EIB World Trade Headlines

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

January 15, 2016 - Volume 8, Issue 1

DEPARTMENT OF THE TREASURY

Office of Foreign Assets Control

31 CFR Part 578

Cyber-Related Sanctions Regulations

AGENCY: Office of Foreign Assets Control, Treasury. **ACTION:** Final rule.

SUMMARY: The Department of the Treasury's Office of Foreign Assets Control (OFAC) is issuing regulations to implement Executive Order 13694 of April 1, 2015 (''Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities''). OFAC intends to supplement this part 578 with a more comprehensive set of regulations, which may include additional interpretive and definitional guidance and additional general licenses and statements of licensing policy.

DATES: *Effective:* December 31, 2015. **FOR FURTHER INFORMATION CONTACT:** The

Department of the Treasury's Office of Foreign Assets Control: Assistant Director for Licensing, tel.: 202–622– 2480, Assistant Director for Regulatory Affairs, tel.: 202–622–4855, Assistant

*(*Continued On The Following Page)*

NEWSLETTER NOTES

***Cyber-Related Sanctions Regulations**

***Stag Down: Feds Revoke AR-15 Manufacturer's License …**

***The FBI Issues Warnings about an Email Scam …**

***The Pentagon Will Step up Cyber-Security Training…**

***Cloud More at Risk than Ever, Says Report**

***CSC, NetCracker Fined for Using Uncleared Coders…**

***Woods Hole Oceanographic Institution Says Hack …**

***IRANIAN COMPANY SENTENCED …**

***U.S. State Department, Directorate of Defense Trade Controls**

***Guidance on Charging and Penalty Determinations**

***Russian Sanctions: Addition of Certain Persons…**

***Watch an awesome flyover of a B-2 Spirit Stealth Bomber**

Background

On April 1, 2015, the President issued Executive Order 13694 (80 FR 18077, April 2, 2015) (E.O. 13694), invoking the authority of, *inter alia,* the International Emergency Economic Powers Act (50 U.S.C. 1701–1706). OFAC is issuing the Cyber-Related Sanctions Regulations, 31 CFR part 578 (the ''Regulations''), to implement E.O. 13694, pursuant to authorities delegated to the Secretary of the Treasury in E.O. 13694. A copy of E.O. 13694 appears in Appendix A to this part.

The Regulations are being published in abbreviated form at this time for the purpose of providing immediate guidance to the public. OFAC intends to supplement this part 578 with a more comprehensive set of regulations, which may include additional interpretive and definitional guidance, including regarding ''cyber-enabled'' activities, and additional general licenses and statements of licensing policy. The appendix to the Regulations will be removed when OFAC supplements this part with a more comprehensive set of regulations.

NEW RULE WILL INCLUDE A NEW LISTING OF PROHIBITED PARTIES IN SDN ''[CYBER].''

Subpart B—Prohibitions § 578.201 Prohibited transactions.

All transactions prohibited pursuant to Executive Order 13694 of April 1, 2015, are also prohibited pursuant to this part.

Note 1 to § 578.201: The names of persons designated pursuant to Executive Order 13694, whose property and interests in property therefore are blocked pursuant to this section, are published in the **Federal Register** and incorporated into OFAC's Specially Designated Nationals and Blocked Persons List (SDN List) with the identifier ''[CYBER].'' The SDN List is accessible through the following page on OFAC's Web site: *www.treasury.gov/sdn*. Additional information pertaining to the SDN List can be found in Appendix A to this chapter. *See*

§ 578.406 concerning entities that may not be listed on the SDN List but whose property and interests in property are nevertheless blocked pursuant to this section.

Note 2 to § 578.201: **The International Emergency Economic Powers Act (50 U.S.C. 1701–1706), in Section 203 (50 U.S.C. 1702), authorizes the blocking of property and interests in property of a person during the pendency of an investigation. The names of persons whose property and interests in property are blocked pending investigation pursuant to this section also are published in the** Federal Register **and incorporated into the SDN List with the identifier ''[BPI–CYBER]''.**

Stag Down: Feds Revoke AR-15 Manufacturer's License For Sloppy Record-Keeping

Stag Arms, the Connecticut-based AR-15 manufacturer, has lost it's federal firearms license as a result of not properly keeping track of serialized lower receivers.

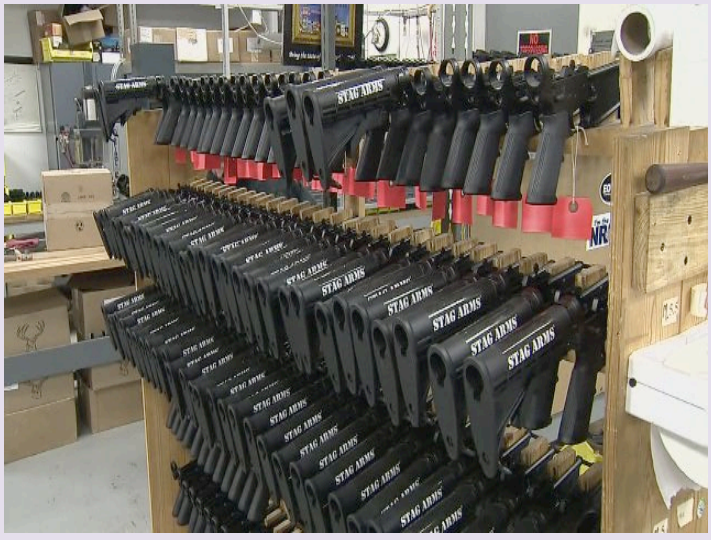
New Britain-based Stag Firearms LLC pleaded guilty Tuesday to violating federal firearms laws and as part of a plea agreement company president and owner Mark Malkowski agreed to sell the company and have no further ownership or management role in a gun manufacturer.

The company, with Malkowski serving as its representative, pleaded guilty in U.S. District Court in Hartford to a single felony count of possession of a machine gun not registered to the company.

The Bureau of Alcohol, Tobacco and Firearms is also revoking Stag's federal license to manufacture firearms.

Malkowski is also scheduled to plead guilty Wednesday in U.S. District Court in New Haven to a misdemeanor count of failure to maintain firearms records.

The federal government began its investigation of Stag in July 2014, after a routine Bureau of Alcohol, Tobacco and Firearms inspection turned up a variety of recording keeping violations, missing firearms and unregistered firearms, the government said.



The guilty plea, Stag said in a prepared statement, was in the best interest of the company and its approximately 100 employees. Malkowski is in advanced talks with a New York private equity firm to sell the company, Stag and the government said.

"For the first time in Connecticut, and there have only been a few of these prosecutions throughout the nation, a large manufacturer is pleading guilty to a felony charge relating to record keeping violations," Connecticut U.S. Attorney Deirdre M. Daly said Tuesday. The company will pay a fine of $500,000 as part of the plea agreement.

For his guilty plea, Malkowski, 37, will pay a $100,000 fine and will not be permitted to own, operate or manage a firearms company.

As we noted earlier this year, Stag Arms was raided for stupidity, not criminal enterprise. They did not properly serialize and track lower receivers at the time of their creation as required by law, and are receiving a harsh penalty as a result.

It is unclear at this time what will become of the company or it's employees as a result of the plea deal.

Update: A statement from Stag Arms.

"Stag Arms, LLC today announced that the company and its founder, Mark Malkowski, have reached a resolution with government officials stemming from an investigation that began last year relating primarily to the timing of recordkeeping during the manufacturing process and compliance with federal firearms manufacturing and registration requirements. Both Stag Arms and Mr. Malkowski cooperated fully with the government throughout the investigation. While both Stag Arms and Mr. Malkowski believe that public safety was never compromised, they have agreed to enter guilty pleas and to pay significant fines, because doing so is in the best interests of the company and its employees. Mr. Malkowski has also agreed to transition the business to new ownership and is in advanced talks with a potential buyer. Mr. Malkowski will continue as a marketing consultant to the business and the industry for a period of time following the sale. Stag Arms takes its obligations to comply with all laws and regulations very seriously and has made comprehensive changes to ensure that similar problems cannot happen again and that best compliance practices are maintained in all of its operations."

The FBI Issues Warnings about an Email Scam That's Stolen More Than $1.2 Billion

The Federal Bureau of Investigations (FBI) put out a pair of warnings in recent weeks regarding a fraud scheme that involves email, wire transfers, checks, and international business. The target of these schemes are businesses that work with foreign suppliers and those that perform wire transfer payments.

The warnings state that since January, the number of victims has nearly tripled, at an increase of 270 percent. Victims have been reported in all 50 U.S. states and across 79 different countries. More than 8,000 victims and $800 million in losses later, the report dives into how social engineering and phishing have been the point of attack. Once the target is compromised (potentially you), the attacker conducts unauthorized transfers of funds, typically stealing through wire transfers. Once the international law enforcement reports are tallied into the figure, the losses total more than $1.2 billion. One of the biggest hauls on record comes from the networking company known as Ubiquiti Networks, which reports that cyber thieves stole $46.7 million with this scam.
Common methods, direct targets The culprit here in most cases is phishing, and more specifically, spearphishing. The intended victim will receive a link with a malicious payload in their email, which will appear to come from a valid source. Once the victim clicks the link the malware is installed. Next thing you know, usernames, passwords financial information, etc. is all theirs. The bottom line: If you work in international business, and you wire transactions, you might be a target. The FBI prescribes awareness and detection, as well as a few common sense things to avoid being a victim.

Possible ways to protect yourself, or your business:
· Create intrusion detection system rules that flag emails with extensions that are similar to company email. For example, legitimate email of abc_company.com would flag fraudulent email of abc-company.com.
· Register all company domains that are slightly different than the actual company domain.
· Verify changes in vendor payment location by adding additional two-factor authentication such as having a secondary sign- off by company personnel.
· Confirm requests for transfers of funds. When using phone verification as part of the two-factor authentication, use previously known numbers, not the numbers provided in the email request.
· Know the habits of your customers, including the details of, reasons behind, and amount of payments.
· Carefully scrutinize all email requests for transfer of funds to determine if the requests are out of the ordinary.

The Pentagon Will Step up Cyber-Security Training for Small Defense Contractors

The Department of Defense will help small defense contractors protect their networks from increasingly threatening cyber actors who are stealing trade secrets and waging economic espionage.

The Pentagon will step up its efforts after a Government Accountability Office (GAO) report criticized it for failing to offer these smaller companies adequate support.
The entire U.S. defense-contractor field faces a rising tide of cyberattacks, but small businesses in particular lack the resources to defend themselves. Major contractors like Boeing and Lockheed Martin have larger cybersecurity budgets and can hire more researchers and engineers to bolster their defenses.

In the face of the sustained theft and espionage campaigns against its corporate partners, the Pentagon will begin hosting training events and education programs for employees of the smaller companies. The new policy aligns with the Defense Department's goal, outlined in its 2015 Cyber Strategy, of stepping up its partnership with the private sector to defend American networks.

Small defense companies accounted for $55.5 billion in Pentagon contracts in 2014, about 12 percent of the military's total budget.

The Pentagon acknowledged the GAO report's findings and pledged a new approach to cybersecurity for small military contractors.

"Future outreach by the [Department of Defense Office of Small Business Programs] will increase awareness of cybersecurity education for its stakeholders," OSBP director Kenyata Wesley wrote in response to the report. "The DoD OSBP will also increase awareness of the cybersecurity education resources among the DoD Small Business workforce through training events, education programs and by issuing guidance to the Military Departments and Defense Agencies."
The most pressing cyber threats identified in the report included botnets, independent criminals, hacktivists, insider threats (namely rogue employees), terrorist groups, and nation-states.

http://www.dailydot.com/politics/pentagon-cyberattack-small-businesses-contractors/

*(*Continued On The Following Column)*

Cloud More at Risk than Ever, Says Report

Cyber-criminals and hackers are increasingly attacking cloud infrastructure, which they see as a "fruit bearing jackpot" as more organisations are making use of the public cloud to store their data than ever before, a security company claims. While organisations are embracing the cloud, a report by security-as-a-service provider Alert Logic suggests that IT decision makers shouldn't assume that data they store off-premises is harder to acquire.

The company warns there has been a 45% increase in application attacks against cloud deployments.
Alert Logic bases its findings on an analysis of one billion events in the IT environments of more than 3,000 of its customers between January 1st and December 31st 2014, which revealed more that 800,000 security incidents.

One of the key findings was an increase in attack frequency on organisations that store their infrastructure in the cloud.
"This is not surprising," says the Alert Logic Cloud Security Report. "Production workloads, applications and valuable data and shifting to cloud environments and so are attacks.

"Hackers, like everyone else, have a limited amount of time to complete their job," the report continues, adding "They want to invest their time and resources into attacks that will bear the most fruit: businesses using cloud environments are largely considered that fruit bearing jackpot."
http://www.itsecurityguru.org/2015/10/07/cloud-more-at-risk-than-ever-says-report/

CSC, NetCracker Fined for Using Uncleared Coders in Classified DISA Work

Two companies accused of using employees without security clearances to work on sensitive Defense Information Systems Agency software projects agreed to pay over $12 million to resolve claims they violated the False Claims Act.
Waltham, Mass.-based telecom software and services firm NetCracker Technology Corp. agreed to pay $11.4 million and Falls Church, Va.-based information technology firm Computer Sciences Corp. agreed to pay $1.35 million to settle the case, according to the Justice Department.

According to a Nov. 2 Justice Department statement, NetCracker and CSC implemented software that used to help manage the telecommunications network used by the Department of Defense, under a contract with DISA, in which CSC was the prime contractor and NetCracker was a CSC subcontractor.

*(*Continued On The Following Page)*

Between 2008 and 2013, NetCracker allegedly used employees who lacked security clearances to perform work when it knew the contract required those individuals to have clearance, resulting in CSC recklessly submitting false claims for payment to DISA.

An investigation from Public Integrity**,** which sourced recently unsealed court documents in the case, revealed that a whistleblower discovered the companies used Russian computer programmers to write software for the sensitive U.S. military project -- potentially opening up the Pentagon's communications systems to cyberattacks.

Army contractor John Kingsley alleged, according to 2011 court documents, that the code written by the programmers included "numerous viruses" that could have harmed DOD networks. The reason the companies used the foreign programmers, he said, was because they worked for one-third the rate of U.S. programmers.

The Justice Department said Kingsley will receive $2,358,750 as his share of the recovery in the case.

https://fcw.com/articles/2015/11/05/contracting-fines-russian-programmers.aspx

Woods Hole Oceanographic Institution Says Hack Linked to China

Woods Hole Oceanographic Institution, a private, nonprofit facility that does scientific research on the world's oceans, says it was the target of an "aggressive" cyberattack it believes to have originated in China.
The hackers gained access to Woods Hole data and email, WHOI President and Director Mark Abbott told staff in a letter this week.

Christopher Land, WHOI's general counsel and leader of its internal investigation, told NBC News on Friday there's no indication to date that the stolen data has been used maliciously.

In addition to marine and oceanic research, Woods Hole also does classified work for the Defense Department. Data related to that work is stored on a separate computer system and was not affected by the breach, Land said.

*(*Continued On The Following Column)*

"The attack was similar to those that have been experienced by many federal agencies, defense contractors and other businesses developing advanced technologies. The investigation of the attack is ongoing, however, the investigation indicates the intent was not to obtain financial or personal identity information," Abbott's letter said.
Abbott said WHOI hired cybersecurity firm Mandiant to investigate after WHOI's cybersecurity system detected the intrusion in June. WHOI said didn't disclose the breach until this week in part because Mandiant didn't want to "tip off" the intruders.

"Our cybersecurity firm identified evidence of attacker activity attributed to a targeted threat group, which the firm believes was made by an Advanced Persistent Threat (APT) group based in China," Abbott said in his letter. "These conclusions were based on the firm's experience investigating these types of attacks and the group's distinct tools, tactics, and procedures."

On Tuesday, the oceanographic institution, based in Woods Hole, Massachusetts, ordered its roughly 1,100 employees and 300 affiliated staff to change their email passwords.
http://www.nbcnews.com/tech/security/woods-hole-oceanographic-institution-says-hack-linked-china-n446226

IRANIAN COMPANY SENTENCED FOR U.S. EXPORT VIOLATION

HARRISBURG - The United States Attorney's Office for the Middle District of Pennsylvania and the Office of Export Enforcement of the United States Department of Commerce announced that FIMCO, an Iranian corporation, was sentenced today to pay a $100,000 criminal fine by United States District Court Judge Yvette Kane in Harrisburg for conspiracy to evade export licensing requirements.

The conspiracy was in connection with an attempt to smuggle to Iran a machine with possible military as well as civilian applications.

According to U.S. Attorney Peter Smith, in December 2012, a federal grand jury in Harrisburg charged FIMCO in a sealed indictment made public in July 2015. In April 2014, an American company, Hetran, Inc., an engineering and manufacturing corporation in Orwigsburg, Schuylkill County, Pennsylvania, and its President, Helmut Oertmann, were charged with participating in the conspiracy. A guilty plea was entered on behalf of the corporation in July 2015 before United States Magistrate Judge Susan E. Schwab.
Hetran manufactured a large horizontal lathe, also described as a bar peeling machine ("peeler"), valued at more than $800,000 and weighing in excess of 50,000 pounds. The machine is used in the production of high grade steel for the manufacture of automobile and aircraft parts.

*(*Continued On The Following Page)*

Under U.S. law and regulations, American companies are forbidden to ship “dual use” items (items with civilian as well as military or proliferation applications), such as the peeler, to Iran without first obtaining a license from the U.S. Government. Aware that it was unlikely that such a license would be granted, FIMCO, which does business in Dubai, United Arab Emirates, and other alleged co-conspirators agreed to falsely state on the shipping documents that the end-user of the peeler was Crescent International Trade and Services FZE (Crescent), an affiliated company, knowing that the machine would subsequently be shipped to Iran after being off-loaded in Dubai.

In June 2012, Hetran caused the peeling machine to be shipped from Pennsylvania to Dubai in the United Arab Emirates, fraudulently listing Crescent as the end-user, knowing that the shipment was ultimately being sent by FIMCO to Iran in violation of federal law. The Office of Export Enforcement, Bureau of Industry and Security (BIS), U.S. Department of Commerce detected the shipment and ordered that it be re-delivered to the United States. The seizure of key shipping documents, emails and correspondence from Hetran to Iran revealed the scheme, and was critical to the success of the case, and to shutting down the contemplated shipment.

As part of its plea agreement with the United States, FIMCO agreed that the government would recommend a criminal fine. The company also has agreed under a settlement with BIS to pay a $837,500 civil penalty to the U.S. Department of Commerce, of which it paid $587,500 out-of-pocket, with the remaining $250,000 suspended for two years. The suspended portion of the civil penalty will be waived thereafter so long as FIMCO complies with the terms of the plea agreement and any criminal sentence and satisfies certain additional conditions. FIMCO will also be made subject to a two-year suspended denial of its export privileges.

"The penalty imposed today, together with the six-figure administrative penalty being paid by FIMCO to the Department of Commerce, reflects the seriousness of the violation, said Under Secretary of Commerce Eric L. Hirschhorn. The Office of Export Enforcement will continue to pursue and fully prosecute those who violate our export control laws and threaten our national security."

*(*Continued On The Following Column)*

During the investigation by the Department of Commerce’s Bureau of Industry and Security (BIS), FIMCO and Crescent were placed on BIS’s Entity list in August 2014. The Entity List identifies foreign parties that are prohibited from receiving listed items unless the exporter secures a license. Those persons present a greater risk of diversion to weapons of mass destruction (WMD) programs, terrorism, or other activities contrary to U.S. national security or foreign policy interests. By publicly listing such persons, the Entity List serves as an important tool to prevent unauthorized trade in such items. In December 2014, Helmut Oertmann and Hetran were sentenced by Judge Kane to 12 months’ probation; Oertmann and Hetran were ordered as part of a settlement with BIS to pay a penalty of $837,500 with $337,500 of that amount paid out-of-pocket and the remainder conditionally suspended, which penalty Judge Kane adopted as to Oertmann and Hetran. The other indicted company, Crescent International Trade and Services FZE, and the three Iranian individuals who served as officers of FIMCO, Khosrow Kasraei, Reza Ghoreishi, and Mujahid Ali, are presently fugitives.

The case was investigated by the New York Field Office of the Office of Export Enforcement, Bureau of Industry and Security, Department of Commerce. The Department of Commerce’s Office of the Chief Counsel for Industry and Security handled the civil proceedings. The prosecution was handled by Assistant U.S. Attorney Christy H. Fawcett and was overseen by the National Security Division of the U.S. Department of Justice.

U.S. State Department, Directorate of Defense Trade Controls

Web Notice: A proposed revision to the "Guidelines for Preparing Agreements" has been posted for public comment. Comment period ends February 5, 2016. Comments should be emailed to DDTCResponseTeam@state.gov with the subject line "Agreement Guidelines. (1.06.16)
http://www.pmddtc.state.gov/Licensing/documents/DraftGuidelinesforPreparingAgreementsRev43.pdf

DEPARTMENT OF COMMERCE
Bureau of Industry and Security

15 CFR Part 766
[Docket No. 151204999-5999-01]
RIN 0694-AG73

Guidance on Charging and Penalty Determinations in Settlement of Administrative Enforcement Cases, Revision of Supplement No. 1 to Part 766 of the Export Administration Regulations

AGENCY: Bureau of Industry and Security, Commerce.

ACTION: Proposed rule.

SUMMARY: This proposed rule would revise Bureau of Industry and Security's (BIS) guidance regarding administrative enforcement cases based on violations of the Export Administration Regulations (EAR). The rule would rewrite Supplement No. 1 to part 766 of the EAR, setting forth the factors BIS considers when setting penalties in settlements of administrative enforcement cases and when deciding whether to pursue administrative charges or settle allegations of EAR violations. This proposed rule would not apply to alleged violations of part 760—Restrictive Trade Practices and Boycotts, which would continue to be subject to Supplement No. 2 to part 766. BIS is proposing these changes to make administrative penalties more predictable to the public and aligned with those promulgated by the Department of the Treasury, Office of Foreign Assets Control (OFAC).

DATES: Comments must be received no later than February 26, 2016.

ADDRESSES: You may submit comments by any of the following methods:
Federal eRulemaking Portal: http://www.regulations.gov. The identification number for this rulemaking is BIS–2015–0051.

By email directly to: publiccomments@bis.doc.gov. Include RIN 0694–AG73 in the subject line.
By mail or delivery to Regulatory Policy Division, Bureau of Industry and Security, U.S. Department of Commerce, Room 2099B, 14th Street and Pennsylvania Avenue NW, Washington, DC 20230. Refer to RIN 0694–AG73.

FOR FURTHER INFORMATION CONTACT:
Norma Curtis, Assistant Director, Office of Export Enforcement, Bureau of Industry and Security. Tel: (202) 482–5036, or by email at norma.curtis@bis.doc.gov.

*(*Continued On The Following Column)*

SUPPLEMENTARY INFORMATION:
Background

The mission of the Office of Export Enforcement (OEE) at BIS is to enforce the provisions of the Export Administration Regulations (EAR), secure America's trade, and preserve America's technological advantage by detecting, investigating, preventing, and deterring the unauthorized export and reexport of U.S.-origin items to parties involved with: (1) Weapons of mass destruction programs; (2) threats to national security or regional stability; (3) terrorism; or (4) human rights abuses. Export Enforcement at BIS is the only federal law enforcement agency exclusively dedicated to the enforcement of export control laws and the only agency constituted to do so with both administrative and criminal export enforcement authorities. OEE's criminal investigators and analysts leverage their subject-matter expertise, unique and complementary administrative enforcement tools, and relationships with other federal agencies and industry to protect our national security and promote our foreign policy interests. OEE protects legitimate exporters from being put at a competitive disadvantage by those who do not comply with the law. It works to educate parties to export transactions on how to improve export compliance practices, supporting American companies' efforts to be reliable trading partners and reputable stewards of U.S. national and economic security. BIS also discourages, and in some circumstances prohibits, U.S. companies from furthering or supporting any unsanctioned foreign boycott (including the Arab League boycott of Israel). OEE at BIS may refer violators of export control laws to the U.S.
Department of Justice for criminal prosecution, and/or to BIS's Office of Chief Counsel for administrative prosecution. In cases where there has been a willful violation of the EAR, violators may be subject to both criminal fines and administrative penalties. Administrative penalties may also be imposed when there is no willful intent, allowing administrative cases to be brought in a much wider variety of circumstances than criminal cases. BIS has a unique combination of administrative enforcement authorities including both civil penalties and denials of export privileges. BIS may also place individuals and entities on lists that restrict or prohibit their involvement in exports, reexports, and transfers (in-country). In this rule, BIS is proposing to amend the EAR to update its Guidance on Charging and Penalty Determinations in Settlement of Administrative Enforcement Cases (the ''Guidelines'') found in Supplement No. 1 to part 766 of the EAR in order to make civil penalty determinations more predictable and transparent to the public and aligned with those promulgated by the Treasury Department's Office of Foreign Assets Control (OFAC). OFAC administers most of its sanctions programs under the International Emergency Economic Powers Act (IEEPA), the same statutory authority by which BIS implements the EAR. OFAC uses the transaction value as the starting point for determining civil penalties pursuant to its Economic Sanctions Enforcement Guidelines.

*(*Continued On The Following Page)*

Under IEEPA, criminal penalties can reach 20 years imprisonment and $1 million per violation, and administrative monetary penalties can reach $250,000 or twice the value of the transaction, whichever is greater. Both agencies coordinate and cooperate on investigations involving violations of export controls that each agency enforces, including programs relating to weapons of mass destruction, terrorism, Iran, Sudan, Specially Designated Nationals and Specially Designated Global Terrorists. This guidance would not apply to civil administrative enforcement cases for violations under part 760 of the EAR—Restrictive Trade Practices and Boycotts. Supplement No. 2 to Part 766 continues to apply to enforcement cases involving part 760 violations. The Guidelines would provide factors by which violations could be characterized as either egregious or nonegregious and describe the difference in the base penalty amount likely to apply in an enforcement case. The base penalty would depend on whether the violation is egregious or non-egregious and whether or not the case resulted from a voluntary self-disclosure that satisfies all the requirements of § 764.5 of the EAR. Base penalty amounts would be described in terms of the applicable statutory maximum, the transaction value, or the applicable schedule amount. The terms ''transaction value'' and ''applicable schedule amount'' would be defined in the Guidelines. The ''statutory maximum'' would be the maximum permitted by § 764.3(a)(1) of the EAR

(15 CFR 764.3(a)(1)) subject to adjustment under the Federal Civil Penalties Inflation Adjustment Act of 1990 (28 U.S.C. 2461). Additional information about the changes proposed here and how they differ from the current Guidelines set forth in Supplement No. 1 to Part 766 is described below. Once the base penalty amount has been determined, Factors set forth in these Guidelines would be applied to determine whether the base penalty amount should be adjusted downward or, subject to the statutory maximum, upward. Factors set forth in the current Guidelines would be reorganized into the following categories: (1) Aggravating Factors (e.g., willfulness or recklessness); (2) General Factors that could be considered either aggravating or mitigating depending upon the circumstances (e.g., the absence or presence and adequacy of an internal compliance program); (3) Mitigating Factors (e.g., remedial measures taken); and (4) other Relevant Factors on a caseby- case basis (e.g., additional violations or other enforcement actions). Voluntary self-disclosures (VSDs) would no longer be listed as mitigating factors in and of themselves, but credit accorded to VSDs would be built into the determination of the base penalty amount. This credit would no longer be characterized as constituting ''great weight'' mitigation, but violations disclosed in a complete and timely VSD may be afforded a deduction of 50 percent of the transaction value or, in egregious cases, the statutory maximum in determining the base penalty amount. Mitigating Factors would also be assigned specific percentages off the base penalty amount, as further described below.

*(*Continued On The Following Column)*

Mitigating Factors may be combined for a greater reduction in penalty but mitigation will generally not exceed 75 percent of the base penalty. Willfulness, recklessness and concealment would be set forth as Aggravating Factor A—Willful or Reckless Violation of Law in the revised Guidelines. The degree to which these actions are present would determine the degree of aggravation factored into the penalty calculation. Aggravating Factor B—Awareness of Conduct at Issue would be listed as a separate factor in the revised Guidelines to address situations where the Respondent knew or had reason to know of the violation(s), and took no action to address them. Currently, knowing violations are subsumed within consideration of the ''Degree of Willfulness.'' Harm to regulatory program objectives would be listed as Aggravating Factor C—Harm to Regulatory Program Objectives. This factor would take into account all of the following: The destination involved, the end use and end user, and the sensitivity and control level of the item(s) involved in the transaction. Aggravating Factors A–C would be considered key in determining whether a violation was egregious or not, as further discussed below. Other aggravating facts, whether relating to the General Factors or Other Relevant Factors discussed below, may also be pertinent in determining whether a violation was egregious. Under this proposed rule, General Factors could either be mitigating or aggravating depending upon the circumstances. Two General Factors would be set forth in the revised Guidelines: General Factor D, involving an assessment of the individual characteristics of a Respondent; and General Factor E, assessing the presence and adequacy of a compliance program. General Factor D—Individual Characteristics would encompass an evaluation of the Respondent's commercial sophistication, exporting experience, volume and value of transactions, and regulatory history. General Factor E—Compliance Program—would involve a determination of whether or not the Respondent had an effective risk-based BIS compliance program in place at the time of the apparent violation, including an assessment of the extent to which it complied with BIS's Export Management System (EMS) Guidelines. Under General Factor E, if the Respondent's compliance program served to uncover the violation and led to prompt and comprehensive remedial measures taken to ensure against future violations, additional mitigation may be accorded to the Respondent under Mitigating Factor F, Remedial Response. That factor looks at whether the Respondent took corrective action in response to the apparent violation, such as stopping the conduct at issue. Mitigating Factor G—Exceptional Cooperation with OEE may result in a 25 percent to 40 percent reduction of the base penalty amount. This level of cooperation goes beyond what would be considered minimally necessary to address a violation and take corrective measures. In cases not involving a VSD, the Respondent must have provided substantial additional information regarding the apparent violation and/or other apparent violations caused by the same course of conduct. Exceptional cooperation in cases involving VSDs may also be considered as a further mitigating factor.

(*Continued On The Following Page)

Transactions that would likely have received a license had one been sought, as set forth in Mitigating Factor H— License Was Likely To Be Approved also may result in up to a 25 percent reduction of the base penalty amount. First offenses, addressed in the context of calculation of the base penalty amount, may also result in a reduction of that amount by up to 25 percent. Finally, proposed Factors I–M pertain to factors that may be relevant in certain circumstances and considered on a caseby- case basis. Factor I—Related Violations would address situations in which a single export transaction can give rise to multiple violations. Factor J—Multiple Unrelated Violations would address situations where multiple unrelated violations, as described in this proposed rule, could warrant a stronger enforcement response, including a denial order. Factor K—Other Enforcement Action would provide that corresponding enforcement action taken by federal, state, or local agencies in response to the apparent violation or similar apparent violations may be considered, particularly with regard to global settlements or criminal convictions and/or plea agreements.

Factor L—Future Compliance/ Deterrence Effect would address the impact that the administrative action may have with regard to promoting future compliance and deterring such conduct by other similar parties, particularly in the same industry sector. Factor M—Other Factors That BIS Deems Relevant would serve as a ''catch-all'' category to retain flexibility to consider factors not already specifically addressed in the Guidelines, whether proposed by the Respondent or BIS. Consideration of these Factors would not dictate a particular outcome in any particular case, but rather is intended to identify those Factors most relevant to BIS's decision and to guide the agency's exercise of its discretion. The Guidelines would provide sufficient flexibility to allow for the consideration of the Factors most relevant to a particular case. Penalties for settlements reached after the initiation of an enforcement proceeding and litigation through the filing of a charging letter will usually be higher than those described by these Guidelines. In accordance with OEE's existing posture that enhanced maximum civil penalties authorized by the International Emergency Economic Powers Enhancement Act (Enhancement Act) (Pub. L. 110–96, 50 U.S.C. 1701, et seq.) should be reserved for the most serious cases, the Guidelines would formally account for the substantial increase in the maximum penalties for violations of IEEPA and distinguish between egregious and non-egregious civil monetary penalty cases. Egregious cases would be those involving the most serious violations, based on an analysis of all applicable Factors, with substantial weight given to considerations of willfulness or recklessness, awareness of the conduct giving rise to an apparent violation, and harm to the regulatory program objectives, taking into account the individual characteristics of the parties involved. As described below, the Guidelines generally would provide for significantly higher civil penalties for egregious cases. OEE anticipates that the majority of apparent violations investigated by OEE will fall in the nonegregious category.

*(*Continued On The Following Column)*

OEE does not expect that adoption of these guidelines will increase the number of cases that are charged administratively rather than closed with a warning letter. The Guidelines define the ''transaction value'' to mean the dollar value of a subject transaction. Where the dollar value cannot be determined with certainty, the Guidelines would provide sufficient flexibility to allow for the determination of an appropriate transaction value in a wide variety of circumstances. The applicable schedule amounts, which would provide for a graduated series of penalties based on the underlying transaction values, reflect appropriate starting points for penalty calculations in non-egregious cases not involving VSDs. The base penalty amount for a non-egregious case involving a VSD would equal one-half of the transaction value, capped at $125,000, for an apparent violation of the EAR. Such calculation would ensure that the base penalty for a VSD case will not be more than one-half of the base penalty for a similar case that is not voluntarily self-disclosed. This difference is intended to serve as an additional incentive for the submission of VSDs. In the interest of providing greater transparency and predictability to BIS administrative enforcement actions, BIS would also allot penalty reductions—all from the base penalty amount—of between 25 and 40 percent for exceptional cooperation, and up to an additional 25 percent for first offenses and for transactions where a license was likely to be approved. BIS encourages the submission of VSDs by persons who believe they may have violated the EAR. The purpose of an enforcement action includes raising awareness, increasing compliance, and deterring future violations, not merely punishing past conduct. VSDs are a compelling indicator of a person's present intent and future commitment to comply with U.S. export control requirements. The purpose of mitigating the enforcement response in voluntary self-disclosure cases is to encourage the notification to OEE of apparent violations about which OEE would not otherwise have learned. OEE's longstanding policy of encouraging the submission of VSDs involving apparent violations is reflected by the fact that, over the past several years, on average only three percent of VSDs submitted have resulted in a civil penalty. The majority of cases brought to the attention of OEE through VSDs result in the issuance of warning letters, containing a finding that a violation may have taken place. With respect to VSDs generally, OEE will issue warning letters in cases involving inadvertent violations and cases involving minor or isolated compliance deficiencies, absent the presence of aggravating factors. Finally, in appropriate cases in the context of settlement negotiations, BIS may suspend or defer payment of a civil penalty, taking into account whether the Respondent has demonstrated a limited ability to pay, whether the matter is part of a global settlement with other U.S. government agencies, and/or whether the Respondent will apply a portion or all of the funds suspended or deferred for purposes of improving its internal compliance program. Cases will continue to be processed in accordance with the enforcement guidelines and precedents currently in existence until the new Guidelines are issued in final form after review of public comments.

DEPARTMENT OF COMMERCE
Bureau of Industry and Security
15 CFR Part 744
[Docket No. 150825778–5999–01]
RIN 0694–AG64
Russian Sanctions: Addition of Certain Persons to the Entity List

AGENCY: Bureau of Industry and Security, Commerce.
ACTION: Final rule.

SUMMARY: The Bureau of Industry and Security (BIS) amends the Export Administration Regulations (EAR) by adding sixteen persons under seventeen entries to the Entity List. The sixteen persons who are added to the Entity List have been determined by the U.S. Government to be acting contrary to the national security or foreign policy interests of the United States. BIS is taking this action to ensure the efficacy of existing sanctions on the Russian Federation (Russia) for violating international law and fueling the conflict in eastern Ukraine. These persons will be listed on the Entity List under the destinations of the Crimea region of Ukraine, Cyprus, Luxembourg,
Panama, Russia, Switzerland, and the United Kingdom. Lastly, this final rule includes a clarification for how entries that include references to § 746.5 on the Entity List are to be interpreted.

DATES: This rule is effective December 28, 2015.

FOR FURTHER INFORMATION CONTACT:
Chair, End-User Review Committee, Office of the Assistant Secretary, Export Administration, Bureau of Industry and Security, Department of Commerce, Phone: (202) 482–5991, Fax: (202) 482– 3911, Email: ERC@bis.doc.gov.

For the sixteen persons under seventeen entries added to the Entity List on the basis of activities described in Executive Orders 13661 or 13685, BIS imposes a license requirement for all items subject to the EAR and a license review policy of presumption of denial. The license requirements apply to any transaction in which items are to be exported, reexported, or transferred (incountry) to any of the persons or in which such persons act as purchaser, intermediate consignee, ultimate consignee, or end-user. In addition, no license exceptions are available for exports, reexports, or transfers (incountry) to the persons being added to the Entity List in this rule. The acronyms ''a.k.a.'' (also known as) and ''f.k.a.'' (formerly known as) are used in entries on the Entity List to help exporters, reexporters and transferors to better identify listed persons on the Entity List. This final rule adds the following sixteen persons under seventeen entries to the Entity List:

*(*Continued On The Following Column)*

Crimea Region of Ukraine

(1) Aktsionernoe Obschestvo 'Yaltinskaya Kinodstudiya,' a.k.a., the following eight aliases:
—CJSC Yalta-Film; —Film Studio Yalta-Film; —Joint Stock Company Yalta Film Studio; —JSC Yalta Film Studio; —Kinostudiya Yalta-Film; —Oao Yaltinskaya Kinostudiya; —Yalta Film Studio; and —Yalta Film Studios. Ulitsa Mukhina, Building 3, Yalta, Crimea 298063, Ukraine; and Sevastopolskaya 4, Yalta, Crimea, Ukraine;

(2) Crimean Enterprise Azov Distillery Plant, a.k.a., the following five aliases:
—Azovsky Likerogorilchany Zavod, Krymske Respublikanske Pidpryemstvo; —Azovsky Likerovo-Dochny Zavod; —Crimean Republican Enterprise Azov Distillery; —Crimean Republican Enterprise Azovsky Likerovodochny Zavod; and —Krymske Respublikanske Pidpryemstvo Azovsky Likerogorilchany Zavod. Bud. 40 vul. Zaliznychna, Smt Azovske, Dzhankoisky R–N, Crimea 96178, Ukraine; and 40 Railway St., Azov, Dzhankoy District 96178, Ukraine; and 40 Zeleznodorozhnaya str., Azov, Jankoysky District 96178, Ukraine;

(3) Resort Nizhnyaya Oreanda (f.k.a., Federalnoe Gosudarstvennoe Byudzhetnoe Uchrezhdenie Sanatori Nizhnyaya Oreanda Upravleniya), a.k.a., the following three aliases:
—Federalnoe Gosudarstvennoe Byudzhetnoe Uchrezhdenie Sanatori Nizhnyaya Oreanda Upravleniya Delami Prezidenta Rossiskoi Fe; —FGBU Sanatori Nizhnyaya Oreanda; and —Sanatorium Nizhnyaya Oreanda. Pgt Oreanda, Dom 12, Yalta, Crimea 298658, Ukraine; and Resort Nizhnyaya Oreanda, Oreanda, Yalta 08655, Crimea; Oreanda—12, Yalta 298658, Crimea;

(4) State Concern National Production and Agricultural Association Massandra, a.k.a., the following four aliases:
—Massandra National Industrial Agrarian Association of Wine Industry; —Massandra State Concern, National Production and Agrarian Union, OJSC; —Nacionalnoye Proiz-Vodstvenno Agrarnoye Obyedinenye Massandra; and —State Concern National Association of Producers Massandra. 6, str. Mira, Massandra, Yalta 98600, Ukraine; and 6, Mira str., Massandra, Yalta, Crimea 98650, Ukraine; and Mira str, h. 6, Massandra, Yalta, Crimea 98600, Ukraine; and 6,
Myra st., Massandra, Crimea 98650, Ukraine;

*(*Continued On The Following Page)*

(5) State Enterprise Factory of Sparkling Wine Novy Svet, a.k.a., the following six aliases: —Derzhavne Pidpryemstvo Zavod Shampanskykh Vyn Novy Svit; —Gosudarstvenoye Predpriyatiye Zavod Shampanskykh Vin Novy Svet; —Novy Svet Winery; —Novy Svet Winery State Enterprise; —State Enterprise Factory of Sparkling Wines New World; and —Zavod Shampanskykh Vyn Novy Svit, DP. 1 Shaliapin Street, Novy Svet Village, Sudak, Crimea 98032, Ukraine; and Bud. 1 vul. Shalyapina Smt, Novy Svit, Sudak, Crimea 98032, Ukraine; and 1 Shalyapina str. Novy Svet, Sudak 98032, Ukraine;

(6) State Enterprise Magarach of the National Institute of Wine, a.k.a., the following five aliases:

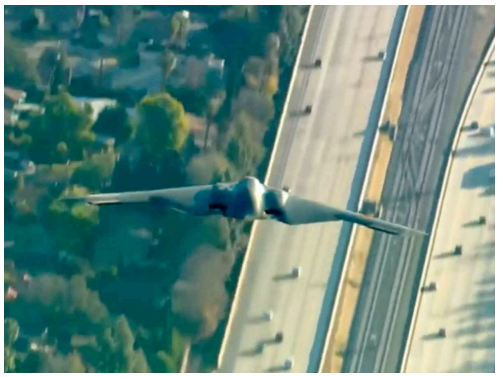
For more information:

https://www.bis.doc.gov/index.php/regulations/federal-register-notices#FR80643

Complying with U.S. Export Controls seminar

Registration Still Available for January 2016 Complying with U.S. Export Controls seminar – Memphis, TN The Bureau of Industry and Security invites you to register for the following seminar to learn about export control requirements under the Export Administration Regulations. ■ Complying with U.S. Export Controls – 2 Days January 27-28, 2016 Memphis, TN – $360. This two-day program is 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 on commercial goods and other items controlled under the EAR. We will focus on what items and activities are subject to the EAR; how to determine your export control classification number (ECCN); steps to take to determine the export licensing requirements for your item; when you can export or reexport without applying for a license; export clearance procedures; and record keeping requirements. View Complying with U.S. Export Controls event details. [Insert LINK tohttps://www.bis.doc.gov/index.php/compliance-a-training/current-seminar-schedule/81-compliance-a-training/export-administration-regulations-training/seminar-details/966-january-27-28-memphis-tn] Please follow the Bureau of Industry and Security on Twitter: http://twitter.com/BISgov

Watch an awesome flyover of a B-2 Spirit Stealth Bomber during the Rose Parade.



http://www.flyingmag.com/video-b-2-spirit-stealth-bomber-flyover-during-rose-parade?src=SOC&dom=tw