



EIB World Trade Headlines

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

October 1, 2020 - Volume 12, Issue 17



Commerce Department Statement on U.S. District Court Ruling on TikTok Preliminary Injunction

FOR IMMEDIATE RELEASE
Sunday, September 27, 2020

News Media Contact:
Office of Public Affairs, 202-482-4883

Commerce Department Statement on U.S. District Court Ruling on TikTok
Preliminary Injunction

WASHINGTON – On September 27, 2020, the United States District Court for the District of Columbia granted a nationwide preliminary injunction against the implementation of Executive Order (E.O.) 13942, limited to the Secretary of Commerce’s Identification of Prohibited Transactions with TikTok/ByteDance involving ‘any provision of services... to distribute or maintain the TikTok mobile application, constituent code, or application updates through an online mobile application store.’ The E.O. is fully consistent with the law and promotes legitimate national security interests. The Government will comply with the injunction and has taken immediate steps to do so, but intends to vigorously defend the E.O. and the Secretary’s implementation efforts from legal challenges.

NEWSLETTER NOTES

- * Commerce Department Statement on ...
- * V-Shaped Germany
- * “Buy American” ...
- * Soldier who helped save 70 captives...
- * Boeing 737 Max ...
- * Federal Reserve sees rates nea...
- * Settlement Agreement ...
- * Treasury Sanctions Russia-Linked ...
- * Commerce Department Prohibits ...
- * EU companies selling surveillance ...
- * Commerce Adds Five Scientists ...
- * Bucks County Man Indicted for ...
- * U.S. Places Restrictions on China’s Leading Chip Maker

V-Shaped Germany

If any country has managed to weather the economic chaos of 2020, it would appear to be Germany. As Morgan Stanley's Ruchir Sharma told Fareed recently, years of fiscal discipline supplied leeway for emergency measures, setting up the country as a possible winner (in the relative sense) amid Covid-19's depredations.

That prediction is coming true, according to Christian Reiermann's report in Der Spiegel this week. German Economic Minister Peter Altmaier unfurled a literally "v"-shaped forecast graph on Sept. 1, and Reiermann writes that "Berlin reacted quickly and decisively to the crisis and mobilized more money, as a share of GDP, than any other country in the world. More than 1 trillion euros were made available ... around one-third of the country's annual gross domestic product." (By comparison, the US mobilized \$3.6 trillion, good for a nearly 17% Covid-19-stimulus-to-GDP ratio. Those figures do not include the activity of central banks, which have been busy buying up assets and injecting trillions of monetary stimulus on their own.) Germany's efforts have included expanded compensation to companies covering a portion of furloughed workers' salaries—a program just extended by another year—and grants to small businesses and the self-employed.

"The result has been rather incredible," Reiermann writes. "Although gross domestic product ... shrank by almost 10 percent during the second quarter, disposable incomes fell by only 0.8 percent. The federal government followed an old economic policy recipe: When companies and workers are weakened in a downturn because of shrinking income, the state jumps in to try to boost demand." Which it could afford to do: "During the first half of 2020, fiscal authorities in Germany recorded a deficit of 3.2 percent of GDP ... Other countries run deficits of a similar magnitude even during normal times. But because Germany has been generating budget surpluses for years, federal and state governments were able to go all out."

Not everything is working perfectly. A reduction in the country's VAT tax is unlikely to be passed onto consumers in full, Reiermann writes. Accounting delays may have only forestalled bankruptcies. But given the global state of ruin, a "v"-shaped forecast doesn't sound so bad.

"Buy American" (Again): New Executive Order Requires Changes (By 2020)

This is not our forte, so at the bottom of this article there is a company you can reach out to that seems to have the required expertise.- Jeanette Reed, Evolutions in Business

By David Gallacher on July 31, 2019 Posted in BAA and TAA, Country of Origin, Domestic Preferences, Executive Orders
On July 15, 2019, President Trump signed an Executive Order requiring regulations implementing the Buy American Act, 41 U.S.C. §§ 8301-8305, to be changed. While President Trump has previously issued two other policy-based "Buy American" Executive Orders, this new Order directs that specific changes be made, reversing government policies that have been in place for 65 years. These changes have the potential to significantly disrupt many government contractors' supply chains and internal compliance programs. As such, companies should start planning now for the final regulations that are expected sometime in 2020.

The Buy American Act (BAA)

Subject to multiple exceptions (some of which are discussed below), the BAA requires the government to purchase products "manufactured in the United States substantially all from articles, materials, or supplies mined, produced, or manufactured in the United States." 41 U.S.C. § 8302(a)(1). The Federal Acquisition Regulation ("FAR") has interpreted this statutory requirement by requiring a "domestic end product" to meet a two part test: (i) the end product must be manufactured in the United States; and (ii) at least 50% of the cost of the components must also be of U.S. origin. FAR 25.003. This second part is commonly referred to as the "component test." The 50% threshold for the "component test" dates back to the Eisenhower administration and a 1954 Executive Order (E.O. 10582), which interpreted the phrase "substantially all" to mean at least 50%. But, of course, the phrase is open to interpretation.

Summary of New Executive Order

The new Executive Order 13811, "Maximizing Use of American-Made Goods, Products, and Materials," (the "Order") interprets the statute differently. Unlike the two prior Trump Executive Orders (discussed here and here), which mainly made broad policy statements and asked government agencies to assess what they could do to improve efforts to "Buy American," this new Order largely revokes the Eisenhower Executive Order and directs the FAR Council to change the regulations in at least two key ways:

*(*Continued On The Following Page)*

1. The “Component Test.” The Order directs the thresholds under the “component test” to be increased, splitting out separate requirements for “iron and steel end products” and “all other end products.”

	Current Test: U.S. Origin Components by Cost	Future Test: U.S. Origin Parts or Materials
Iron and Steel end products	≥ 50%	≥ 95%
Other end products	≥ 50%	≥ 55%

A few key points are worth highlighting about this new rubric:

- Components vs. Products. The terms used in the Order do not line up precisely with the definitions used in the FAR. The FAR speaks in terms of “components” and “cost of components” (FAR 25.003), while the Order speaks in terms of “products used in” an end product and the associated costs. These are not necessarily the same thing – a “component” is different from a subcomponent, and many U.S. manufacturers have been able to meet the BAA requirements by converting foreign-origin materials and subcomponents into a U.S. origin “component” by performing intermediate manufacturing steps in the U.S. The FAR Council may ultimately reconcile the various terms and apply the commonly understood “component” definition already in place. But, then again, maybe they won’t.
- Another Love Letter to Domestic Iron & Steel. The radical increase in the iron and steel threshold now puts the Buy American Act on par with the Buy America (no “n”) Act, 49 U.S.C. § 5323(j); 23 U.S.C. § 313, which requires iron and steel of completely U.S. origin on transportation, highway, and infrastructure projects. Why the difference? Well, remember that the BAA requires only that the iron or steel be “substantially all” of U.S. origin, leaving a little daylight for some foreign content. As has been seen with the President’s tariffs on steel and aluminum (discussed here), the President loves domestic metals. And, much like Spinal Tap, the President seems committed to “turning it up to 11.”
- Up, Up and Away? The Order asks the FAR Council to consider whether the thresholds should be raised even further, potentially as high as 75% for “other end products.” (As noted above, the 95% threshold for iron and steel is probably as high as it can get). The Order suggests that the threshold might be raised, even incrementally, “based on the feasibility and desirability” of any such changes. We can take some small comfort that changes greater than 55% won’t happen immediately; but industry will live under the specter of an increasingly tougher standard that might incrementally slide over the course of several years. Such a result would not lead to the regulatory predictability that industry prefers.

*(*Continued On The Following Column)*

2. The “Evaluation Factor.” One of the most widely used exceptions to the BAA is when the domestic end product is unreasonably expensive compared to a foreign product. FAR 25.103(c); 25.202(a)(3). As such, the BAA does not – strictly speaking – require the government to “Buy American.” It merely encourages the government to “Buy American.” When comparing offers that propose delivering domestic and foreign end products, the FAR directs the government to apply an evaluation factor in favor of domestic end products, inflating (for price comparison purposes) the evaluated cost of the foreign product. The chart below summarizes the current and future evaluation factors:

	Current Evaluation Factor	Future Evaluation Factor
Large Business Offerors (FAR 25.105(b)(1))	6%	20%
Small Business Offerors (FAR 25.105(b)(2))	12%	30%
DOD Contractors (DFARS 225.105(b))	50%	50%

The process by which these evaluation factors are applied is set forth in FAR Subpart 25.5. It is not simple, but (in a nutshell) it works something like this:

- Assume that the government calls for proposals for the delivery of 1,000 widgets; the RFP calls for a lowest price/technically acceptable procurement.
- Assume that Company A offers \$100 per widget for a total proposed price of \$100,000. These widgets were all manufactured in China.
- Assume that Company B offers \$110 per widget for a total proposed price of \$110,000. These widgets were all manufactured in the United States.
- Using the current evaluation factors (assuming Company B is a large business), Company A’s proposed price would be inflated by 6%. Company A’s evaluated price would be \$106,000; Company B’s evaluated price would be \$110,000. Company A, as the lowest evaluated price offeror, would receive the \$100,000 award, notwithstanding the fact that Company A is delivering foreign-made products.
- Using the current evaluation factors (and assuming that Company B is a small business), then Company A’s proposed price would be inflated by 12%. Company A’s evaluated price would be \$112,000; Company B’s evaluated price would be \$110,000. Company B, as the lowest evaluated price offeror, would receive the \$110,000 award, notwithstanding the fact that it’s actual proposed price was higher.
- Using the Order’s new evaluation factors, Company B would win in practically every scenario. In fact, Company B’s price could be as high as nearly \$120-\$130 per widget (compared to the foreign alternatives priced at \$100), and Company B could still be considered the lowest price offer. What this means practically is that foreign-made products will now need to be significantly cheaper than the domestic alternatives in order for the government to be able to buy under the BAA.

*(*Continued On The Following Page)*

3. "To The Maximum Lawful Extent." The Order encourages the FAR Council to update the BAA regulations "to most effectively carry out the goals of the Buy American Act and [the] Administration's policy of enforcing the Buy American Act to its maximum lawful extent." It also calls for government agencies to make recommendations by January 2020 for other ways that the regulations may be changed. One area that the FAR Council is directed to look into (as discussed above) is incremental increases to the costs of components under the "component test." But other issues may also be considered by the FAR Council, even though they are not expressly spelled out in the Order. For example:

- Will the exception to the "component test" for commercial off-the-shelf ("COTS") products continue? Currently, COTS products need only meet the first prong of the BAA – the end product must be manufactured in the United States. FAR 25.100(a)(3). 41 U.S.C. § 1907 authorizes the FAR Council to streamline federal procurements, determining that certain normal requirements will not apply to purchases of COTS products. Back in 2009, the FAR Council exempted COTS products from the "component test. But who's to say that the policy winds haven't shifted? The FAR Council could easily reverse the 2009 decision, which would impose a massive (and unwelcome) regulatory burden on COTS vendors.
- Will the exception for commercial information technology continue? Currently, the government can purchase "information technology" (a broad term defined under FAR 2.101) that is a "commercial item" (another broad term) without regard to the BAA. FAR 25.103(e) and 25.202(a)(4). This is a statutory requirement (Section 535, Pub. L. No. 108-199), so the FAR Council may have less latitude in limiting this exception. Nonetheless, where the commercial IT exception allows the government to buy massive amounts of foreign-made products, and where the Order's priorities are clear, the FAR Council may narrow the scope of this commonly used exception.
- Will the processes be tightened for obtaining "public interest" or "nonavailability" waivers? The FAR sets forth the process by which these two types of exceptions can be invoked. FAR 25.103(a) and (b); 25.202(a)(1) and (2). The process is already: (i) involved; (ii) invoked at high levels; and (iii) subject to extra scrutiny. The FAR Council could easily add other hurdles to these processes, requiring more public notice and more public comment, all of which tamp down on a contracting officer's willingness to purchase products that are not domestically manufactured. Moreover, the FAR Council could also require agencies to reassess previously issued nonavailability determinations, applying the new standards.

*(*Continued On The Following Column)*

Timeline for Changes

The Order instructs the FAR Council to issue a proposed rule for public comment within 180 days, which corresponds roughly with January 11, 2020. Once public comments have been received and evaluated, the FAR Council is required to "promptly" issue a final rule. Those familiar with the rulemaking process may scoff at the idea that anything can (or even will) happen "promptly." Nonetheless, this timeline seems to indicate that new, final rules may be in effect as early as Spring 2020. And, of course, this timeline could be accelerated even further if the FAR Council decides to issue an interim rule instead of a proposed rule. Such an interim step is unlikely, to be sure, but the language of the Order does not expressly rule this out.

Conclusion

It goes without saying that contractors are well-advised to continue closely monitoring country of origin requirements in their contracts, and ensuring that the products purchased through the supply chain match the contract requirements. With regard to the pending changes to the BAA:

- Companies can start by identifying their contracts that include the Buy American Act, as opposed to contracts that include the Trade Agreements Act ("TAA"), FAR 52.225-5. While these clauses are often lumped together by some companies in their compliance programs, the two statutes impose distinct compliance obligations. But the Order affects only the BAA – not TAA. So if your contract is not subject to the BAA, then you probably have less to worry about.
- Manufacturers can start by looking at their supply chain, assessing whether there are any end products that are "close" under the new component threshold (in the 50-55% domestic content range) and that may need to be adjusted to ensure compliance in 2020.
- Manufacturers may also begin considering whether there are changes to their manufacturing processes, where they can bring more manufacturing into the U.S. in order to better meet the various legal requirements. (But remember... even though NAFTA or the U.S.-Mexico-Canada Agreement may or may not be in place next month, these free trade agreements do not apply to the Buy American Act unless the contracts exceed certain dollar thresholds set by the U.S. Trade Representative. FAR 25.402).
- Resellers can start by reviewing their list of suppliers and products, identifying potentially problematic products that may qualify under the BAA today, but may not qualify under the new rules. If a product is a "close call," it simply might not be worth the potential risk of selling to the government in an era where "Buy American" is something that everyone is watching more closely.

*(*Continued On The Following Page)*

Hopefully, whatever rules are ultimately proposed will follow the Order as closely as possible, will hew to the existing rubrics and definitions currently used in FAR Part 25, and will limit the erosion of other exceptions (many of which industry has come to rely on). Hopefully, the public comments will be heard and implemented in an even-handed manner. While we all support the *idea* of “Buy American,” the simple fact is that in this modern, international economy, every product has *something* in it that is foreign. Forcing the government to pay astronomical prices for commercially available products simply makes no sense; let’s hope that a little balance can be measured throughout the “Buy American” rally cry.

[Tweet](#) [Like](#) [Email](#) [LinkedIn](#)

Print

Tags: [BAA](#), [Buy American Act](#)

This alert is provided for information purposes only and does not constitute legal advice and is not intended to form an attorney client relationship. Please contact your Sheppard Mullin attorney contact for additional information.

Soldier who helped save 70 captives from execution by Islamic State receives Medal of Honor

Army Sgt. Maj. Thomas Payne is the first service member to receive the honor for actions in the fight against the Islamic State. Payne, who enlisted months after the Sept. 11 terrorist attacks, has served on 17 deployments.

Boeing 737 Max crashes were ‘horrific culmination’ of errors, investigators say

The chief project engineer for Boeing’s 737 Max jet told House investigators that he approved a critical design change to software on the plane even though he was unaware of key details about how it worked or of a previous warning from a test pilot that if the system malfunctioned, the results could be “catastrophic.”

A new comprehensive report released Wednesday by the House Transportation Committee also says that the crashes of two new 737 Max aircraft in less than five months “were the horrific culmination of a series of faulty technical assumptions by Boeing’s engineers, a lack of transparency on the part of Boeing’s management, and grossly insufficient oversight by the FAA.”

Federal Reserve sees rates near zero at least through 2023

WASHINGTON (AP) — The Federal Reserve expects to keep its benchmark interest rate pegged near zero at least through 2023 as it strives to accelerate economic growth and drive down the unemployment rate.

The central bank also said Wednesday that it will seek to push inflation above 2% annually. The Fed left its benchmark short-term rate unchanged at nearly zero, where it has been since the pandemic intensified in March.

The Fed’s benchmark interest rate influences borrowing costs for home buyers, credit card users, and businesses. Fed policy makers hope an extended period of low interest rates will encourage more borrowing and spending, though their new policy also carries risks of inflating stock or causing other financial market bubbles.

Settlement Agreement between the U.S. Department of the Treasury’s Office of Foreign Assets Control and Comtech Telecommunications Corp.

The U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) today announced a \$894,111 settlement with Comtech Telecommunications Corp. (“Comtech”), based in Melville, New York, and its wholly-owned subsidiary, Comtech EF Data Corp. (“EF Data”), headquartered in Tempe, Arizona. Comtech, a company specializing in the sales of advanced communications systems, software, and services, has agreed to settle its potential civil liability for four apparent violations of the Sudanese Sanctions Regulations, 31 C.F.R. part 538 (SSR). Specifically, between June 2014 and October 2015, Comtech, through its subsidiary EF Data, indirectly exported warrantied satellite equipment and facilitated services and training to a government-owned entity in Sudan in apparent violation of the SSR. OFAC determined that Comtech voluntarily disclosed the apparent violations and that the apparent violations constituted an egregious case.

Treasury Sanctions Russia-Linked Election Interference Actors

September 10, 2020

Washington – Today, the Department of the Treasury’s Office of Foreign Assets Control (OFAC) designated four Russia-linked individuals for attempting to influence the U.S. electoral process. Russia uses a variety of proxies to attempt to sow discord between political parties and drive internal divisions to influence voters as part of Moscow’s broader efforts to undermine democratic countries and institutions. In the United States, Russia has used a wide range of influence methods and actors to target our electoral process, including targeting U.S. presidential candidates.

Treasury designated Andrii Derkach (Derkach) pursuant to Executive Order (E.O.) 13848 for his efforts to influence the 2020 U.S. presidential election. Derkach, a Member of the Ukrainian Parliament, has been an active Russian agent for over a decade, maintaining close connections with the Russian Intelligence Services. Derkach has directly or indirectly engaged in, sponsored, concealed, or otherwise been complicit in foreign interference in an attempt to undermine the upcoming 2020 U.S. presidential election. Today’s designation of Derkach is focused on exposing Russian malign influence campaigns and protecting our upcoming elections from foreign interference. This action is a clear signal to Moscow and its proxies that this activity will not be tolerated. The Administration is working across the U.S. Government, and with state, local, and private sector partners, to make the 2020 election secure.

“Andrii Derkach and other Russian agents employ manipulation and deceit to attempt to influence elections in the United States and elsewhere around the world,” said Secretary Steven T. Mnuchin. “The United States will continue to use all the tools at its disposal to counter these Russian disinformation campaigns and uphold the integrity of our election system.”

Derkach’s Election Influence Efforts

From at least late 2019 through mid-2020, Derkach waged a covert influence campaign centered on cultivating false and unsubstantiated narratives concerning U.S. officials in the upcoming 2020 Presidential Election, spurring corruption investigations in both Ukraine and the United States designed to culminate prior to election day. Derkach’s unsubstantiated narratives were pushed in Western media through coverage of press conferences and other news events, including interviews and statements.

*(*Continued On The Following Column)*

Between May and July 2020, Derkach released edited audio tapes and other unsupported information with the intent to discredit U.S. officials, and he levied unsubstantiated allegations against U.S. and international political figures. Derkach almost certainly targeted the U.S. voting populace, prominent U.S. persons, and members of the U.S. government, based on his reliance on U.S. platforms, English-language documents and videos, and pro-Russian lobbyists in the United States used to propagate his claims.

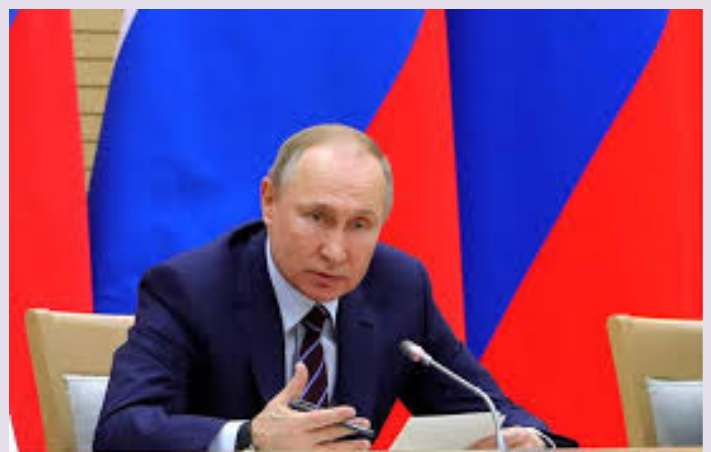
Treasury Continues to Hold Russian Actors Accountable

Today’s designation of Derkach is another example of the Treasury department promoting accountability for Kremlin-linked individuals seeking to undermine confidence in U.S. democratic processes. Treasury has previously designated the Russian troll factory known as the Internet Research Agency (IRA), and its Russian financier Yevgeniy Prigozhin. Prigozhin has been designated by the United States pursuant to E.O. 13661, E.O. 13694, as amended, and most recently by E.O. 13848 for providing material support to the IRA’s influence activities against the 2018 U.S. midterm elections.

Today, Treasury also designated three IRA actors pursuant to E.O. 13694, as amended by E.O. 13757, and E.O. 13848 for having acted or purported to act for or on behalf of, directly or indirectly, the IRA, an entity designated pursuant to E.O. 13694, as amended, and E.O. 13848. Russian nationals Artem Lifshits, Anton Andreyev, and Darya Aslanova, as employees of the IRA, supported the IRA’s cryptocurrency accounts. The IRA uses cryptocurrency to fund activities in furtherance of their ongoing malign influence operations around the world.

OFAC coordinated today’s action against the IRA with the U.S. Attorney’s Office for the Eastern District of Virginia and the United States Secret Service.

As a result of today’s designations, all property and interests in property of these targets that are subject to U.S. jurisdiction are blocked, and U.S. persons are generally prohibited from engaging in transactions with them. Additionally, any entities 50 percent or more owned by one or more designated persons are also blocked.



Commerce Department Prohibits WeChat and TikTok Transactions to Protect the National Security of the United States

FOR IMMEDIATE RELEASE
Friday, September 18, 2020

News Media Contact:
Office of Public Affairs, 202-482-4883

WASHINGTON – In response to President Trump’s Executive Orders signed August 6, 2020, the Department of Commerce (Commerce) today announced prohibitions on transactions relating to mobile applications (apps) WeChat and TikTok to safeguard the national security of the United States. The Chinese Communist Party (CCP) has demonstrated the means and motives to use these apps to threaten the national security, foreign policy, and the economy of the U.S. Today’s announced prohibitions, when combined, protect users in the U.S. by eliminating access to these applications and significantly reducing their functionality.

“Today’s actions prove once again that President Trump will do everything in his power to guarantee our national security and protect Americans from the threats of the Chinese Communist Party,” said U.S. Department of Commerce Secretary Wilbur Ross. “At the President’s direction, we have taken significant action to combat China’s malicious collection of American citizens’ personal data, while promoting our national values, democratic rules-based norms, and aggressive enforcement of U.S. laws and regulations.”

While the threats posed by WeChat and TikTok are not identical, they are similar. Each collects vast swaths of data from users, including network activity, location data, and browsing and search histories. Each is an active participant in China’s civil-military fusion and is subject to mandatory cooperation with the intelligence services of the CCP. This combination results in the use of WeChat and TikTok creating unacceptable risks to our national security.

As of September 20, 2020, the following transactions are prohibited:

Any provision of service to distribute or maintain the WeChat or TikTok mobile applications, constituent code, or application updates through an online mobile application store in the U.S.;

Any provision of services through the WeChat mobile application for the purpose of transferring funds or processing payments within the U.S.

*(*Continued On The Following Column)*

As of September 20, 2020, for WeChat and as of November 12, 2020, for TikTok, the following transactions are prohibited:

Any provision of internet hosting services enabling the functioning or optimization of the mobile application in the U.S.;

Any provision of content delivery network services enabling the functioning or optimization of the mobile application in the U.S.;

Any provision directly contracted or arranged internet transit or peering services enabling the function or optimization of the mobile application within the U.S.;

Any utilization of the mobile application’s constituent code, functions, or services in the functioning of software or services developed and/or accessible within the U.S.

Any other prohibitive transaction relating to WeChat or TikTok may be identified at a future date. Should the U.S. Government determine that WeChat’s or TikTok’s illicit behavior is being replicated by another app somehow outside the scope of these executive orders, the President has the authority to consider whether additional orders may be appropriate to address such activities. The President has provided until November 12 for the national security concerns posed by TikTok to be resolved. If they are, the prohibitions in this order may be lifted.

The notices for these actions will be posted on the Federal Register at approximately 8:45AM EDT on Friday, September 18, 2020.

Background:

On August 6, 2020, President Trump signed Executive Orders (E.O.) 13942, Addressing the Threat Posed by TikTok, and E.O. 13943, Addressing the Threat Posed by WeChat. In the E.O.s, the President determined that the apps capture vast swaths of information from U.S. users, leaving the data vulnerable to CCP access for nefarious purposes. Commerce, at the Direction of the President, was required to identify transactions within 45 days to protect national security and the private data of millions of people across the country. Today’s announced prohibitions fulfill the President’s direction and mitigate national security risks.



EU companies selling surveillance tools to China's human rights abusers

Amnesty International found that three companies based in France, Sweden and the Netherlands sold digital surveillance systems, such as facial recognition technology and network cameras, to key players of the Chinese mass surveillance apparatus. In some cases, the export was directly for use in China's indiscriminate mass surveillance programmes, with the risk of being used against Uyghurs and other predominantly Muslim ethnic groups throughout the country.

Most EU governments, including France and Sweden, are resisting calls to strengthen export rules to include strong human rights safeguards in biometric surveillance technology, an area that European companies dominate. Germany, which has held the EU presidency since 1 July, and the Netherlands have both expressed the need for stronger human rights safeguards in the past but have so far failed to address this successfully at EU level.

"Europe's biometric surveillance industry is out of control. Our revelations of sales to Chinese security agencies and research institutions that support them are just the tip of the iceberg of a multi-billion Euro industry that is flourishing by selling its wares to human rights abusers, with few safeguards against end-use abuses," said Merel Koning, Senior Policy Officer, Technology and Human Rights at Amnesty International.

Across China, mass surveillance projects such as "Skynet" and "Sharp Eyes" are being rolled out to keep people under constant observation. China's public security agencies are key players in developing this unprecedented expansion of surveillance. Biometric surveillance is ubiquitous in northwest China's Xinjiang Uyghur Autonomous Region, where an estimated up to one million Uyghurs and members of other ethnic groups have been arbitrarily held captive in so-called "re-education camps".

"EU governments' condemnation of the systematic repression in Xinjiang rings hollow if they continue to allow companies to sell the very technology that could be enabling these abuses. The current EU export regulation system is broken and needs fixing fast," said Merel Koning.

Biometric surveillance tools, including facial recognition software, are among the most invasive digital surveillance technologies that enable governments to identify and track individuals in public spaces or single them out based on their physiological or behavioural characteristics. These technologies pose a clear threat to the rights to privacy, freedom of assembly, speech, religion and non-discrimination.

(*Continued On The Following Column)

Amnesty's investigation identified the sale of three different types of digital surveillance technologies to Chinese state security agencies, entities that contribute to the upholding of laws that violate human rights, as well as entities in Xinjiang.

Morpho, which is now part of Idemia, a French multinational, was awarded a contract to supply facial recognition equipment directly to the Shanghai Public Security Bureau in 2015. The company specializes in security and identity systems, including facial recognition systems and other biometric identification products. Amnesty International calls for a ban on the use, development, production, sale and export of facial recognition technology for identification purposes by both state agencies and private-sector actors. Amnesty's research found that Axis Communications, a Swedish company, even boasts on its website of its involvement in expanding the Chinese surveillance state. Axis develops and markets network cameras, which specialize in security surveillance and remote monitoring. The company has supplied its technology to China's public security apparatus and is repeatedly listed as a "recommended brand" in Chinese state surveillance tender documents dating from 2012 to 2019. The company's website states it expanded the network of security cameras from 8,000 to 30,000 in Guilin, a city in the south of China with a population of approximately 5 million people, as part of an upgrade of the city's Skynet surveillance programme. The cameras in the network have a 360-degree angle and a range of 300 to 400 metres, making it possible to track targets from all directions.

"Chinese public security agencies are using products sold by European companies to build up their abusive surveillance capacity. These companies are profiting from the sale of digital surveillance technologies that are linked to horrific human rights violations. The companies should have known full well that sales to China's authorities were of significant risk but apparently took no steps to prevent their products from being used and studied by human rights abusers. In so doing, they totally failed in their human rights responsibilities. This is why the EU legislature needs to act to stop similar abusive trade," said Merel Koning.

A Dutch company, Noldus Information Technology, sold emotion recognition systems to public security and law enforcement-related institutions in China. The company's "FaceReader" software is used for automated analysis of facial expressions that convey anger, happiness, sadness, surprise and disgust. FaceReader was found to be used by Chinese universities with links to the public security apparatus and the police, as well as by the Ministry of Public Security. China's legal system falls short of international standards in numerous respects and is often misused by the authorities to restrict human rights. Amnesty International also found that Noldus sold its digital surveillance technology to at least two universities in Xinjiang between 2012 and 2018. This included supplying its "The Observer XT" software to Shihezi University in 2012.

(*Continued On The Following Page)

The university falls under the administration of the Xinjiang Production and Construction Corps (XPCC). XPCC fulfils a special role “in safeguarding the country's unification and Xinjiang's social stability and in cracking down on violent terrorist crimes”.

In 2012, it was already known that the Chinese government routinely conflates Uyghur cultural and religious practice with terrorism. In the years that followed, the technological advancement of the suppression of minorities in Xinjiang became apparent, with emotion and behavioural analysis systems of particular interest to the Chinese authorities.

The investigated exports by the EU companies pose a significant risk to human rights. None of the companies provided Amnesty International with clear answers as to what due diligence was carried out before completing these sales. This is one of the reasons why the EU must take action now.

Amnesty's report illustrates the major shortcomings in the current export regulation framework of the EU, the Dual Use Regulation. Amnesty is calling on the EU legislature to include all digital surveillance technology under its export framework, strengthen human rights safeguards in export decisions and ensure all companies conduct a human rights impact assessment.

“In response to Amnesty International, Axis Communications said that they do not require a license for the export of cameras for use in Chinese mass surveillance programmes. This is exactly the problem of the current EU exports regulation framework. EU governments need to face up to their responsibilities and rein in this unchecked industry,” said Merel Koning.

“Until the EU does, they have serious questions to answer about their potential role in human rights violations perpetrated by the Chinese government.”



Commerce Adds Five Scientists Involved in Iran's Nuclear Weapons Development Program to the Entity List

FOR IMMEDIATE RELEASE
Monday, September 21, 2020

News Media Contact:
Office of Public Affairs, 202-482-4883

WASHINGTON – U.S. Secretary of Commerce Wilbur Ross today announced that the Department is adding five Iranian scientists to the Entity List for enabling or assisting Iran's nuclear development program, which is contrary to the national security and foreign policy interests of the United States. The individuals added to the Entity List are Ahmad Nozad Gholik, Behnam Pouremadi, Hamid Sepehrian, Mojtaba Farhadi Ganjeh, and Sayyed Javad Ahmadi.

“These five individuals played a critical role in Iran's nuclear weapons development program and continue to work for the Iranian regime. Iran must comply with its nuclear safeguard obligations and immediately cooperate with the international community. Iran's nuclear escalation adds to destabilization in the region and the Iranian regime is a clear threat to international peace and security,” said Secretary Ross. “The Department of Commerce stands by President Trump in his commitment to preventing Iran from ever acquiring a nuclear weapon. We will continue to aggressively investigate and designate individuals and parties to the Entity List who act contrary to the national security of the United States and international law.”

Since 2017, Commerce has added more than 60 entities around the world to the Entity List for their involvement in activities that support Iran's missile, nuclear, WMD and other military programs.

Pursuant to Section 744.11(b) of the Export Administration Regulations (EAR), the Entity List identifies persons or organizations reasonably believed to be involved, or to pose a significant risk of being or becoming involved, in activities contrary to the national security or foreign policy interests of the United States. The EAR imposes additional license requirements on, and limits the availability of, most license exceptions for, exports, re-exports, and transfers (in-country) to listed entities.

Bucks County Man Indicted for Trafficking Firearms to St. Lucia

PHILADELPHIA – First Assistant United States Attorney Jennifer Arbittier Williams announced that Thomas Harris Jr., 27, of Croydon, PA was arrested and charged by Indictment with multiple firearms trafficking offenses stemming from his scheme to sell almost 40 guns to a buyer on the island of St. Lucia. Specifically, the defendant was charged with making false statements to a federal firearm licensee, dealing in firearms without a license, delivery of firearms to a common carrier without written notice, and smuggling goods from the United States.

The Indictment alleges that Harris purchased approximately 38 firearms in 12 transactions at two Bucks County, PA, gun shops between April 20, 2019, and February 15, 2020, and provided a false address as his place of residence on the required federal forms that he completed during each transaction. It is further alleged that the defendant then illegally trafficked, and attempted to traffic, the guns to St. Lucia, a sovereign island nation in the West Indies, despite his not having a license to deal in firearms nor a license to export them as required by law. He also allegedly failed to notify the shipping company he used that his shipments contained firearms, as required by law.

One of Harris's suspected packages to St. Lucia was intercepted by federal agents at the warehouse of a local shipping company. Inside, concealed in household items such as packages of diapers, cat litter and laundry detergent, the agents found seven Glock semiautomatic pistols, one Ruger semiautomatic pistol, two AK-47 pattern pistols, two AK-47 pattern rifles, two AR-15 lower receivers, two AR-15 upper receivers, ten high capacity Glock ammunition magazines, seven additional assorted ammunition magazines, and 815 rounds of ammunition. Harris allegedly used the alias "Lance Brown" when he presented this package to the shipping company for shipment to St. Lucia, and he allegedly falsely told a shipping company representative that the package contained household items. After the defendant left this package with the shippers, he traveled to St. Lucia himself in March 2020. He remained there until returning to the United States on July 25, 2020, when he was arrested at an airport in New York.

"As alleged in the Indictment charging him with firearms trafficking offenses, Harris has a brazen disrespect for our laws meant to regulate and monitor the sale of weapons," said First Assistant U.S. Attorney Williams. "After sending his most recent shipment of guns overseas he also left the country for a few months, but all that did was postpone the inevitable. If you are charged in the Eastern District of Pennsylvania with a federal offense, there is no place to hide, here or abroad. We will not rest until we find you and hold you accountable."

*(*Continued On The Following Column)*

"Illicit international firearms trafficking is a top priority for the Office of Export Enforcement," said P. Lee Smith, Performing the Non-exclusive Functions and Duties of the Assistant Secretary for Export Enforcement at the Department of Commerce. "We will continue to work with our law enforcement partners to arrest and prosecute individuals who violate United States export control laws that are intended to keep the most dangerous goods out of the most dangerous hands."

"Preventing the illegal use and trafficking of firearms is a central focus of ATF's strategy to combat violent crime and protect our communities," said John Schmidt, acting Special Agent in Charge of ATF's Philadelphia Field Division. "Illegally purchased firearms often end up in the hands of violent offenders and affect communities near and far, in this instance Saint Lucia in the Caribbean. Ensuring firearms traffickers are aggressively investigated and swiftly brought to justice is a top priority for the Philadelphia Field Division -- this collaborative effort between our local, state and federal partners is a prime example of such."

"If you want to be a firearms dealer and exporter, get the proper licenses and follow the law," said Michael J. Driscoll, Special Agent in Charge of the FBI's Philadelphia Division. "Guns illegally exported overseas are quite likely to end up in the wrong hands and be used to commit further criminal acts. The FBI is committed to working with our law enforcement partners to combat weapons trafficking, in the interests of public safety here and abroad."

If convicted, the defendant faces a maximum possible sentence of 80 years in prison, three years of supervised release, a \$3,750,000 fine, and a \$1,500 special assessment.

The case was investigated by the U.S. Department of Commerce, Office of Export Enforcement, New York Field Office; the Bureau of Alcohol, Tobacco, Firearms, and Explosives; and the Federal Bureau of Investigation, and is being prosecuted by Assistant United States Attorney Joseph A. LaBar and U.S. Department of Justice National Security Division Trial Attorney Michael E. Eaton.

An indictment, information, or criminal complaint is an accusation. A defendant is presumed innocent unless and until proven guilty.

Topic(s):

Firearms Offenses

Component(s):

USAO - Pennsylvania, Eastern

Contact:

UNITED STATES ATTORNEY'S OFFICE EASTERN DISTRICT OF PENNSYLVANIA Suite 1250, 615 Chestnut Street Philadelphia, PA 19106 JENNIFER CRANDALL Media Contact 215-861-8300

U.S. Places Restrictions on China's Leading Chip Maker

WASHINGTON — The Trump administration has placed new restrictions on exports to Semiconductor Manufacturing International Corporation, China's most advanced maker of computer chips, a measure that could deepen the technology conflict between China and the United States. In a letter on Friday, the Department of Commerce told American companies in the chip industry that they must first acquire a license to sell technology to SMIC and its subsidiaries. The department said it was taking the action after a review in which it determined that the Chinese company "may pose an unacceptable risk of diversion to a military end use in the People's Republic of China."

The measure, which could cut SMIC off from the American software and other technology it needs to make its products, comes as the Trump administration takes a harsher stance against Chinese technology companies that it has deemed a national security threat. The administration has clamped down on shipments to the Chinese tech giant Huawei, restricted exports to dozens of other Chinese companies by placing them on a blacklist this year and moved to ban the Chinese-owned social media services WeChat and TikTok. A spokesperson for the Bureau of Industry and Security, a division of the Commerce Department, said the bureau could not comment on specific licensing issues, but that it was "constantly monitoring and assessing any potential threats to U.S. national security and foreign policy interests" and would "take appropriate action as warranted."

The letter was first reported by The Financial Times. The Pentagon, in particular, has expressed concerns that SMIC, whose major shareholders include several Chinese state entities, has ties with the Chinese military. A research report by the U.S. defense contractor SOS International that has been widely circulated within the Trump administration says that researchers at universities associated with the Chinese military appear to have made extensive use of SMIC's processes and technologies in their research and that other SMIC customers probably have ties to the Chinese defense industry. A SMIC spokeswoman said on Saturday that the company had no relationship with the Chinese armed forces and that it produced chips solely for commercial and civilian use. She added that the company had not received any official notice from the Commerce Department regarding new export restrictions.

(*Continued On The Following Column)

"Learn how to be happy with what you have while you pursue all that you want."

Factories in China churn out a huge share of the world's cellphones, computers and internet equipment. But the silicon brains of that gear are often shipped in from overseas.

Last year, mainland China imported more than \$300 billion in computer chips, more than it spent on crude oil. The country's leader, Xi Jinping, has put enormous resources toward making China more self-reliant in semiconductors and other advanced technologies. But state support has only taken Chinese chip companies so far. Though SMIC is China's most technologically advanced chip maker, its manufacturing processes are years behind those of industry leaders like Samsung and Taiwan Semiconductor Manufacturing Company in terms of the number of transistors they can squeeze onto a piece of silicon. That means SMIC cannot make the intricate chips that best support the latest, most demanding applications.

Even to produce its less sophisticated semiconductors, SMIC relies on software and machines from American companies. Analysts at the investment bank Jefferies estimate that up to half of SMIC's equipment currently comes from U.S. suppliers. SMIC could struggle to stay in business if those partners cannot service and upgrade the company's manufacturing equipment.

SMIC's business has already been hit this year by the Trump administration's curbs on Huawei. In recent months, the Commerce Department has curtailed the Chinese tech giant's ability to buy semiconductors anywhere in the world, including from SMIC. Huawei's chip unit accounted for nearly one-fifth of SMIC's sales last year, according to estimates by Credit Suisse analysts. Qualcomm, the American chip giant, is another customer of SMIC's.

Ana Swanson reported from Washington, and Raymond Zhong from Taipei, Taiwan.

NOTE: In accordance with Title 17 U.S.C. Section 107, this material is distributed without profit or payment for non-profit news reporting and educational purposes only.

Reproduction for private use or gain is subject to original copyright restrictions.