EIB World Trade Headlines

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

August 1, 2018 - Volume 10, Issue 14

U.S. Commerce Dept.

The Department of Commerce has signed the escrow agreement with ZTE. Once ZTE has completed the $400 million escrow deposit, BIS will issue a notice lifting the denial order. Until such notice, the denial order remains in full force and effect. Once the monitor is selected and brought on board, the three-pronged compliance regime – the new 10-year suspended denial order, the $400 million escrow, and the monitor – will be in place. The ZTE settlement represents the toughest penalty and strictest compliance regime the Department has ever imposed in such a case. It will deter future bad actors and ensure the Department is able to protect the United States from those that would do us harm.

NEWSLETTER NOTES

Training

Interested to learn about the latest updates to the Export Administration Regulations? Register today for BIS seminars in California and Rhode Island before these programs fill up. Registration is also available for a one-day Encryption Controls Seminar in Northern California, following a two-day Complying with U.S. Export Controls seminar. Details below.

■ Complying with U.S. Export Controls – 2 Day
August 14-15, 2018
Milpitas, CA
Registration: $485

■ Encryption Controls – 1 Day
August 16, 2018
Milpitas, CA
Registration: $375

■ Complying with U.S. Export Controls – 2 Day
September 12-13, 2018
Smithfield, RI
Registration: $450

■ Complying with U.S. Export Controls – 2 Day
September 19-20, 2018
Los Angeles, CA
Registration: $500

"Complying with U.S. Export Controls" is a two-day program led by BIS's professional counseling staff and provides an in-depth examination of the Export Administration Regulations (EAR). The program will cover the information exporters need to know to comply with U.S. export control requirements under these regulations. We will focus on what items and activities are subject to the EAR; steps to take to determine the export licensing requirements for your item, how to determine your export control classification number (ECCN), when you can export or reexport without applying for a license, export clearance procedures and record keeping requirements, and real life examples in applying this information. Presenters will conduct a number of "hands-on" exercises that will prepare you to apply the regulations to your own company's export activities.

"Encryption Controls" is a one-day program that will focus on the unique provisions related to encryption under the EAR. BIS export policy specialists will provide the latest updates to the encryption provisions in the EAR, and cover a variety of topics specific to encryption, including determining if your items are controlled for encryption reasons under the EAR, license exceptions and mass market provisions, commodity classification requests and reporting requirements, and applying for an encryption license. Prerequisite: Complying with U.S. Export Controls or equivalent experience.

*(*Continued On The Following Column)*

For additional details about the BIS seminars, please visit the BIS Current Seminar Schedule page at: https://www.bis.doc.gov/index.php/compliance-a-training/current-seminar-schedule

For general information about the BIS Seminar Program, please contact the BIS Outreach and Educational Services Division at OESDSeminar@bis.doc.gov or (202) 482-6031.

For additional information on the California seminars, please contact the BIS Western Regional Office at (408) 998-8806 or (949) 660-0144.

232 Aluminum Investigation

Section 232 National Security Investigation of Aluminum Imports

Information on the Exclusion and Objection Process

Background

On March 8, 2018, President Trump exercised his authority under Section 232 of the Trade Expansion Act of 1962 to impose a 10 percent tariff on aluminum imports, with exemptions for Canada and Mexico, in order to protect our national security. The President's Section 232 decision is the result of an investigation led by the Commerce Department. U.S. Customs and Border Protection will begin collecting the tariffs on March 23, 2018.

In President Trump's proclamation establishing the tariff under Section 232, the President authorized the Secretary of Commerce, in consultation with other appropriate federal agency heads, to provide relief from the additional duties for any aluminum articles determined "not to be produced in the United States in a sufficient and reasonably available amount or of a satisfactory quality and is also authorized to provide such relief based upon specific national security considerations. Such relief shall be provided for any article only after a request for exclusion is made by a directly affected party located in the United States."

Process

Exclusion Requests will be open for public review after being posted to the federal rulemaking portal. During the initial 30 days, U.S. parties may file objections to the exclusion request. After this initial 30 day period, approximately 60 days will be necessary for complete review and vetting of the Exclusion Request and any related Objection Filings. The total processing time for exclusion requests is estimated at 90 days.

*(*Continued On The Following Page)*

A single response to each exclusion request and related objection filings will be posted in regulations.gov indicating if the exclusion request has been granted or denied.

On March 19, 2018, the U.S. Department of Commerce published the procedures to request exclusion from the steel and aluminum tariffs in the Federal Register. See Federal Register, Vol. 83, No. 53, 12106-12112.

Filing Exclusion Requests

If your organization uses aluminum in business activities in the United States and wishes to request an exclusion from the tariff on aluminum article imports:

(1) Download the *Request for Exclusion from Remedies from the Section 232 National Security Investigation of Imports of Aluminum* (Exclusion Request) form.

(2) Complete the form using Microsoft Excel and save a copy on your computer.

(3) Go to Docket Number BIS-2018-0002, complete the required information, and upload the completed Exclusion Request form.

A separate Exclusion Request must be submitted on each distinct type and dimension of aluminum product to be imported.

Exclusion Request Requirements: Only individuals or organizations operating in the United States that use aluminum products in business activities in the United States may submit an Exclusion Request.

For an Exclusion Request to be considered, the exclusion requester must provide factual information on 1) the single type of aluminum product they require using a 10-digit HTSUS code, including its specific dimension; 2) the quantity of product required (stated in kilograms) under a one-year exclusion; 3) a full description of the properties of the aluminum product it seeks to import, including chemical composition, dimensions, strength, toughness, ductility, magnetic permeability, surface finish, coatings, and other relevant data.

All exclusion requests will be reviewed for completeness. Only fully completed exclusion requests will be considered and posted for public review. All exclusion requests will be made available for public inspection and copying.

*(*Continued On The Following Column)*

Filing Exclusion Objections

If your organization manufactures aluminum products in the United States and wishes to object to an existing Exclusion Request, within 30 days of the posting of the related Exclusion Request:

(1) Download the *Response Form for Organizations Filing Objections to Posted Section 232 Exclusion Requests – Aluminum* (Objection Filing) form.

(2) Complete the form using Microsoft Excel and save a copy on your computer.

(3) Go to Docket Number BIS-2018-0002, select the Exclusion Request to which you are objecting, complete the required information, and upload the completed Objection form.

Objection Filing Requirements: Any individual or organization in the United States may file an objection to an Exclusion Request. For an Objection Filing to be considered, organizations must provide factual information on 1) the aluminum products that they manufacture in the United States, 2) the production capabilities at aluminum manufacturing facilities that they operate in the United States; and 3) the availability and delivery time of the products that they manufacture relative to the specific aluminum product that is subject to an Exclusion Request.

Organizations submitting an Objection Filing on an Exclusion Request should provide specific information on the product that their company can provide that is comparable to the aluminum product that is the subject of the Exclusion Request. This information should include 1) discussion on the suitability of its product for the application identified by the Exclusion Requestor, and 2) a full technical description of the properties of the product it manufactures relative to specifications provided in the Exclusion Request posted on regulations.gov, including information on dimensions, strength, toughness, ductility, surface finish, coatings, and other relevant data.

All Objections Filings will be reviewed for completeness. Only fully completed Objection filings will be considered and posted for public review. All Objection Filings will be made available for public inspection and copying.

Contact

Please email or call: aluminum232@bis.doc.gov or 202-482-4757 for any aluminum-related queries.

Why China's New Air Defense System Could be Quite Dangerous Here is what we know.

by Dave Majumdar
China is developing a new generation of surface-to-air missile defenses, but details are scarce.

What does seem apparent is that the new weapon is being designed to counter a wide range of threats ranging from aircraft to cruise missiles to ballistic missiles. Indeed, the Chinese engineers working on the new weapons system seem to indicate that the new system will be designed to provide long-range ballistic missile defense among its various functions.

“Researchers from the academy's Zhang Yiqun Laboratory have been playing a vital role in the development of China's new air-defense missile system by designing its control systems - the ‘brain’ of any missile,” reads a China Military Online posting , which by its own description is “authorized by the Central Military Commission of the People's Republic of China (PRC) and sponsored by the Chinese People's Liberation Army (PLA) News Media Center.”

“Compared with previous generations of air-defense missiles, the new-generation missile system will have a wider range of targets and be much more technologically sophisticated, taking China into the ranks of just a handful of nations capable of designing and producing such a system.”

Given the researchers’ description of the program, the new weapon system is likely to have a strong ballistic missile defense component.

“Metaphorically put, the mission of these control systems is to guide a needle to fly 1,000 kilometers to pierce the eye of another needle,” Wang Mengyi, deputy head of the Second Academy's General Design Department and former leader of the laboratory, told China Daily. “For researchers from Zhang Yiqun Laboratory, their mission is to turn this seemingly impossible task into reality.”

The new weapon could be the HQ-19, which is an advanced ballistic missile defense variant of China’s existing HQ-9 air defense system. The existence of that weapon systems development program was first revealed in a 2016 U.S. Defense Department report on Chinese military capabilities.

“China is advancing a new ballistic missile interceptor, the HQ-19, according to an annual U.S. Defense Department report, in a development that may indicate progress toward a deployed missile defense system,” Alicia Sanders-Zakre wrote for the Arms Control Association .

*(*Continued On The Following Column)*

“As of May 2016, the missile was still undergoing testing to intercept ballistic missiles having a range of 3,000 kilometers. An operational HQ-19 interceptor would be armed with a kinetic kill vehicle and be able to target ballistic missiles and satellites in lower-earth orbit. The HQ-19 is a significantly updated variant of the HQ-9, a long-range surface-to-air missile that has a limited capacity to hit short-range ballistic missiles up to 500 kilometers in range.”

There are also several other Chinese air and missile defense systems under development including the 2,000 km range HQ-26 and the HQ-29. The new Chinese missile could be one of these weapons or it could be something new. It could also be follow-on to the HQ-18, which was reverse engineered by the Chinese from the Russian S-300V series.

“The HQ-18 is a highly-capable, hypersonic air and missile defense system developed by China; most scholars agree it is directly reverse-engineered from the Russian S-300V system, but relatively little information is publicly known about the differences between the two systems,” reads a Missile Defense Advocacy analysis of the HQ-19.

“S-300V has two different versions distinguished by the missile it uses: The SA-12A Gladiator is used primarily for targeting aircraft, whereas the SA-12B Giant is primarily for countering tactical ballistic and cruise missiles. The Gladiator has a range of 75 km and a maximum altitude of 25 km, and the Giant has a range of 100 km and an altitude ceiling between 30 and 40 km.The S-300V system uses a phased-array sector-scan radar with a range of 175 km and can track up to 16 targets simultaneously,” the report noted.

“ A modified version of the S-300V system was revealed in 1998, called the S-300VM, or “Antey-2500.” The Antey-2500 variant has a range of 200 km, a max altitude of 30 km, and can engage 24 targets simultaneously. A typical HQ-18 battery contains between two and six launchers, each of which can hold four missiles.” The current generation of Chinese surface-to-air missile defenses is bad enough; future weapons will be even more of a problem.

“The S-300V family is one of the most capable aerial defense systems in the world, and an upgraded Chinese version should worry Western defense agencies,” the Missile Defense Advocacy states.

“S-300V was originally designed to destroy U.S. tactical ballistic missiles and ISR assets in a late Cold War setting; it has no Western equivalent. Moreover, no F/A-18 variant, nor the Joint Strike Fighter, were designed to penetrate the S-300V/VM’s aerial cover. The survivability of the F-35 ‘will not be significantly better than that of legacy combat aircraft,’ and the U.S. Air Force envisions the F-22 Raptor as the primary aircraft to dispatch an HQ-18. Additional development and production of the HQ-18 will likely replace the HQ-9 for long-range missile defense.”

GUILTY OF FCPA VIOLATIONS

A former official at a Venezuelan state-run electric company pleaded guilty on Monday to U.S. charges that he participated in a scheme to solicit bribes in exchange for helping vendors win favorable treatment from state oil company PDVSA.

Luis Carlos De Leon Perez, 42, pleaded guilty in federal court in Houston to conspiring to violate the Foreign Corrupt Practices Act and to conspiring to commit money laundering, the U.S. Justice Department said.

He became the 12th person to plead guilty as part of a larger investigation by the Justice Department into bribery at Petroleos de Venezuela SA that became public with the arrest of two Venezuelan businessmen in December 2015.

The two men were Roberto Rincon, who was president of Tradequip Services & Marine, and Abraham Jose Shiera Bastidas, the manager of Vertix Instrumentos. Both pleaded guilty in 2016 to conspiring to pay bribes to secure energy contracts. De Leon is scheduled to be sentenced on Sept. 24. His lawyers did not respond to requests for comment.

De Leon was arrested in October 2017 in Spain and was extradited to the United States after being indicted along with four other former Venezuelan officials on charges they solicited bribes to help vendors win favorable treatment from PDVSA.

An indictment said that from 2011 to 2013 the five Venezuelans sought bribes and kickbacks from vendors to help them secure PDVSA contracts and gain priority over other vendors for outstanding invoices during its liquidity crisis.

Prosecutors said De Leon was among a group of PDVSA officials and people outside the company with influence at it who solicited bribes from Rincon and Shiera. De Leon worked with those men to then launder the bribe money, prosecutors said. De Leon also sought bribes from the owners of other energy companies and directed some of that money to PDVSA officials in order help those businesses out, prosecutors said.

Among the people indicted with De Leon was Cesar David Rincon Godoy, a former general manager at PDVSA's procurement unit Bariven. He pleaded guilty in April to one count of conspiracy to commit money laundering.

Others charged included Nervis Villalobos, a former Venezuelan vice minister of energy; Rafael Reiter, who worked as PDVSA's head of security and loss prevention; and Alejandro Isturiz Chiesa, who was an assistant to Bariven's president.

Villalobos and Reiter were, like De Leon, arrested in Spain, where they remain pending extradition, the Justice Department said. Isturiz remains at large.

US TAKES 5 PARTNERS TO WTO OVER METAL TARIFFS

The Trump administration is hitting back at what it considers unjustified retaliatory tariffs that were imposed in response to U.S. steel and aluminum duties.

The U.S. Trade Representative said it launched formal challenges at the World Trade Organization on Monday against China, the European Union, Canada, Mexico and Turkey for retaliating against steel and aluminum tariffs. The Trump administration earlier this year imposed 10 percent duties on aluminum and 25 percent on steel after finding imports of the metals pose a risk to national security.

“Instead of working with us to address a common problem, some “Instead of working with us to address a common problem, some of our trading partners have elected to respond with retaliatory tariffs designed to punish American workers, farmers and companies.,” U.S. Trade Representative Robert Lighthizer said in a statement.

Lighthizer said the U.S. would take “all necessary actions” to protect U.S. interests and urged trading partners to “work constructively” with the Trump administration to address overcapacity in both metal sectors.

Canada, China, the EU, Mexico and Turkey have imposed retaliatory tariffs on $23.4 billion worth of U.S. goods in response to Trump’s tariffs on steel and aluminum.

EU Opposition

A European Commission spokesman said that while the bloc’s decision to retaliate was proportionate and WTO-compatible, the U.S. is entitled to seek an independent review in which the European Union will explain and defend its position.

The Canadian government said its tit-for-tat tariffs are allowed under the rules of the WTO and North American Free Trade Agreement. “The tariffs imposed by the United States on Canadian steel and aluminum are unacceptable and illegal,” Adam Austen, the spokesman for Foreign Minister Chrystia Freeland, said in an emailed statement on Monday.

The Mexican government said in a statement that it will look at the U.S. request with the goal of answering it in the next 10 days. The U.S.’s national-security rationale for its steel and aluminum tariffs was unjustified, according to the statement, and Mexico’s response was a reaction to that. The Mexican government promised to continue to defend its national interest.

*(*Continued On The Following Page)*

The Trump administration has criticized the WTO for encroaching on U.S. legal sovereignty and failing to rein in China's alleged violation of global trading rules. Trump himself threatened to take action against the WTO earlier this month after Axios, a news service, reported that his administration had drafted legislation to withdraw the U.S. from the organization, a move the president repeatedly told advisers he was considering.

The WTO has "not worked well, or not as well as it was intended to work when China was brought into the WTO in the year 2000," Treasury Undersecretary for International Affairs David Malpass said at an event in Washington on Monday.

The U.S. wins 87 percent of the cases it brings to the WTO against other countries and loses 75 percent of the cases other countries bring against Washington, according to a Bloomberg analysis of the 524 cases lodged at the Geneva-based organization since it was founded in 1995 as the successor to the General Agreement on Tariffs and Trade. Both figures are better than the average for all nations.

— With assistance by Bryce Baschuk, Viktoria Dendrinou, Reade Pickert, Josh Wingrove, and Craig Torres

Littoral Combat Ship 13 (Wichita) Completes Acceptance Trials

Littoral Combat Ship (LCS) 13, the future USS Wichita, completed Acceptance Trials in the waters of Lake Michigan. LCS 13 is the seventh Freedom-variant LCS designed and built by the Lockheed Martin (NYSE: LMT)-led industry team, and is slated for delivery to the U.S. Navy later this summer.

"LCS 13's completion of Acceptance Trials means this ship is one step closer to joining the fleet and conducting critical maritime operations for the Navy," said Joe DePietro, vice president, Small Combatants and Ship Systems at Lockheed Martin. "This ship is agile, powerful and lethal, and the industry team and I are looking forward to her delivery, commissioning and deployment."

The trials, conducted July 9-12, included a full-power run, maneuverability testing and air detect-to-engage demonstrations of the ship's combat system. Major systems and features were demonstrated including aviation support, and small boat launch handling and recovery.

*(*Continued On The Following Column)*

"I am extremely proud of our LCS team including our shipbuilders at Fincantieri Marinette Marine," said Jan Allman, Fincantieri Marinette Marine President and CEO. "These are complex vessels, and it takes a strong team effort to design, build and test these American warships."

The future USS Wichita is one of eight ships in various stages of production and test at Fincantieri Marinette Marine, with one more in long-lead production.

The next Freedom-variant in the class is LCS 15, the future USS Billings. LCS 15 is scheduled to complete sea trials this year.

Lockheed Martin's Freedom-variant LCS is a highly maneuverable, lethal and adaptable ship, designed to support focused-missions in the areas of mine countermeasures, anti-submarine warfare and surface warfare. The Freedom-variant LCS integrates new technology and capability to affordably support current and future mission capability from deep water to the littorals.

Source: Lockheed Martin Corporation (NYSE: LMT)
Date: Jul 16, 2018

BIS Issues an Order Terminating the Denial Order Issued on April 15, 2018 Against ZTE

On July 13, 2018, the Acting Assistant Secretary of Commerce for Export Enforcement issued an Order terminating the Denial Order issued on April 15, 2018 against Zhongxing Telecommunications Equipment Corporation and ZTE Kangxun Telecommunications Ltd. The Order is posted on BIS's website (link) and will be published in the Federal Register shortly. For additional information, please call BIS's Exporter Counseling Desks at one of the following numbers:

*(*Continued On The Following Page)*

(202) 482-4811 - Outreach and Educational Services Division (located in Washington, DC)

(949) 660-0144 - Western Regional Office (located in Irvine, CA)

(408) 998-8806 - Northern California branch (located in San Jose, CA)

or e-mail your inquiry to the Export Counseling Division of the Office of Exporter Services at: ECDOEXS@bis.doc.gov ."

Additional information is available here.

The FAR Takes Aim at Russia's Kaspersky Lab: What Every Contractor Must Know

At this point, even casual observers of the news likely have heard of Moscow-based Kaspersky Lab. In the wake of reported connections to the Kremlin and Russian intelligence entities, the cybersecurity company was famously banned as a source of supply to the United States Government by Section 1634 of the 2018 National Defense Authorization Act ("NDAA"). Effective October 1, 2018, the NDAA forbids every "department, agency, organization, or other element of the Federal Government" from using "any hardware, software, or services developed or provided, in whole or in part" by (i) Kaspersky and any corporate successors, (ii) any entities controlled by or under common control with Kaspersky and (iii) any entity in which Kaspersky has majority ownership.

In furtherance of the NDAA's statutory mandate, the FAR Council issued an Interim Rule on June 15, 2018 that – beginning July 16, 2018 – amends the FAR to implement the Kaspersky prohibitions. In particular, the Interim Rule:

- Creates FAR Subpart 4.20, which contains policies and procedures that administratively codify the NDAA's requirements; and
- Establishes a new contract clause, FAR 52.204-23, titled "Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities."

*(*Continued On The Following Column)*

The FAR clause, which must be incorporated into all solicitations and contracts and all subcontracts in support thereof, contains two essential terms with which every Federal Government contractor should become familiar: "covered entity" and "covered article." A "covered entity" is defined as Kaspersky Lab, any successor entity to Kaspersky Lab, any entity that shares control, is controlled by, or that controls Kaspersky Lab, and any entity in which Kaspersky Lab has a majority ownership. A "covered article," in turn, is defined as any hardware, software, or service that is developed or provided in whole or in part by a covered entity or which contains components using any hardware or software developed in whole or in part by a covered entity.

As its title foreshadows, the clause "prohibits Government use of any covered article" and similarly bans contractors from (1) providing any covered article that the Government will use on or after October 1, 2018, and (2) using any covered article on or after October 1, 2018 in the development of data or deliverables first produced in the performance of the contract. In addition, contractors are required to report instances in which they either have identified a covered article that has been provided to the Government or have been advised as to the existence of a covered article by a subcontractor at any tier or any other source. The reporting requirements, which vary depending on the affected contract(s), are summarized as follows:

- **For non-DoD contracts**, the contractor must inform the contracting officer in writing within 1 business day from the date it identifies the covered article or is notified of its existence. Contractors holding non-DoD indefinite delivery contracts are required to notify both the contracting officer for the indefinite delivery contract and the contracting officer(s) for any affected order(s). In its notification, the contractor must identify the contract number, the order number(s) (if applicable), the supplier name, brand, model number, original equipment manufacturer number, manufacturer part number or wholesaler number, the item description and any readily available information about mitigation actions undertaken or recommended.
    - Within 10 business days of providing the initial notification, the contractor must report any further available information about mitigation actions undertaken or recommended. Additionally, the contract is required to describe the efforts it undertook to prevent use or submission of a covered article, any reasons that led to the use or submission of the covered article, and any additional efforts that will be incorporated to prevent future use or submission of covered articles.

*(*Continued On The Following Page)*

For DoD contracts, the contractor must include the foregoing data elements, to be provided in accordance with the same timelines, in a report to be filed at https://dibnet.dod.mil.

Compliance in Four Steps: Practical Guidance for Contractors

The Interim Rule was issued without the opportunity for public comment because of the Government's determination that "urgent and compelling reasons exist" for the imposition of the NDAA's requirements on federal contractors. Although the full prohibitions do not take effect until October 1, 2018, the FAR Council has explicitly advised contractors to "take steps immediately to meet this deadline." We agree that this is a prudent course of action, particularly given the sweeping nature of the new requirements. Accordingly, here are four key actions that we recommend contractors consider as the compliance deadline nears:

1. Immediately evaluate the products and services in your supply chain to ensure that your company is not providing products or services with any nexus to Kaspersky Lab. If and as any such product or service is discovered, it should be identified, isolated, and removed as soon as possible.

2. Establish internal policies and procedures to ensure compliance with the new reporting requirements. Remember, FAR 52.204-23 requires that the identification/notification of a covered article be reported to the Government within 1 business day of discovery. In addition to the multiple data elements and mitigation measures that must be reported, a detailed follow-up report must be filed within 10 business days.

3. Inform your existing and potential subcontractors of the new requirements by providing them with a copy of FAR 52.204-23 and by obtaining written assurances that they (a) understand what the clause mandates and (b) will comply with its requirements.

4. Modify your existing FAR flow-down templates to include FAR 52.204-23 for all subcontracts awarded on or after July 16, 2018.

At an indeterminate point in the future, the Government will issue a Final Rule that will likely modify at least some of the foregoing requirements. If your company would like to propose changes to the Interim Rule or otherwise engage with the Government regarding the requirements, it must submit comments by August 14, 2018. But for now, these are the new rules with which every contractor must comply.

Military secrets on the Air Force's Reaper drone were listed for sale on the dark web, says a security company.

Military secrets are often heavily guarded, but it's meaningless if there's weak router security.

Researchers from Recorded Future, a threat intelligence company, say they found a cache of sensitive military documents for sale on the dark web, including details on the US Air Force's MQ-9 Reaper drones, as well as training courses on tanks, survival and improvised explosive devices.

A hacker had stolen the secret files by taking advantage of a router vulnerability known about since 2016, according to Recorded Future. The Air Force didn't respond to a request for comment.

Cybercriminals often cast a wide net across the web looking for any opening they can find. Routers can be an entry point if people fail to keep up with security updates.

In June, the FBI asked that people reboot their routers after Russian hackers infected over 500,000 of the devices in 54 countries. Routers are also prized targets because they allow access to web activity, passwords and, potentially, top secret documents.

The hacker had used Shodan, a search engine for connected devices, to look for routers that were still vulnerable to attacks, Recorded Future said.

"The fact that a single hacker with moderate technical skills was able to identify several vulnerable military targets and exfiltrate highly sensitive information in a week's time is a disturbing preview of what a more determined and organized group with superior technical and financial resources could achieve," Andrei Barysevich, Recorded Future's director of advanced collection, said in a blog post.

The hacker also bragged to Recorded Future's researchers that he was able to watch live footage from border surveillance cameras and airplanes, sending a screenshot of footage from a drone flying over the Gulf of Mexico.

In one Dark Web post, the cybercriminal named his asking price to a potential buyer. "I expect about $150 or $200 for being classified information," reads a screenshot of the posting. The post was accompanied by a schematic of the drone.

*(*Continued On The Following Page)*

The MQ-9 Reaper drone is one of the most widely used military drones around the world, deployed by the Air Force as well as the US Navy, the CIA and NASA.

Recorded Future's researchers said they contacted the thief, who was able to steal the documents from a computer belonging to a captain stationed at an Air Force base in Nevada, using a vulnerability on a misconfigured router.

The vulnerability had been publicly announced in early 2016, with Netgear warning people that they should change the default passwords on their routers. Despite finishing a cybersecurity training course on Feb. 16 this year, the hacked captain didn't change the default password on the router, Recorded Future's researchers said.

The security analysts found that there were more than 4,000 routers around the world vulnerable to the same attack, even though the warning has been out for two years.

It's unclear how thieves got hold of the second set of documents spoken of by Recorded Future -- with secrets on how the US military avoids IEDs and operates tanks. The confidential files were listed for sale about two weeks after the first listing, Recorded Future said.

The company said it was cooperating with law enforcement's investigation of the data breach.

The Very Purpose of the Chinese Tech Company ZTE is to Spy on Other Countries, a Competitor Alleges in New Court Documents

•ZTE was created for intelligence-gathering reasons and has been engaged in extensive bribery, according to new documents filed in a Dallas County, Texas, district court.

• Fairfax Media found case files in which a competitor alleges ZTE was founded by China's Ministry of Aerospace in order to spy on targets overseas.

•Officials in Liberia reportedly testified that they received "brown paper bags" filled with cash as bribes to act against the interest of ZTE's competitor.

•Court documents apparently include a 2015 report from an ethics council for Norway's Government Pension Fund, which said ZTE had been accused of corruption in 18 countries.
ZTE was created by China for the purpose of spying, and openly used bribery to accomplish its goals, court documents allege. 4

*(*Continued On The Following Column)*

Fairfax Media reported that files in a Dallas case between Chinese telecommunications firm ZTE and Universal Telephone Exchange contain shocking claims regarding the purposes and practices of the company at the center of the Trump administration's trade talks with China.

"China's Ministry of Aerospace founded ZTE as a front to send officers abroad under non-diplomatic covers such as scientists, businessmen and executives for the purpose of collecting intelligence," documents in the case allege.

The documents also include testimony, taken under oath, from two telecom executives from Liberia who said ZTE bribed officials, allegedly including judges and the country's former president, between 2005 and 2007.

The officials said they were offered 5% of the value of a ZTE contract if the deal was taken away from Universal Telephone Exchange. Both men testified to receiving cash in "brown paper bags."

One of the men allegedly also received travel and an "unlimited shopping spree" in China, according to the court documents cited by Fairfax Media.

ZTE denied the claims in a statement to Fairfax, but Norway's central bank banned its Government Investment Fund from investing in ZTE in 2016 because of what it deemed to be an unacceptable risk of "gross corruption."

The report this claim was based on is, according to Fairfax, part of the Texas case documents. It alleges that, in 2015, ZTE had been "accused of corruption in a total of 18 countries and been investigated for corruption in 10 of these."

"ZTE operates in a sector where large public-sector contracts are common and has allegedly repeatedly paid large bribes so that public-sector employees will favour it in competitive tenders. This has supposedly taken place in countries such as Zambia, the Philippines, Papua New Guinea, Liberia, Myanmar and Nigeria," the report read.

According to a previous investigation by Fairfax Media, ZTE not only regularly bribed foreign officials but had an entire department dedicated to managing bribe payments.

In February, six intelligence chiefs — including the heads of the CIA, FBI, and NSA — testified they do not use, and would not recommend private citizens use products from ZTE and smartphone maker Huawei. The Pentagon announced in early May it had stopped selling ZTE and Huawei phones and modems in stores on its military bases because they "may pose an unacceptable risk."

In Australia, ZTE and Chinese smartphone maker Huawei have been shortlisted to develop a 5G network.

Senate Republicans drop bid to block Trump from lifting sanctions on Chinese telecom giant ZTE

The retreat means that ZTE — a company found guilty of selling U.S. goods to Iran in violation of sanctions — will get to duck tough Commerce Department penalties that bar U.S. companies from doing business with it. Chinese officials said those penalties would effectively put ZTE out of business.

President Trump had ordered his own Commerce Department to lift the penalties, but senators wanted to reimpose them as part of a sweeping defense policy bill set to be unveiled next week. They have now agreed to language advanced by the House instead, which bars government contractors from doing business with ZTE but allows the company to continue doing business with private U.S. firms, according to a source who spoke on the condition of anonymity to speak about the internal negotiations.

Former NSA Contractor Pleads Guilty

A former contractor with the National Security Agency arrested in August 2016 will plead guilty this month to one of the 20 counts he faces.

Harold Martin III, 52, will plead guilty on Jan. 22 to one count of willful retention of national defense information, according to The New York Times.

He faces up to 10 years in prison, three years of supervised release and fines of up to $250,000 for that charge, according to Nextgov.

Federal authorities have stated that Martin removed classified information from the agencies he worked for and stored those documents in his Maryland home for decades. Some of the documents were classified as top secret and sensitive compartmented information.

Martin's attorneys describe him as a "compulsive hoarder," the Times reported. He began taking home highly classified documents from the National Security Agency and other government agencies in the late 1990s. They were in paper form, as well as on hard drives and flash drives in his Glen Burnie, Maryland home; in a shed in his yard; and in his car. In all, he stole 50 terabytes of data, and his activity "went undetected until his arrest on Aug. 27, 2016."

*(*Continued On The Following Column)*

Among the cache of information he took were NSA hacking tools. Those tools wound up available for purchase on the internet.

There is no deal on the table for Martin, and although he has pleaded to this solitary charge, he won't be sentenced until all of the remaining counts are resolved, Nextgov reported.

A schedule laid out by Judge Marvin J. Garbis of United States District Court lists additional dates for continuing legal action regarding the other 19 charges Martin still faces, the Times reported.

This is an interesting case to watch, because the amount of documents Martin took outnumbers that of Edward Snowden, perhaps the most security clearance-related case in the past few years, said Catie Young, a security clearance lawyer.

Snowden was a contractor who stole hundreds of thousands of secret documents and gave them to journalists.

When it's time for Martin to be sentenced, his attorneys plan to argue for leniency "on the grounds that he suffers from a mental disorder that caused him to take the material home year after year; that he never tried to give it to the news media, a foreign country or anyone else; and that he is a Navy veteran and a patriot who served his country for years," the Times reported.

Americans can legally download 3-D printed guns starting next month

(CNN)Gun-rights activists have reached a settlement with the government that will allow them to post 3-D printable gun plans online starting August 1.

The settlement ends a multi-year legal battle that started when Cody Wilson, who describes himself as a post-left anarchist, posted plans for a 3-D printed handgun he called "The Liberator" in 2013.
The single-shot pistol was made almost entirely out of of ABS plastic -- the same stuff they make Lego bricks out of -- that could be made on a 3-D printer. The only metal parts were the firing pin and a piece of metal included to comply with the Undetectable Firearms Act.

The US State Department told Wilson and his non-profit group Defense Distributed to take down the plans. It said the plans could violate International Traffic in Arms Regulations (ITAR), which regulate the export of defense materials, services and technical data.

*(*Continued On The Following Page)*

In essence, officials said someone in another country -- a country the US doesn't sell weapons to -- could download the material and make their own gun.

Wilson complied, but said the files already had been downloaded a million times.

He sued the federal government in 2015.

The settlement

The settlement, which is dated June 29, says that Wilson and Defense Distributed can publish plans, files and 3-D drawings in any form and exempts them from the export restrictions. The government also agreed to pay almost $40,000 of Wilson's legal fees and to refund some registration fees.

The settlement has not been made public, but Wilson's attorneys provided a copy to CNN.

"We asked for the Moon and we figured the government would reject it, but they didn't want to go to trial," said Alan M. Gottlieb with the Second Amendment Foundation, which helped in the case. "The government fought us all the way and then all of the sudden folded their tent."

Gottlieb said they filed the lawsuit during the Obama administration, but he doesn't think that explains the change of heart.

"These were all career people that we were dealing with. I don't think there was anything political about it," he said.

Avery Gardiner, the co-president of the Brady Campaign to Prevent Gun Violence, said she'd be astonished if the settlement wasn't approved by political appointees.

"We were shocked and disappointed that the Trump administration would make a secret backroom deal with very little notice," Gardiner said. She said she found out about the settlement from a magazine article.

The group has filed a Freedom of Information Act request for emails and other documents related to the settlement.

Josh Blackman, Wilson's attorney, said he wished the settlement signaled a philosophical change.

*(*Continued On The Following Column)*

"They were going to lose this case," Blackman said. "If the government litigated this case and they lost this decision could be used to challenge other kinds of gun control laws."

The implications

Do-it-yourself firearms like The Liberator have been nicknamed "Ghost Guns" because they don't have serial numbers and are untraceable.

Wilson has built a website where people will be able to download The Liberator and digital files for an AR-15 lower receiver, a complete Baretta M9 handgun and other firearms. Users will also be able to share their own designs for guns, magazines and other accessories.

He says the files will be a good resource for builders, even though it's not yet practical for most people to 3-D print most of the guns.

"It's still out of reach for them. We'll get to watch it all develop," Wilson said. "The plans will be here when that moment comes."

For Wilson and his supporters, the ability to build unregulated and untraceable guns will make it much harder, if not impossible for governments to ban them.

Gardiner fears it will make it easier for terrorists and people who are too dangerous to pass criminal background checks to get their hands on guns.

"I think everybody in America ought to be terrified about that."

The fact that high end 3-D printers are still too expensive for most people doesn't ease her concerns.

"The people who make them will be state actors or well financed criminal cartels who have the ability to execute well organized criminal attacks in the United States and elsewhere," she said.

She said that providing the plans to anyone in the world, who has Internet access is a national security threat.

The Defense Distributed website proclaims that "the age of the downloadable gun formally begins."

Russian National Charged in Conspiracy to Act as an Agent of the Russian Federation within the United States

A criminal complaint was unsealed today in the District of Columbia charging a Russian national with conspiracy to act as an agent of the Russian Federation within the United States without prior notification to the Attorney General. 5

The announcement was made by Assistant Attorney General for National Security John C. Demers, U.S. Attorney for the District of Columbia Jessie K. Liu, and Nancy McNamara, Assistant Director in Charge of the FBI's Washington Field Office.

Maria Butina, 29, a Russian citizen residing in Washington D.C., was arrested on July 15, 2018, in Washington, D.C., and made her initial appearance this afternoon before Magistrate Judge Deborah A. Robinson in the U.S. District Court for the District of Columbia. She was ordered held pending a hearing set for July 18, 2018. According to the affidavit in support of the complaint, from as early as 2015 and continuing through at least February 2017, Butina worked at the direction of a high-level official in the Russian government who was previously a member of the legislature of the Russian Federation and later became a top official at the Russian Central Bank. This Russian official was sanctioned by the U.S. Department of the Treasury, Office of Foreign Assets Control in April 2018.

The court filings detail the Russian official's and Butina's efforts for Butina to act as an agent of Russia inside the United States by developing relationships with U.S. persons and infiltrating organizations having influence in American politics, for the purpose of advancing the interests of the Russian Federation. The filings also describe certain actions taken by Butina to further this effort during multiple visits from Russia and, later, when she entered and resided in the United States on a student visa. The filings allege that she undertook her activities without officially disclosing the fact that she was acting as an agent of Russian government, as required by law. The charges in criminal complaints are merely allegations and every defendant is presumed innocent unless and until proven guilty beyond a reasonable doubt. The maximum penalty for conspiracy is five years. The maximum statutory sentence is prescribed by Congress and is provided here for informational purposes. If convicted of any offense, a defendant's sentence will be determined by the court based on the advisory U.S. Sentencing Guidelines and other statutory factors.

The investigation into this matter was conducted by the FBI's Washington Field Office. The case is being prosecuted by the National Security Section of the U.S. Attorney's Office for the District of Columbia and the National Security Division of the U.S. Department of Justice.

Eight Arrested in Africa-Based Cybercrime and Business Email Compromise Conspiracy

In accordance with the Justice Department's recent efforts to disrupt business email compromise (BEC) schemes that are designed to intercept and hijack wire transfers from businesses and individuals, including many senior citizens, the Department announced Operation Keyboard Warrior, an effort coordinated by United States and international law enforcement to disrupt online frauds perpetrated from Africa. Eight individuals have been arrested for their roles in a widespread, Africa-based cyber conspiracy that allegedly defrauded U.S. companies and citizens of approximately $15 million since at least 2012. Acting Assistant Attorney General John P. Cronan of the Justice Department's 6

Criminal Division, U.S. Attorney D. Michael Dunavant of the Western District of Tennessee and Executive Assistant Director David T. Resch of the FBI, made the announcement today. Five individuals were arrested in the United States for their roles in the conspiracy including Javier Luis Ramos Alonso, 28, a Mexican citizen residing in Seaside, California; James Dean, 65, of Plainfield, Indiana; Dana Brady, 61, of Auburn, Washington; Rashid Abdulai, 24, a Ghanaian citizen residing in the Bronx, New York, who has been charged in a separate indictment; and Olufolajimi Abegunde, 31, a Nigerian citizen residing in Atlanta, Georgia. Maxwell Atugba Abayeta aka Maxwell Peter, 26, and Babatunde Martins, 62, of Ghana and Benard Emurhowhoariogho Okorhi, 39, a Nigerian citizen who resides in Ghana, have been arrested overseas and are pending extradition proceedings to face charges filed in the Western District of Tennessee.

The indictment also charges Sumaila Hardi Wumpini, 29; Dennis Miah, 34; Ayodeji Olumide Ojo, 35, and Victor Daniel Fortune Okorhi, 35, all of whom remain at large. Abegunde had his detention hearing today before U.S. District Court Judge Sheryl H. Lipman of the Western District of Tennessee, who ordered him detained pending trial, which has been set for Oct. 9.

"The defendants allegedly unleashed a barrage of international fraud schemes that targeted U.S. businesses and individuals, robbing them to the tune of approximately $15 million," said Acting Assistant Attorney General Cronan. "The Department of Justice will continue to work with our international partners to aggressively disrupt and dismantle criminal enterprises that victimize our citizens and businesses."

"Today, the FBI and our partners are announcing indictments as part of Operation Keyboard Warrior," said FBI Executive Assistant Director Resch.

*(*Continued On The Following Page)*

"Following the success of Operation WireWire in early June, these indictments continue to demonstrate the FBI's commitment to working with our partners around the globe to disrupt and dismantle criminal enterprises that target Americans and their businesses. This should stand as a warning that our work is not over, and we will continue to work together with our law enforcement partners to put an end to these fraud schemes. I want to thank all the agents and analysts at the FBI, our partners at the Department of Justice, and our Ghanaian partners at the Economic and Organised Crime Office for all their tireless work to continue to pursue this issue at every turn."

The indictment was returned by a grand jury in the U.S. District Court for the Western District of Tennessee on Aug. 23, 2017, and charges the defendants with conspiracy to commit wire fraud, wire fraud, conspiracy to commit money laundering, conspiracy to commit computer fraud, and aggravated identity fraud.

The indictment alleges that the Africa-based coconspirators committed, or caused to be committed, a series of intrusions into the servers and email systems of a Memphis-based real estate company in June and July 2016. Using sophisticated anonymization techniques, including the use of spoofed email addresses and Virtual Private Networks, the coconspirators identified large financial transactions, initiated fraudulent email correspondence with relevant business parties, and then redirected closing funds through a network of U.S.-based money mules to final destinations in Africa. Commonly referred to as business email compromise, or BEC, this aspect of the scheme caused hundreds of thousands in loss to companies and individuals in Memphis.

(*Continued On The Following Column)

Web Notice: The Directorate of Defense Trade Controls (DDTC) is currently in the process of modernizing its IT systems. During this time period, we anticipate there may be delays in response times and time to resolve IT related incidents and requests. We apologize for any inconvenience, and appreciate your patience while we work to improve DDTC services. If you need assistance, please contact the DDTC Service Desk at (202) 663-2838, or email at DtradeHelpDesk@state.gov (06.28.16)

"Difficult roads often lead to beautiful destinations."

In addition to BEC, some of the Africa-based defendants are also charged with perpetrating, or causing to be perpetrated, various romance scams, fraudulent-check scams, gold-buying scams, advance-fee scams, and credit card scams. The indictment alleges that the proceeds of these criminal activities, both money and goods, were shipped and/or transferred from the United States to locations in Ghana, Nigeria, and South Africa through a complex network of both complicit and unwitting individuals that had been recruited through the various Internet scams. Some of the defendants are also charged with concealing their conduct by, among other means, stealing or fraudulently obtaining personal identification information (PII) and using that information to create fake online profiles and personas. Through all their various schemes, the defendants are believed to have caused millions in loss to victims across the globe. 7

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

The FBI led the investigation. The FBI's Transnational Organized Crime of the Eastern Hemisphere Section of the Criminal Investigative Division, Major Cyber Crimes Unit of the Cyber Division, the Legal Attaché in Accra, and International Organized Crime Intelligence and Operations Center all provided significant support in this case, as did the Ghanaian Economic and Organised Crime Office, INTERPOL Washington, the U.S. Marshals Service, and the U.S. Attorney's Offices of the Northern District of Georgia, Western District of Washington, Central District of California, Southern District of New York, and the Northern District of Illinois.

Senior Trial Attorney Timothy C. Flowers of the Criminal Division's Computer Crime and Intellectual Property Section and Assistant U.S. Attorney Debra L. Ireland of the U.S. Attorney's Office for the Western District of Tennessee are prosecuting the case, with significant assistance from the Department of Justice's Office of International Affairs.