be involved, or to pose a significant risk of becoming involved, in activities contrary to the national security or foreign policy interests of the United States. Additional license requirements apply to exports, re-exports, and transfers (in-country) of items subject to the EAR to listed entities, and the availability of most license exceptions is limited.

For more information, visit www.bis.doc.gov.

## Canada to open its border to fully vaccinated U.S. citizens on Aug. 9

U.S. citizens and permanent residents who reside in the United States and have been inoculated with Canadian-authorized vaccines will be allowed to enter Canada for nonessential travel without quarantining, the country's public health agency announced. Travelers will be required to present a negative coronavirus molecular test taken before entering.

## U.S.-Russia Presidential Joint Statement on Strategic Stability

June 16, 2021 • Statements and Releases

We, President of the United States of America Joseph R. Biden and President of the Russian Federation Vladimir Putin, note the United States and Russia have demonstrated that, even in periods of tension, they are able to make progress on our shared goals of ensuring predictability in the strategic sphere, reducing the risk of armed conflicts and the threat of nuclear war.

The recent extension of the New START Treaty exemplifies our commitment to nuclear arms control. Today, we reaffirm the principle that a nuclear war cannot be won and must never be fought.

Consistent with these goals, the United States and Russia will embark together on an integrated bilateral Strategic Stability Dialogue in the near future that will be deliberate and robust. Through this Dialogue, we seek to lay the groundwork for future arms control and risk reduction measures.

# FACT SHEET: NATO Summit: Revitalizing the Transatlantic Alliance

June 13, 2021 • Statements and Releases

"The transatlantic alliance is the strong foundation on which our collective security and our shared prosperity are built. The partnership between Europe and the United States, in my view, is and must remain the cornerstone of all that we hope to accomplish in the 21st century, just as we did in the 20th century… The United States is fully committed to our NATO Alliance… we'll keep faith with Article 5."

– President Biden, February 19, 2021

President Biden will participate on June 14 in the NATO Summit in Brussels that brings together the leaders of all 30 Allied nations. During the Summit, the President will reaffirm the enduring Transatlantic bond through NATO and underscore the United States' ironclad commitment to Article 5 – an attack on one is an attack on all and will be met with a collective response. Allied leaders will launch an ambitious set of initiatives to ensure NATO continues to provide security to our citizens through 2030 and beyond.

The Transatlantic relationship is built on a foundation of shared democratic values. NATO's strength comes not only from its military might, but also its unity and common purpose founded on respect for democracy, individual liberty, and the rule of law, as enshrined in the Washington Treaty. Now in its 73rd year, NATO is the most powerful and successful Alliance in history. NATO faced down the Communist bloc in the Cold War and today provides security for approximately one billion people in Europe and North America. As NATO winds down its military presence in Afghanistan after nearly 20 years, the United States and our NATO Allies and partners will continue supporting the people of Afghanistan through civilian and security assistance. The United States will also continue to stand shoulder to shoulder with our Allies and partners in NATO's non-combat advisory mission in Iraq.

NATO played a pivotal role in coordinating the civilian response to COVID-19, airlifting hundreds of tons of critical supplies around the world and building almost 100 field hospitals, while maintaining its deterrence and defense posture. This assistance is saving lives and proves that defense investment and capacity building increase our nations' resilience in the face of all kinds of crises, not only against military threats.

Key Summit Outcomes:

*(*Continued On The Following Column)*

A New Strategic Concept: Allies will agree to revise NATO's Strategic Concept, a framework that will guide the Alliance's approach to the evolving strategic environment, which includes Russia's aggressive policies and actions; challenges posed by the People's Republic of China to our collective security, prosperity, and values; and transnational threats such as terrorism, cyber threats, and climate change. The new Strategic Concept will be prepared for adoption at the NATO Summit in 2022.

Updating Cyber Defenses: Leaders will endorse a new Cyber Defense Policy for NATO that will strengthen Allied coordination to ensure the Alliance is resilient against the increasingly frequent and severe threats we face from malicious cyber activity perpetrated by state and non-state actors, including disruptive ransomware attacks against critical infrastructure. This updated policy will also provide strategic guidance for NATO's political, military, and technical cyber efforts to deter, defend against, and counter the full spectrum of cyber threats. Leaders will also affirm the importance of defending our networks and ensuring Allies rely on trustworthy providers for next generation telecommunication networks.

Preserving our Technological Edge: Leaders will affirm that NATO's ability to ensure our common defense relies on maintaining our technological edge. Allies will launch a Defense Innovation Accelerator to facilitate their technological cooperation and speed the adoption of emerging technologies that will enhance the Alliance's defense and security.

Combatting Climate Change: Leaders will agree to a Climate Security Action Plan and set the ambition for NATO to become the leading international organization for understanding and adapting to the impact of climate change on security. They will agree to reduce greenhouse gases from military activities and installations in line with national commitments under the Paris Agreement, and agree to initiate a regular high-level global climate and security dialogue.

Strengthened Deterrence and Defense: Allies will commit to implementation of new military concepts and strategies that strengthen NATO's deterrence and defense posture to meet threats from Russia and elsewhere. NATO also continues to monitor the Russian deployments in and around Ukraine.

Greater Sharing of Responsibility: Non-U.S. defense spending has risen for seven consecutive years since the Wales Defense Investment Pledge adopted during the Obama-Biden Administration in 2014. Allied leaders will recommit to the Wales Pledge in its entirety and to providing NATO with cash, capabilities, and contributions of ready forces.

*(*Continued On The Following Page)*

Investing in NATO: Allies will also commit to ensuring NATO is led, staffed, and resourced at levels necessary to deliver on the decisions taken at the Summit. Leaders will agree to identify the additional resources, including through NATO common funding, to enhance NATO's ability to meet security challenges today and in the future.

Increased Consultation and Cohesion: Allies will commit to enhance political coordination at NATO on all matters related to their individual and collective security. Leaders will also reaffirm their commitment to their common values, including individual liberty, human rights, democracy, and the rule of law.

Stronger Societies: Recognizing the increasingly complex threats to our security, Allied leaders will affirm that national and collective resilience are essential for credible deterrence and defense, and vital to safeguard our societies, citizens, and shared values. Allied leaders will issue a Strengthened Resilience Commitment to outline future priorities, including on the security of supply chains, critical infrastructure, and energy networks, as well as preparedness for pandemics and natural disasters.

Deeper Partnerships: Allies will enhance NATO's ability to strengthen the rules-based international order by increasing dialogue and practical cooperation with the Alliance's partners, including the European Union and those in the Indo-Pacific (Australia, Japan, New Zealand, and the Republic of Korea). Leaders will recommit to NATO's Open Door Policy, which provides a path to membership for any European country that shares our values and meets the necessary responsibilities and obligations.

## Settlement Agreements between the U.S. Department of the Treasury's Office of Foreign Assets Control and Alfa Laval Middle East Ltd. and Alfa Laval Inc.

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) today announced a $415,695 settlement with Alfa Laval Middle East Ltd. ("AL Middle East"), a company located in Dubai, United Arab Emirates that sells fluid handling and other equipment for the energy industry and other sectors. AL Middle East has agreed to settle its potential civil liability for apparent violations of the Iranian Transactions and Sanctions Regulations, 31 C.F.R. part 560 (ITSR). Specifically, the apparent violations were committed between May 2015 and March 2016 when AL Middle East conspired with Dubai- and Iran-based companies to export Gamajet brand storage tank cleaning units from the United States to Iran.

*(*Continued On The Following Column)*

As a result of this conspiracy, AL Middle East caused its U.S.-based affiliate to indirectly export goods from the United States to Iran by falsely listing a Dubai-based company as the end-user on its export documentation. The scope of the conspiracy included additional incomplete and contemplated export transactions with Iran that would have employed the same scheme. OFAC determined that AL Middle East did not voluntarily self-disclose the apparent violations, and that the apparent violations constitute an egregious case.

Separately, OFAC today announced a $16,875 settlement with Alfa Laval Inc. ("AL U.S."), a company located in Richmond, Virginia. AL U.S. has agreed to settle its potential civil liability for apparent violations of the ITSR on behalf of its former subsidiary (now an operating unit) Alfa Laval Tank, Inc. ("AL Tank"), located in Exton, Pennsylvania. Specifically, the apparent violations were committed between May 2015 and March 2016 when AL Tank, which manufactures and sells storage tank cleaning equipment, referred a known Iranian business opportunity to its foreign affiliate in Dubai. The foreign affiliate then orchestrated a scheme to export goods from the United States to Iran and did so by using AL Tank to export its Gamajet brand cleaning units to Iran. OFAC determined that AL U.S. did not voluntarily self-disclose the apparent violations, and that the apparent violations constitute a non-egregious case.

## FACT SHEET: Executive Order Addressing the Threat from Securities Investments that Finance Certain Companies of the People's Republic of China

June 03, 2021 • Statements and Releases

Today, President Biden signed an Executive Order (E.O.) to further address the ongoing national emergency declared in E.O. 13959 of November 12, 2020 with respect to the threat posed by the military-industrial complex of the People's Republic of China (PRC). President Biden also expanded the scope of this national emergency by finding that the use of Chinese surveillance technology outside the PRC, as well as the development or use of Chinese surveillance technology to facilitate repression or serious human rights abuses, constitute unusual and extraordinary threats. This E.O. allows the United States to prohibit – in a targeted and scoped manner – U.S. investments in Chinese companies that undermine the security or democratic values of the United States and our allies.

Specifically, the E.O. the President is signing today will:

***(*Continued On The Following Page)***

Solidify and strengthen a previous E.O to prohibit U.S. investments in the military-industrial complex of the People's Republic of China: This E.O. will amend E.O. 13959 by creating a sustainable and strengthened framework for imposing prohibitions on investments in Chinese defense and surveillance technology firms. The E.O. prohibits United States persons from engaging in the purchase or sale of any publicly traded securities of any person listed in the Annex to the E.O. or determined by the Secretary of the Treasury, in consultation with the Secretary of State, and, as the Secretary of the Treasury deems appropriate, the Secretary of Defense:

To operate or have operated in the defense and related materiel sector or the surveillance technology sector of the economy of the PRC; or
To own or control, or to be owned or controlled by, directly or indirectly, a person who operates or has operated in any sector described above, or a person who is listed in the Annex to this E.O. or who has otherwise been determined to be subject to the prohibitions in this E.O.
Ensure that U.S. investments are not supporting Chinese companies that undermine the security or values of the United States and our allies: This E.O. prevents U.S. investment from supporting the Chinese defense sector, while also expanding the U.S. Government's ability to address the threat of Chinese surveillance technology firms that contribute — both inside and outside China — to the surveillance of religious or ethnic minorities or otherwise facilitate repression and serious human rights abuses. It signals that the Administration will not hesitate to prevent U.S. capital from flowing into the PRC's defense and related materiel sector, including companies that support the PRC's military, intelligence, and other security research and development programs; or into Chinese companies that develop or use Chinese surveillance technology to facilitate repression or serious human rights abuse. Tackling these challenges head-on is consistent with the Biden Administration's commitment to protecting core U.S. national security interests and democratic values, and the Administration will continue to update the list of PRC entities as appropriate. At the same time, the E.O.'s prohibitions are intentionally targeted and scoped.

The President listed the following 59 entities as subject to the E.O.'s prohibitions. The prohibitions against the entities listed in the Annex to this E.O. shall take effect beginning at 12:01 a.m. eastern daylight time on August 2, 2021. The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) will also list these 59 entities on its new Non-SDN Chinese Military-Industrial Complex Companies List (NS-CMIC List).

Defense and Related Materiel Sector of the Economy of the PRC:

*(*Continued On The Following Column)*

Aero Engine Corporation of China; Aerospace CH UAV Co., Ltd; Aerospace Communications Holdings Group Company Limited; Aerosun Corporation; Anhui Greatwall Military Industry Company Limited; Aviation Industry Corporation of China, Ltd.; AVIC Aviation High-Technology Company Limited; AVIC Heavy Machinery Company Limited; AVIC Jonhon Optronic Technology Co., Ltd.; AVIC Shenyang Aircraft Company Limited; AVIC Xi'An Aircraft Industry Group Company Ltd.; Changsha Jingjia Microelectronics Company Limited; China Academy of Launch Vehicle Technology; China Aerospace Science and Industry Corporation Limited; China Aerospace Science and Technology Corporation; China Aerospace Times Electronics Co., Ltd; China Avionics Systems Company Limited; China Communications Construction Company Limited; China Electronics Technology Group Corporation; China General Nuclear Power Corporation; China Marine Information Electronics Company Limited; China Mobile Communications Group Co., Ltd.; China National Nuclear Corporation; China National Offshore Oil Corporation; China North Industries Group Corporation Limited; China Nuclear Engineering Corporation Limited; China Railway Construction Corporation Limited; China Satellite Communications Co., Ltd.; China Shipbuilding Industry Company Limited; China Shipbuilding Industry Group Power Company Limited; China South Industries Group Corporation; China Spacesat Co., Ltd.; China State Shipbuilding Corporation Limited; China Telecommunications Corporation; China United Network Communications Group Co., Ltd.; Costar Group Co., Ltd.; CSSC Offshore & Marine Engineering (Group) Company Limited; Fujian Torch Electron Technology Co., Ltd.; Guizhou Space Appliance Co., Ltd; Hangzhou Hikvision Digital Technology Co., Ltd.; Huawei Technologies Co., Ltd.; Inner Mongolia First Machinery Group Co., Ltd.; Inspur Group Co., Ltd.; Jiangxi Hongdu Aviation Industry Co., Ltd.; Nanjing Panda Electronics Company Limited; North Navigation Control Technology Co., Ltd.; Panda Electronics Group Co., Ltd.; Semiconductor Manufacturing International Corporation; Shaanxi Zhongtian Rocket Technology Company Limited; and Zhonghang Electronic Measuring Instruments Company Limited.

Surveillance Technology Sector of the Economy of the PRC:

Hangzhou Hikvision Digital Technology Co., Ltd. and Huawei Technologies Co., Ltd.

Own or Control, or Owned or Controlled by, Directly or Indirectly, a Person Who Operates or Has Operated in at Least One of These Two Sectors of the PRC Economy, or a Person Who Is Listed in the Annex to the E.O.:

China Communications Construction Group (Limited); China Electronics Corporation; China Mobile Limited; China Telecom Corporation Limited; China Unicom (Hong Kong) Limited; CNOOC Limited; Huawei Investment & Holding Co., Ltd.; Panda Electronics Group Co., Ltd.; Proven Glory Capital Limited; and Proven Honour Capital Limited.

## Electrical Engineer Sentenced to More Than Five Years in Prison for Conspiring to Illegally Export to China Semiconductor Chips with Military Uses

A California man was sentenced today to 63 months, or more than five years, in prison for his role in a scheme to illegally export integrated circuits with military applications to China the required filing of electronic export information. As part of his sentence, the Judge ordered Shih to pay $362,698 in restitution to the IRS and fined him $300,000**.**

Yi-Chi Shih, 66, of Hollywood Hills, was convicted on July 2, 2019, to one count of conspiracy to violate the International Emergency Economic Powers Act (IEEPA) and the Export Administration Regulations (EAR). Shih also was convicted of four counts of mail fraud, two counts of wire fraud, one count of conspiracy to gain unauthorized access to a protected computer to obtain information, one count of making false statements to an FBI agent, three counts of subscribing to a false tax return, and four counts of making false statements to the IRS about his foreign assets.

According to court documents, Shih defrauded a U.S. company that manufactured broadband, high-powered semiconductor chips known as monolithic microwave integrated circuits (MMICs) out of its confidential and proprietary business information that was part of its MMIC manufacturing services, according to trial evidence. As part of the scheme, Shih accessed the victim company's web portal after obtaining that access through an associate who posed as a domestic customer seeking to obtain custom-designed MMICs that would be used solely in the United States. In this way, Shih concealed his true intent to export the U.S. company's MMICs to the People's Republic of China.

The victim company's semiconductor chips have several commercial and military applications. MMICs are used in missiles, missile guidance systems, fighter jets, electronic warfare, electronic warfare countermeasures and radar applications. The MMICs Shih exported to China were intended for AVIC 607, a state-owned entity in the PRC.

Shih was the President of Chengdu GaStone Technology Company (CGTC), a Chinese company that was building a MMIC manufacturing facility in Chengdu. In 2014, CGTC was placed on the Commerce Department's Entity List, according to court documents, "due to its involvement in activities contrary to the national security and foreign policy interest of the United States – specifically, that it had been involved in the illicit procurement of commodities and items for unauthorized military end use in China."

*(*Continued On The Following Column)*

Shih used a Hollywood Hills-based company he controlled – Pullman Lane Productions, LLC – to funnel funds provided by Chinese entities to finance the manufacturing of the MMICs by the victim company. Pullman Lane received financing from a Beijing-based company that was placed on the Entity List the same day as CGTC "on the basis of its involvement in activities contrary to the national security and foreign policy interests of the United States," according to court documents.

Shih's associate, Kiet Mai, pleaded guilty in December 2018 to one felony count of smuggling and was sentenced to 18 months' probation and a $5,000 fine.

Acting Assistant Attorney General Mark Lesko of the Justice Department's National Security Division and Acting U.S. Attorney Tracy Wilkison for the Central District of California made the announcement. The FBI, the U.S. Department of Commerce's Bureau of Industry and Security Office of Export Enforcement, and IRS Criminal Investigation investigated the case, with valuable assistance provided by the Royal Canadian Mounted Police.

Assistant U.S. Attorneys Judith A. Heinz, Melanie Sartoris, Khaldoun Shobaki, William M. Rollins, James C. Hughes and Daniel G. Boyle of the Central District of California prosecuted the case with assistance from Elizabeth Cannon, Deputy Chief of the National Security Division's Counterintelligence and Export Control Section.

## Imposing Sanctions in Defense of Human Rights Syria

Antony J. Blinken, Secretary of State

The United States is taking action to promote accountability for entities and individuals that have perpetuated the suffering of the Syrian people. The United States is sanctioning eight Syrian prisons, five Assad regime officials in the institutions that run those facilities, two militia groups, and two militia leaders. These actions underscore the U.S. commitment to promote respect for human rights and accountability for abuse against Syrians.

Many of the prisons designated today were highlighted in the pictures provided by Caesar, a Syrian regime defector who worked as an official photographer for the Syrian military and exposed the regime's ruthless and cruel treatment of detainees. Today's action furthers the goals of the Act named after him, the Caesar Syria Civilian Protection Act of 2019, which seeks to promote accountability for the Assad regime's abuses.

**Continue Here**

## Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research

A federal grand jury in San Diego, California, returned an indictment in May charging four nationals and residents of the People's Republic of China with a campaign to hack into the computer systems of dozens of victim companies, universities and government entities in the United States and abroad between 2011 and 2018. The indictment, which was unsealed on Friday, alleges that much of the conspiracy's theft was focused on information that was of significant economic benefit to China's companies and commercial sectors, including information that would allow the circumvention of lengthy and resource-intensive research and development processes. The defendants and their Hainan State Security Department (HSSD) conspirators sought to obfuscate the Chinese government's role in such theft by establishing a front company, Hainan Xiandun Technology Development Co., Ltd. (海南仙盾) (Hainan Xiandun), since disbanded, to operate out of Haikou, Hainan Province.

The two-count indictment alleges that Ding Xiaoyang (丁晓阳), Cheng Qingmin (程庆民) and Zhu Yunmin (朱允敏), were HSSD officers responsible for coordinating, facilitating and managing computer hackers and linguists at Hainan Xiandun and other MSS front companies to conduct hacking for the benefit of China and its state-owned and sponsored instrumentalities. The indictment alleges that Wu Shurong (吴淑荣) was a computer hacker who, as part of his job duties at Hainan Xiandun, created malware, hacked into computer systems operated by foreign governments, companies and universities, and supervised other Hainan Xiandun hackers.

The conspiracy's hacking campaign targeted victims in the United States, Austria, Cambodia, Canada, Germany, Indonesia, Malaysia, Norway, Saudi Arabia, South Africa, Switzerland and the United Kingdom. Targeted industries included, among others, aviation, defense, education, government, health care, biopharmaceutical and maritime. Stolen trade secrets and confidential business information included, among other things, sensitive technologies used for submersibles and autonomous vehicles, specialty chemical formulas, commercial aircraft servicing, proprietary genetic-sequencing technology and data, and foreign information to support China's efforts to secure contracts for state-owned enterprises within the targeted country (e.g., large-scale high-speed railway development projects).

*(*Continued On The Following Column)*

As alleged, the charged MSS officers coordinated with staff and professors at various universities in Hainan and elsewhere in China to further the conspiracy's goals. Not only did such universities assist the MSS in identifying and recruiting hackers and linguists to penetrate and steal from the computer networks of targeted entities, including peers at many foreign universities, but personnel at one identified Hainan-based university also helped support and manage Hainan Xiandun as a front company, including through payroll, benefits and a mailing address. "These criminal charges once again highlight that China continues to use cyber-enabled attacks to steal what other countries make, in flagrant disregard of its bilateral and multilateral commitments," said Deputy Attorney General Lisa O. Monaco. "The breadth and duration of China's hacking campaigns, including these efforts targeting a dozen countries across sectors ranging from healthcare and biomedical research to aviation and defense, remind us that no country or industry is safe. Today's international condemnation shows that the world wants fair rules, where countries invest in innovation, not theft."

"The FBI, alongside our federal and international partners, remains committed to imposing risk and consequences on these malicious cyber actors here in the U.S. and abroad," said Deputy Director Paul M. Abbate of the FBI. "We will not allow the Chinese government to continue to use these tactics to obtain unfair economic advantage for its companies and commercial sectors through criminal intrusion and theft. With these types of actions, the Chinese government continues to undercut its own claims of being a trusted and effective partner in the international community."

"This indictment alleges a worldwide hacking and economic espionage campaign led by the government of China," said Acting U.S. Attorney Randy Grossman for the Southern District of California. "The defendants include foreign intelligence officials who orchestrated the alleged offenses, and the indictment demonstrates how China's government made a deliberate choice to cheat and steal instead of innovate. These offenses threaten our economy and national security, and this prosecution reflects the Department of Justice's commitment and ability to hold individuals and nations accountable for stealing the ideas and intellectual achievements of our nation's best and brightest people."

"The FBI's San Diego Field Office is committed to protecting the people of the United States and the community of San Diego, to include our universities, health care systems, research institutes, and defense contractors," said Special Agent in Charge Suzanne Turner of the FBI's San Diego Field Office. "The charges outlined today demonstrate China's continued, persistent computer intrusion efforts, which will not be tolerated here or abroad. We stand steadfast with our law enforcement partners in the United States and around the world and will continue to hold accountable those who commit economic espionage and theft of intellectual property."

*(*Continued On The Following Page)*

The defendants' activity had been previously identified by private sector security researchers, who have referred to the group as Advanced Persistent Threat (APT) 40, BRONZE, MOHAWK, FEVERDREAM, G0065, Gadolinium, GreenCrash, Hellsing, Kryptonite Panda, Leviathan, Mudcarp, Periscope, Temp.Periscope and Temp.Jumper.

According to the indictment, to gain initial access to victim networks, the conspiracy sent fraudulent spearphishing emails, that were buttressed by fictitious online profiles and contained links to doppelgänger domain names, which were created to mimic or resemble the domains of legitimate companies. In some instances, the conspiracy used hijacked credentials, and the access they provided, to launch spearphishing campaigns against other users within the same victim entity or at other targeted entities. The conspiracy also used multiple and evolving sets of sophisticated malware, including both publicly available and customized malware, to obtain, expand and maintain unauthorized access to victim computers and networks. The conspiracy's malware included those identified by security researchers as BADFLICK, aka GreenCrash; PHOTO, aka Derusbi; MURKYTOP, aka mt.exe; and HOMEFRY, aka dp.dll. Such malware allowed for initial and continued intrusions into victim systems, lateral movement within a system, and theft of credentials, including administrator passwords.

The conspiracy often used anonymizer services, such as The Onion Router (TOR), to access malware on victim networks and manage their hacking infrastructure, including servers, domains and email accounts. The conspiracy further attempted to obscure its hacking activities through other third-party services. For example, the conspiracy used GitHub to both store malware and stolen data, which was concealed using steganography. The conspiracy also used Dropbox Application Programming Interface (API) keys in commands to upload stolen data directly to conspiracy-controlled Dropbox accounts to make it appear to network defenders that such data exfiltration was an employee's legitimate use of the Dropbox service.

*(*Continued On The Following Column)*

"Don't expect to see a change if you don't make one."

Coinciding with today's announcement, to enhance private sector network defense efforts against the conspirators, the FBI and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) released a Joint Cybersecurity Advisory containing these and further technical details, indicators of compromise and mitigation measures.

The defendants are each charged with one count of conspiracy to commit computer fraud, which carries a maximum sentence of five years in prison, and one count of conspiracy to commit economic espionage, which carries a maximum sentence of 15 years in prison. The maximum potential sentences in this case are prescribed by Congress and are provided here for informational purposes only, as any sentencings of the defendants will be determined by the assigned judge.

The investigation was conducted jointly by the U.S. Attorney's Office for the Southern District of California, the National Security Division's Counterintelligence and Export Controls Section, and the FBI's San Diego Field Office. The FBI's Cyber Division, Cyber Assistant Legal Attachés and Legal Attachés in countries around the world provided essential support. Numerous victims cooperated and provided valuable assistance in the investigation.

Assistant U.S. Attorneys Fred Sheppard and Sabrina Feve of the Southern District of California and Trial Attorney Matthew McKenzie of the National Security Division's Counterintelligence and Export Control Section are prosecuting this case.