EIB World Trade Headlines

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

July 1, 2018 - Volume 10, Issue 12

FBI Boston Division: Boston Area is 'Target Rich' for Cyber Attack

The head of the FBI Boston Division is warning the threat of cyber attacks is real and the Boston area has a lot to lose.

Boston 25 News anchor Kerry Kavanaugh sat down with Special Agent in Charge Hank Shaw who says the area is "target rich" with an abundance of Fortune 500 companies, first class universities, hospitals and more.

"The threats are coming at us. They consistently change. And we have to change and adapt," said Shaw. "We have cutting edge technology happening here. We have hundreds of cleared defense contractors. The crown jewels of any numbers of businesses, private sector or academic, which could be stolen."
We have seen small scale attacks locally for years.

In 2013, cyber thieves targeted the Swansea Police Department. The same threat hit Tewksbury Police in 2015, costing them $500 in ransom.

And just in April, hackers targeted Leominster Public Schools, which paid hackers thousands to regain access to school computers.

*(*Continued On The Following Page)*

NEWSLETTER NOTES

Just this year, hackers have aimed even higher, targeting big city governments. We saw something in Atlanta. We saw in Baltimore. Could Boston be next?

Shaw said it could, but he believes the Greater Boston Area has been proactive.

"I would describe it as the forefront of engagement of cyber security threats," said Hawk.

But between phishing emails and ransomware, hackers are getting more sophisticated. Shaw says there must be a plan to respond in place before disaster strikes.

PSA: Ransomware victims urged to report infections to federal law enforcement

https://www.ic3.gov/media/2016/160915.aspx

"What they would do to be able to respond to that? What is their plan in terms of hardening their networks?

What impact would it have on that company if that information was actually lost?" said Shaw. "We have a lot to lose."

Investigators had been able to recover more than $40 million over the last years for victims. Though they can't always find the hacker, the FBI needs the suspicious emails reported. You can report any suspicious emails here.

If you would like to continue reading this article, please follow the link:

https://www.fox25boston.com/news/fbi-boston-division-boston-area-is-target-rich-for-cyber-attack

California pair guilty of illegal night vision exports
U.S.-made components made their way to Russia without required State Department licenses.

A California couple pleaded guilty in a federal court on Tuesday to their role in an illicit scheme to export night vision and thermal device components to Russia.

Specifically, Naum Morgovsky, 69, and Irina Morgovsky, 66, of Hillsborough, Calif., violated the Arms Export Control Act.

According to their guilty pleas, which were heard in a district court in Northern California, the couple carried out the scheme through their company, Hitek International, from April 2012 to Aug. 25, 2016. A Russian buyer would provide them a list of parts needed to manufacture the night vision equipment.

The couple shipped the U.S.-made components to Russia, or a European country from where they would be hand-carried into Russia, without the required U.S. export licenses from the State Department.

Naum Morgovsky attempted to hide the scheme by laundering the payments into a U.S.-based bank account under the name of a deceased person.

According to the Justice Department, the Morgovskys worked with Mark Migdal, 72, of Portola Valley, Calif. On April 24, Migdal was sentenced to 18 months in jail and ordered to pay a $1 million fine and $460,215 in restitution and to serve three years of supervised release for his role in the export scheme.

A sentencing hearing for the Morgovskys' guilty pleas is scheduled for Sept. 18. No date has been scheduled yet to resolve the remaining charges against Naum Morgovsky.

Canada, EU Join WTO Dogpile Against US Metal Duties

Law360 (June 6, 2018, 1:35 PM EDT) -- Major U.S. trading partners continued their campaign against the Trump administration's national security-based steel and aluminum tariffs on Wednesday, with both Canada and the European Union filing new World Trade Organizationcases alleging that the duties flout global trade rules.

Canadian Foreign Minister Chrystia Freeland, seen here March 5, said in a Wednesday statement that the tariffs imposed by the U.S. "are inconsistent with the United States international trade obligations and WTO rules." (AP) Following in the footsteps of both China andIndia, the EU and Canada each brought formal WTO legal action against the U.S. over its steel and aluminum tariffs after Trump moved to extend the duties to their producers last week.

The cases, announced by each respective government shortly after Trump's move, were published by the WTO on Wednesday and broadly follow in the steps of their predecessors by accusing the U.S. of using national security as a veil for economic protectionism.

"These unilateral tariffs, imposed under a false pretext of safeguarding U.S. national security, are inconsistent with the United States international trade obligations and WTO rules," Canadian Foreign Minister Chrystia Freeland said in a statement. For its part, Mexico's Secretariat of Economy has also announced that it will bring WTO action against the U.S., but the WTO has yet to publish a formal complaint from the government.

Officially, the EU and Canada have requested to hold consultations with the U.S. in an attempt to strike a mutual resolution, which is the first step in the WTO dispute settlement system. If those talks, which must be held within 30 days, do not yield any progress, both countries will be allowed to seek a panel that will adjudicate its claims against the U.S.

Both complaints claim that the law Trump used to impose the tariffs — Section 232 of the Trade Expansion Act of 1962 — is in violation of WTO rules "as such," meaning that the illegality lies with the text of the law itself, not just with how Trump is applying it in this context.

Section 232 allows the president to impose trade restrictions on certain products if he deems those imports to be a national security threat. The WTO's rules, specifically Article XXI of the General Agreement on Tariffs and Trade, allow for a national security exception, but its limits have never been tested in litigation. In its consultation request, Canada looked to head off a U.S. bid to use Article XXI, saying that Section 232 doesn't qualify for the national security exception because it requires the U.S. "to account for economic welfare and other factors that are not necessary for the protection of its essential security interests."

Trump's Steel Tariffs May Worsen Permian Pipeline Crunch

Law360 (June 6, 2018, 7:23 PM EDT) -- President Donald Trump's decision to move ahead with sweeping steel tariffs could further tighten the current pipeline logjam in the oil-rich Permian Basin of West Texas, making it tougher for producers to get their oil and gas out of the ground and into the market, experts say.

The Permian is the epicenter of U.S. crude oil production, pumping out nearly 3.3 million barrels a day, according to the latest figures from the U.S. Energy Information Administration. But that production is outpacing the capacity of existing pipeline infrastructure in the region, creating transportation bottlenecks that make Permian oil worth increasingly less compared to U.S. and global oil benchmark prices.

Now the price tag of new pipelines will grow due to the 25 percent tariffs on steel imposed by the Trump administration, as well as quotas on steel imports with few exceptions. A good portion of the steel needed to build oil pipelines simply isn't made in the U.S.

That has companies like Plains All American Pipeline LP, one of the largest crude oil transportation firms in the U.S. and a major Permian presence, sounding the alarm over a deepening pipeline crunch in the region and a growing inability to get Permian oil to refineries on the Gulf Coast.

"We need pipeline capacity in the Permian," PAA CEO Greg Armstrong said Monday at the 2018 EIA Energy Conference in Washington, D.C. "Eighty percent of a pipeline doesn't do us any good. Everyone is trying to get on a ship, and there's no room and ticket prices are going up."

Armstrong said his company is still moving ahead with projects aimed at boosting its Permian pipeline capacity by the end of 2019. But other pipeline companies may not be in the same position, experts say.

"You have a lot of planned pipeline projects in the formal planning stages, with some of the earlier projects whose in-service dates are 2019 at the earliest," Austin, Texas-based Thompson & Knight LLP counsel Nicolas A. McTyre, who previously handled pipeline issues as a Federal Energy Regulatory Commission trial attorney, said. "To the extent that any of these projects are on the economic margin, the increased costs of the pipeline steel could be something that leads to the cancellation of a project going from the Permian to the Gulf Coast."

*(*Continued On The Following Page)*

Houston-based Foley Gardere partner John Melko, who does restructuring work in the oil and gas sector, said one of his firm's major pipeline clients is already fielding higher price quotes from vendors and suppliers.

"The Permian is already constrained right now," Melko said. "It's going to make those projects a little more expensive."

And those costs are ultimately borne by the upstream sector, which is already being squeezed by higher transportation costs due to the current pipeline crunch. Crude oil delivered at Midland, Texas, in the heart of the Permian, is trading at approximately $12 a barrel lower than the U.S. benchmark price set at the trading hub of Cushing, Oklahoma, according to the latest EIA figures. That discount balloons to over $20 a barrel compared to the global Brent oil price benchmark.

"As long as that gap exists between the pipeline capacity and production, that differential could have an impact," Saad Rahim, chief economist for commodity trading giant Trafigura, said Monday at the EIA conference. "Effectively, you're turning steel into oil. As these costs play through, they're potentially put[ting] a limit on what we're seeing out there."

For oil and gas producers in the Permian, the steel tariffs represent a lose-lose proposition, experts say. Either they absorb the additional costs now rolled into the construction of new pipelines, or face even higher transportation costs if new pipelines aren't built because the tariffs no longer make them economically viable.

"If they can't get pipelines built, then they're going to be stuck with production they can't get to market, or will be suffering a significant discount due to increased transportation costs," Melko said. "It will definitely have an effect on upstream producers, especially those who have higher acquisition and drilling costs."

But upstream and midstream companies have a codependent relationship, and many midstream companies haven't recovered from the previous oil slump as quickly as their upstream counterparts.

Most major pipeline projects need to have at least one long-term upstream customer signed up before they start building, or even secure financing. Ultimately, producers are beholden to oil prices and are already dealing with a steep discount in the Permian. They won't sign up for a new pipeline if the tariff-augmented costs they have to shoulder outweigh the price they get for their oil, experts say.

*(*Continued On The Following Column)*

"The big pipelines, they already have these customers and they build on that," Houston-based King & Spalding LLP oil and gas partner Peter Hays, who works with upstream companies, said. "It's these non-big pipeline companies, the smaller midstream startups that are trying to find business on the fringes … any incremental cost can negatively affect those markets."

With the tariffs in place, shipping contracts between producers and pipeline companies should be watched carefully, Hays said. They usually contain provisions for dealing with any changes in law, and who foots the bill, after they're signed.

For contracts that are still being hammered out, producers could look to negotiate themselves a stake in a new pipeline project in order to help offset any increased shipping costs they might be hit with, Hays said.

Any further Permian pipeline crunch due to steel tariffs won't lead to a mass exodus of drillers, who have poured billions of dollars into West Texas since 2016. There's simply too much oil to be tapped and the region boasts some of the lowest drilling costs in the U.S.

But with oil prices having recovered to a level where it's profitable to drill in several other U.S. regions, the prospect of even higher transportation costs could remove a bit of the Permian's shine for some oil and gas producers, experts say.

"It will cause people to rethink, with the tariff on top of the overall transportation issues," Houston-based Paul Hastings LLP partner Doug Getten, who works in both the upstream and midstream sectors, said. "It will make people think about, if they operate in more than one basin, is there a better place to operate and deploy capital?"

Senate Begins Debate On $716B Defense Bill For 2019

Law360 (June 6, 2018, 7:18 PM EDT) -- The U.S. Senate on Wednesday kicked off a debate on its $715.9 billion version of the sweeping 2019 defense authorization bill, legislation that includes a focus on emerging technologies, a planned makeover for the U.S. Department of Defense's promotion system and other policy provisions.

Sen. Jim Inhofe, R-Okla. — serving as chairman of the Senate Armed Services Committee with the absence of Sen. John McCain, R-Ariz., due to medical treatment — described the 2019 National Defense Authorization Act, the broad annual defense policy and budget bill, as "the most important piece of legislation [the Senate] considers every year."

*(*Continued On The Following Page)*

"[The bill] takes steps to ensure we're prepared for a world defined by strategic competition with China and Russia," Inhofe said on the Senate floor.

Procedural issues will need to be addressed over the next few days, after Sen. Pat Toomey, R-Pa., objected to the Senate formally proceeding to the bill until he is guaranteed that his amendment to the Committee on Foreign Investment in the United States will be considered. Informal debate will continue in the meantime, with formal debate, amendments and a final vote expected to follow next week.

The bill, approved by the Senate Armed Services Committee in late May, differs from the $717 billion version of the NDAA recently passed by the House in a number of ways, and the two versions will ultimately have to be reconciled into a final bill.

Those differences include the total budget outlined in the bill, with the Senate's proposal falling more than a billion dollars short of the House proposal.

There are also several clashes between the bills regarding DOD aircraft programs, with the Senate bill proposing to fund 75 F-35 fighter jets in 2019, two fewer than the 77 the department has requested, alongside a suite of proposals meant to improve accountability within the F-35 program — the DOD's largest-ever procurement — and make the program more sustainable. The House bill would fully fund the DOD's F-35 request.

Also, while the House bill would withhold some funding from the Air Force unless and until it proceeds with a direct replacement for the Joint Surveillance Target Attack Radar System battlefield surveillance and command aircraft, the Senate bill instead supports the Air Force's planned advanced battle management system.

ABMS would use a network of other aircraft to replace the current JSTARS jets, which the Air Force has argued present too large a target for modern anti-aircraft systems. House lawmakers have been skeptical that ABMS is an adequate replacement for JSTARS.

But the two versions of the bill also reflect many of the same priorities. For example, both want the DOD to put more focus on emerging technologies, seeking to add additional funding in areas such as artificial intelligence and hypersonic and directed energy weapons.

Similarly, both bills call for a ban on the use of equipment made by Chinese telecommunications equipment companies Huawei Technologies Co. Ltd. and ZTE Corp. as possible vectors for Chinese espionage, although the Senate proposal limits the ban to the DOD alone, while the House bill would extend the ban to all federal agencies.

*(*Continued On The Following Column)*

In a similar vein, the Senate bill would require current and prospective defense contractors to disclose any business arrangements they have with foreign governments that would require them to hand over sensitive data, like trade secrets and computer source code, to those governments.

Senate and House lawmakers also want the DOD to put more focus on its capabilities in space, and both versions of the bill propose management shakeups at the DOD, although while the House version calls for some "Fourth Estate" agencies — those that don't report to either a military service or directly to the defense secretary — to be eliminated or restructured, the Senate bill instead directs the DOD itself to look into its "major roles and missions" and determine whether it needs to restructure to best meet its needs.

Other provisions in the Senate bill include a clause that would designate all military cyberoperations as "traditional military activities," effectively codifying that cybertroops can go on the offensive to thwart adversaries' cyberefforts.

It would also revamp the position of undersecretary of defense for personnel and readiness so the position can focus exclusively on personnel issues, while further seeking to make over the DOD's "up or out" promotion system.

Under the Senate's proposal, the military promotion system would become more flexible, for example allowing for extended timelines for those who need more time to be ready for promotion, while accelerating timelines for promotion for certain specialities.

In addition to Toomey's CFIUS proposal — seeking to make sure Congress has the ability to review new major regulations proposed by the committee — other expected proposed amendments include a proposal from Sen. Ron Johnson, R-Wis., that would allow law enforcement to bring down — either by seizing control or destroying — malicious drones in U.S. airspace.

Senate Foreign Relations Committee Chairman Bob Corker, R-Tenn., has also signaled that he plans to put forward his recently introduced legislation, which would require congressional approval for trade tariffs implemented for national security purposes, as an amendment to the NDAA.

Navy Told To Fix Shipbuilding Process As Expansion Looms

By Shayna Posses

Law360 (June 6, 2018, 6:23 PM EDT) -- The U.S. Navy could stand to make improvements to its shipbuilding programs as it plans its biggest fleet increase in more than three decades, the U.S. Government Accountability Office said Wednesday, noting that the operation has faced consistent shortcomings over the last 10 years.

The Navy intends to pump hundreds of billions of dollars into its shipbuilding programs over the next decade to meet its goal of a 355-ship fleet, creating an opportunity for the service to learn from past struggles that have led to failures to meet cost, schedule and performance goals set in 2007, according to the watchdog's report.

"The Navy will continue to face daunting acquisition challenges over the next decade as it begins a long-term effort to significantly increase the size of its fleet," the report said. "Though the Navy has started to make some improvements, its current approach to shipbuilding leaves it at risk of continually losing buying power and jeopardizes its ability to achieve its long-range shipbuilding goals."

Upon reviewing its observations about the Navy shipbuilding operation over the last 10 years, the GAO found that the service received $24 billion more in funding than originally planned but ended up with 50 fewer ships than the 330 the Navy hoped to have by 2018, the report said.

Ship costs surpassed estimates by more than $11 billion, and the construction process was plagued by yearslong construction delays, the GAO noted. When the ships did finally make it to the fleet, they often did not live up to quality and performance expectations, according to the watchdog.

A large part of the problem is the Navy's failure to consistently follow shipbuilding best practices, the watchdog found. Rather than ensuring it has all the necessary information before proceeding with shipbuilding programs, the service has a habit of diving into projects before fully understanding the resources required, GAO said.

That is partially because of the effort needed to get funding, the report noted. The process of requesting funding from Congress incentivizes floating ambitious cost, schedule and performance goals before the Navy necessarily knows the resources that will be required, according to the GAO.

*(*Continued On The Following Column)*

"Once the ship is funded and construction progresses, the gap between the over-promised ship and the reality of the shipbuilding effort becomes evident, which creates pressure as costs and schedules grow beyond initial estimates," the report said.

The Navy has put some reform efforts into action, like focusing on finishing design before constructing a ship, but poor outcomes still continue, the report noted. Of the 67 recommendations the watchdog has made for shipbuilding improvements over the last decade, the U.S. Department of Defense and the Navy have implemented only 29, and though they have agreed with the GAO's identified best practices, the Navy has not taken responsive steps in many cases, according to the report.

As the Navy stands on the cusp of efforts to substantially increase its fleet size, the service must take steps to improve shipbuilding outcomes, the GAO said. This is particularly critical to the extent that the Navy plans to meet its goals by building new ship classes, the watchdog added.

The watchdog concluded that the key to breaking "the cycle of cost growth, schedule delays, and capability shortfalls" is for decision makers in the DOD, the Navy and Congress to insist that shipbuilding programs are supported by reasonable project plans.

"Only when decision makers embrace this more disciplined approach to buying ships will acquisition outcomes improve and the needs of the fleet be consistently met," GAO said.

EU Retaliatory Duties On US Goods Slated To Hit In July

By Alex Lawson

Law360 (June 6, 2018, 11:40 AM EDT) -- The European Union announced Wednesday that its duties on more than $3 billion worth of U.S. goods will take effect in July as Brussels retaliates against the Trump administration's steel and aluminum restrictions with a 25 percent levy on U.S. metals, vehicles, food products and scores of other items.

A meeting of the EU's College of Commissioners closed with an endorsement of tariffs put forward by the government's trade wing last month. The move came just days after President Donald Trump opted to extend his national security-based steel and aluminum tariffs to the EU after talks for a bilateral resolution fell flat.

*(*Continued On The Following Page)*

"This is a measured and proportionate response to the unilateral and illegal decision taken by the United States to impose tariffs on European steel and aluminum exports," Trade Commissioner Cecilia Malmström said. "What's more, the EU's reaction is fully in line with international trade law. We regret that the United States left us with no other option than to safeguard EU interests."

The EU's list covers a wide array of items, including steel products and vehicles like motorcycles and boats. But the tariffs likely to inflict the most damage on the U.S. economy are those covering agricultural items like bourbon, peanut butter, cranberries and orange juice.

Brussels has roundly rejected the Trump administration's national security arguments for its steel and aluminum duties, accusing the U.S. of using security as a veil for economic protectionism.

This first round of tariffs is only one part of the EU's response to Trump's aggressive trade enforcement maneuver.

As it imposes the duties on $3.3 billion worth of U.S. goods starting in July, it has also teed up more tariffs covering an additional $4.2 billion in goods that will take effect in three years or whenever the World Trade Organization deems the steel and aluminum duties illegal, whichever comes first.

The EU and Mexico are said to be preparing formal WTO cases against the steel and aluminum tariffs that will be made official in the coming days. Governments like India and China have already begun dispute settlement proceedings, building pressure on the U.S. to walk back its duties.

If the cases gain traction without a negotiated resolution they will test the bounds of the WTO's so-called national security exemption.

Broadly, the WTO allows countries to impose trade restrictions on the basis of national security, but it has never had to define the scope or limit of that exception. The fear among trade liberalization advocates is that the WTO will uphold the U.S. duties and embolden other countries to follow suit with their own, essentially invincible restrictions.

For now, the EU and other countries are treating the U.S. duties not as national security measures but as safeguard tariffs, which are intended to address unexpected import surges. This strategy has enabled them to pursue swift retaliation under the WTO's Agreement on Safeguards.

ENTITIES – 31 CFR 501.805(d)(1)(i)

Ericsson, Inc. and Ericsson AB Settle Potential Civil Liability for an Apparent Violation of the Sudanese Sanctions Regulations: Ericsson AB ("EAB"), located in Sweden, and Ericsson, Inc. ("EUS"), located in Texas, both of which are subsidiaries of Telefonaktiebolaget LM Ericsson ("Ericsson"), have agreed to pay $145,893 to settle potential civil liability for an apparent violation of the International Emergency Economic Powers Act (IEEPA) and the Sudanese Sanctions Regulations, 31 C.F.R. part 538 (SSR).1

OFAC determined that Ericsson voluntarily self-disclosed the apparent violation to OFAC and that the apparent violation constitutes an egregious case. The statutory maximum civil monetary penalty amount for the apparent violation was $360,230, and the base civil monetary penalty amount was $180,115.

On or around September 22, 2011, EAB signed a letter of intent with the Sudanese subsidiary of a third-country telecommunications company in order to provide equipment and services to upgrade and expand telecommunications network coverage in Sudan starting with a test network. Ericsson opted to connect its test network in Sudan via satellite, as it had done in other underdeveloped areas. Ericsson hired BCom Offshore SAL ("BCom") to assist with installing, configuring, and servicing the satellite equipment destined for Sudan.

In late 2011, the high temperatures in Sudan caused some of Ericsson's equipment to malfunction. In response, two now former EAB employees – a radio systems expert and project manager ("EAB Employee #1"), and a senior engagement director within EAB's business unit responsible for managing the implementation of the Sudanese project ("EAB Employee #2") – contacted an EUS subject matter specialist and director of business development with EUS's Hosted Satellite Group ("EUS Employee") to request assistance. The EUS Employee initially responded in a January 2, 2012 email to EAB Employee #1 and his manager ("EAB Manager") among other EAB employees: "Please do not address any emails relating to this country [Sudan] to me. It is a serious matter and Ericsson can get fined and I can get fired."

Notwithstanding the email cited above, the EAB personnel continued to discuss how to repair the damaged equipment with the EUS Employee while no longer referencing Sudan by name. For example, on January 27, 2012, EAB Employee #1 sent an email referencing Sudan by name to the EAB Manager and EUS Employee, to which the EAB Manager responded in Swedish "do not use that word ;)." Additionally, on February 22, 2012, the EUS Employee sent an email with "East Africa" in the subject line advising EAB Employee #1 and EAB Employee #2 on how to move forward with the Sudan project given the heat constraints.

*(*Continued On The Following Page)*

On or about February 28, 2012, the EUS Employee met with EAB Employee #2 and the Chief Operating Officer (COO) of Ericsson's principal subcontractor, BCom, in Barcelona, Spain at a sales conference to specifically discuss the overheating problem in Sudan. The group decided to solve the issue by purchasing an export controlled U.S.-origin satellite hub capable of withstanding the heat.

On March 22, 2012, at the direction of Employee #1, EAB purchased a satellite hub from a U.S.- based company for delivery to BCom's office in Geneva, Switzerland. On or about March 28, 2012, EAB Employee #1 exchanged emails with Ericsson's compliance department explaining what the satellite hub was for and why its purchase was necessary. Ericsson's compliance department informed EAB Employee #1 that the supply of such a satellite hub to Sudan would violate Ericsson's internal policy regarding sanctions compliance.

Despite the information from Ericsson's compliance department, the EUS Employee, EAB Employee #1, and BCom's COO agreed to provide the location of the customer purchasing the satellite hub as "Botswana" if future questions arose. Subsequently, on or about April 2, 2012, EAB Employee #1 structured Ericsson's purchase of the satellite hub into a multistage transaction between EAB and BCom. The multistage transaction involved transshipping the hub through Switzerland and Lebanon, and ultimately to Sudan. Every stage of the transaction except the last was invoiced. BCom did not issue an invoice to EAB for the final stage of the transaction taking the satellite hub from Lebanon to Sudan. Ericsson has since terminated its relationship with BCom.

For more information regarding this matter, please see the Settlement Agreement between OFAC and EAB and EUS here.

The settlement amount reflects OFAC's consideration of the following facts and circumstances, pursuant to the General Factors under OFAC's Economic Sanctions Enforcement Guidelines, 31 C.F.R. part 501, app. A. OFAC considered the following to be aggravating: (1) several EAB employees and an employee of EUS willfully violated the SSR by forming a conspiracy with the employees of a third-country company with the specific purpose of evading the U.S. embargo on Sudan; (2) at least one of the EAB employees involved was a manager; (3) those employees ignored warnings from Ericsson's compliance department that the transaction at issue was prohibited; (4) EAB's actions caused harm to the sanctions program objectives with respect to Sudan; and (5) Ericsson is a large and commercially sophisticated entity.

OFAC considered the following to be mitigating: (1) Ericsson cooperated with OFAC by filing a voluntary self-disclosure, performing a thorough internal investigation, and signing a tolling agreement;

*(*Continued On The Following Column)*

(2) neither Ericsson, EUS, nor EAB have received a penalty notice or finding of violation from OFAC in the five years preceding the date of the transaction giving rise to the apparent violation; (3) Ericsson's remedial response to the apparent violation and adoption of additional compliance controls and procedures; and (4) the low likelihood of recurrence given the individual characteristics of the apparent violation.

This enforcement action highlights the importance of empowering compliance personnel to prevent transactions prohibited by U.S. economic and trade sanctions. Entities should ensure their sanctions compliance teams are adequately staffed, receive sufficient technology and other resources, and are delegated appropriate authority to ensure compliance efforts meet an entity's risk profile. Sanctions compliance personnel should be equipped with the tools necessary to review, assess, and proactively address sanctions-related issues that arise with ongoing or prospective transactions, customers, or counter-parties.

For more information regarding OFAC regulations, please go to: http://www.treasury.gov/ofac.

Justice Department Announces Actions to Disrupt Advanced Persistent Threat 28 Botnet of Infected Routers and Network Storage Devices Additional action necessary worldwide to remediate the botnet.

The Justice Department today announced an effort to disrupt a global botnet of hundreds of thousands of infected home and office (SOHO) routers and other networked devices under the control of a group of actors known as the "Sofacy Group" (also known as "apt28," "sandworm," "x-agent," "pawn storm," "fancy bear" and "sednit"). The group, which has been operating since at least in or about 2007, targets government, military, security organizations, and other targets of perceived intelligence value.

Assistant Attorney General for National Security John C. Demers, U.S. Attorney Scott W. Brady for the Western District of Pennsylvania, Assistant Director Scott Smith for the FBI's Cyber Division, FBI Special Agent in Charge 4

*(*Continued On The Following Page)*

Robert Johnson of the Pittsburgh Division and FBI Special Agent in Charge David J. LeValley of the Atlanta Division made the announcement. “The Department of Justice is committed to disrupting, not just watching, national security cyber threats using every tool at our disposal, and today’s effort is another example of our commitment to do that,” said Assistant Attorney General Demers. “This operation is the first step in the disruption of a botnet that provides the Sofacy actors with an array of capabilities that could be used for a variety of malicious purposes, including intelligence gathering, theft of valuable information, destructive or disruptive attacks, and the misattribution of such activities.” “The United States Attorney’s Office will continue to aggressively fight against threats to our national security by criminals, no matter who they work for” said U.S. Attorney Brady. “This court-ordered seizure will assist in the identification of victim devices and disrupts the ability of these hackers to steal personal and other sensitive information and carry out disruptive cyber attacks. We will be relentless in protecting the people of Western Pennsylvania - from international corporations to local businesses to the elderly - from these threats.” “Today's announcement highlights the FBI's ability to take swift action in the fight against cybercrime and our commitment to protecting the American people and their devices,” said Assistant Director Scott Smith. “By seizing a domain used by malicious cyber actors in their botnet campaign, the FBI has taken a critical step in minimizing the impact of the malware attack. While this is an important first step, the FBI's work is not done. The FBI, along with our domestic and international partners, will continue our efforts to identify and expose those responsible for this wave of malware.” “The FBI will not allow malicious cyber actors, regardless of whether they are state-sponsored, to operate freely,” said FBI Special Agent in Charge Bob Johnson. “These hackers are exploiting vulnerabilities and putting every American’s privacy and network security at risk. Although there is still much to be learned about how this particular threat initially compromises infected routers and other devices, we encourage citizens and businesses to keep their network equipment updated and to change default passwords.” “This action by the FBI, DOJ, and our partners should send a clear message to our adversaries that the U.S. Government will take action to mitigate the threats posed by them and to protect our citizens and our allies even when the possibility of arrest and prosecution may not be readily available,” said FBI Special Agent in Charge David J. LeValley. “As our adversaries’ technical capabilities evolve, the FBI and its partners will continue to rise to the challenge, placing themselves between the adversaries and their intended victims.” The botnet, referred to by the FBI and cyber security researchers as “VPNFilter,” targets SOHO routers and network-access storage (NAS) devices, which are hardware devices made up of several hard drives used to store data in a single location that can be accessed by multiple users. The VPNFilter botnet uses several stages of malware. Although the second stage of malware, which has the malicious capabilities described above,

*(*Continued On The Following Column)*

can be cleared from a device by rebooting it, the first stage of malware persists through a reboot, making it difficult to prevent reinfection by the second stage. In order to identify infected devices and facilitate their remediation, the U.S. Attorney’s Office for the Western District of Pennsylvania applied for and obtained court orders, authorizing the FBI to seize a domain that is part of the malware’s command-and-control infrastructure. This will redirect attempts by stage one of the malware to reinfect the device to an FBI-controlled server, which will capture the Internet Protocol (IP) address of infected devices, pursuant to legal process. A non-profit partner organization, The Shadowserver Foundation, will disseminate the IP addresses to those who can assist with remediating the VPNFilter botnet, including foreign CERTs and internet service providers (ISPs). Owners of SOHO and NAS devices that may be infected should reboot their devices as soon as possible, temporarily eliminating the second stage malware and causing the first stage malware on their device to call out for instructions. Although devices will remain vulnerable to reinfection with the second stage malware while connected to the Internet, these efforts maximize opportunities to identify and remediate the infection worldwide in 5

Frequently Asked Questions (FAQ) on the Superseding Settlement Agreement with ZTE

Question: Is ZTE still on the Denied Persons List?

Answer: Yes. BIS and ZTE have reached a superseding settlement agreement. Under the terms of the agreement, once ZTE pays a civil penalty of $1 billion dollars to the Department of Commerce and places an additional $400 million into an escrow account in a U.S. bank approved by BIS, BIS will terminate the denial order that BIS issued on April 15, 2018 (“April 15, 2018 Order”) (83 FR 17644) against ZTE. When the denial order is terminated BIS will notify the public that ZTE has been removed from the Denied Persons List. Until then, the company will remain subject to the terms and prohibitions of that listing.

Question: When will the April 15, 2018 Order be lifted?

Answer: The April 15, 2018 Order will not be lifted until ZTE has paid $1 billion and placed an additional $400 million in an escrow account in a U.S. bank approved by BIS. Question: Will BIS make an announcement when the April 15th denial order is lifted?

Answer: Yes.

*(*Continued On The Following Page)*

Question: Can I export, reexport, or transfer (in-country) items subject to the EAR to ZTE?

Answer: No, you may not engage in those activities until the restrictions of the April 15, 2018 Order have been lifted.

Note that the lifting of the April 15, 2018 Order will not relieve persons of obligations under part 744 of the Export Administration Regulations (15 CFR 730 – 774) (EAR) or any other part of the EAR, including for example the Entity List.

Question: If and when the April 15, 2018 Order is lifted, should I do business with ZTE?

Answer: BIS cannot advise you on this issue; every company must make its own business decisions. Note that if and when the restrictions of the April 15, 2018 Order have been lifted, the obligations of the EAR continue to apply.

Question: What do I do with items that were transferred in violation of the April 15, 2018 Order?

Answer: If you suspect a violation of the EAR, you should file a voluntary self-disclosure with the Office of Export Enforcement under §764.5 of the EAR. You may also seek permission from BIS to engage in certain activities under §764.5(f) of the EAR once a disclosure is filed.

Question: I submitted a waiver request under §764.3(a)(2) of the EAR. Is BIS going to issue any waivers?

Answer: BIS continues to review waiver requests submitted specific to the April 15, 2018 Order.

Question: If and when the restrictions of the April 15, 2018 Order are lifted, will I need to do anything to follow up on my §764.3(a)(2) waiver request?

Answer: No, you won't. If and when the restrictions of the April 15, 2018 Order are lifted, that action will render all such requests moot. Please note that while §764.3(a)(2) waiver requests (which pertain to future exports or activities, not past misdeeds) may be rendered moot, any violations of the April 15, 2018 Order while it remains in effect would not be mooted or absolved even if that Order is later lifted.

Pentagon Bans Sale of Chinese 'Spy Phones' on US Military Bases

May 3, 2018

The Pentagon has banned the sale of Chinese-made Huawei and ZTE phones on US military bases, over fears that they may be hacked and used for espionage purposes by the Chinese government.

"Huawei and ZTE devices may pose an unacceptable risk to Department's personnel, information and mission," Pentagon spokesman Major Dave Eastburn told CNET on Wednesday. "In light of this information, it was not prudent for the Department's exchanges to continue selling them to DoD personnel."

While the Chinese-made phones will no longer be sold at Exchange stores on bases, personnel will still be allowed to purchase them elsewhere. Eastburn said that the Department of Defense is still mulling issuing a wider advisory on the phones.

Immediately after the ban was announced, Huawei and ZTE phones were also pulled from the military's online Exchange store.

Wednesday's ban comes after six top US intelligence chiefs voiced concerns about the phones to the Senate Intelligence Committee in February. All six intelligence bosses testified that they would never use a Huawei or ZTE phone.

"We're deeply concerned about the risks of allowing any company or entity that is beholden to foreign governments that don't share our values to gain positions of power inside our telecommunications networks," FBI Director Chris Wray stated. "It provides the capacity to maliciously modify or steal information. And it provides the capacity to conduct undetected espionage."

Huawei tried to break into the US market earlier this year through a partnership with carrier AT&T. The deal was axed, however, reportedly due to lobbying from the government. Last month the US Commerce Department banned American companies from exporting products and services to ZTE.

Iran Likely to Retaliate with Cyberattacks after Nuclear Deal Collapse

Businesses in the US, Europe, and their allies — like Saudi Arabia and Israel — are also at risk of cyberattacks.
Iran is likely to respond with cyberattacks against Western businesses in response to the Trump administration's withdrawal from the nuclear deal, cybersecurity experts say.
Research out Wednesday suggests attacks could come "within months, if not faster," according to security firm Recorded Future.
The research paints a detailed picture of how Iran uses contractors and universities to staff its offensive cybersecurity operations -- or hacking efforts -- against foreign targets.
A former insider with knowledge of Iran's hacking operations said the attacks are likely to be launched by contractors and thus pose a greater risk of spinning out of control.
On Tuesday, President Donald Trump announced the US would withdraw from the Iran nuclear deal, a pact of Western nations that pledged to lift economic sanctions against Iran in exchange for limiting its nuclear program. The UN's nuclear verification agency said Iran had complied with the agreement. 9

Although there has been no evidence or intelligence to suggest a cyberattack is in the works, researchers say they predict, based on Iran's past cyber activities, that retaliatory cyberattacks are likely.
"We assess that within months, if not sooner, American companies in the financial, critical infrastructure, oil, and energy sectors will likely face aggressive and destructive cyberattacks by Iranian state-sponsored actors," said Priscilla Moriuchi, a former NSA analyst, now at Recorded Future.
"The Islamic Republic may utilize contractors that are less politically and ideologically reliable -- and trusted -- and as a result, could be more difficult to control," she said.
Countries allied with the US and Europe -- like Saudi Arabia and Israel -- are also at risk, the report said.
Levi Gundert, who co-authored the research, told ZDNet the attacks will likely aim for "maximum impact," such as a malware attack rather than a denial-of-service attack.

*(*Continued On The Following Column)*

"Stay positive, work hard, make it happen."

Much of the research is centered on Iran's long-known history of targeting Western businesses and governments with cyberattacks in response to sanctions, largely because of how quickly the hackers could turn around an attack.
Tehran began strengthening its cyber capabilities following the Green Revolution, a period of intense protests in Iran against the incumbent government during the Arab Spring in 2009.
The government responded with a heavy crackdown, with an increased focus on cyber operations.
But some of the best hackers available were primarily young and financially driven, said the report. This led to mistrust and fears that the hackers could be bought by foreign intelligence agencies.
According to the former insider, that led to a tiered trust system that centered Tehran's hacking efforts around a central team of trusted and ideologically aligned middle management that dishes out assignments to contractors -- often pitting teams against each other -- who get paid only when the work is completed. The government also uses compartmentalization -- giving one team an infiltration mission and using another to launch a remote code execution attack.
It's estimated that at least 50 organizations are competing for government hacking work, the research said, including contractors and universities to conduct hacking operations.
One such institution, Imam Hossein University, was sanctioned by the US Treasury for its connections to the Islamic Revolutionary Guard Corps (IRGC), Iran's military intelligence unit.
But because some of Iran's best operators "are not always the most devout or loyal to the regime," the researchers warn they "could be more difficult to control." That may lead to the IRGC choosing a less ideologically driven contractor, capable of delivering a destructive attack in a short period of time, instead of a trusted and less politically driven contractor.
"It is possible that this dynamic could limit the ability of the government to control the scope and scale of these destructive attacks once they are unleashed," the researchers said.