EIB World Trade Headlines

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

June 15, 2016 - Volume 8, Issue 11

Evolutions In Business June 1st Seminar A Success

Our full day seminar at the Westford Regency went great! It was a very hot day outside, which made the indoor AC a welcomed treat. We had many different manufacturing companies join us representing different sectors across the U.S. A few folks had issues with their flights but we hope to see them in the Fall when we cover this material again. We covered EAR & ITAR Regulations focusing on Export Reform changes and the 600 series. We were honored to have keynote speakers Special Agents William Higgins, Office Of Export Enforcement, BIS and Alex Miris with the US Department of Homeland Security, Homeland Security Investigations (HSI.)
They both gave excellent presentations based upon field work in actual cases related to export violations. The work they do is so vital to our National Security and we thank them for joining us.

We hope to hold another full day seminar sometime in November 2017, more information on that will come out next year!

NEWSLETTER NOTES

Canadian-Iranian Citizen Sentenced In Manhattan Federal Court To Three Years In Prison For Conspiring To Violate Iran Sanctions

Preet Bharara, the United States Attorney for the Southern District of New York, and John P. Carlin, Assistant Attorney General for National Security, announced that ALI REZA PARSA, a Canadian-Iranian dual citizen and resident of Canada, was sentenced on Friday, May 20, 2016, to three years in prison for his participation in a conspiracy to violate the International Emergency Economic Powers Act ("IEEPA") and the Iranian Transactions and Sanctions Regulations ("ITSR"). PARSA was arrested in October 2014 following an investigation by the Federal Bureau of Investigation ("FBI") and United States Department of Commerce, Bureau of Industry and Security ("BIS"). PARSA pled guilty on January 20, 2016, before U.S. District Judge Ronnie Abrams, who imposed Friday's sentence.

Manhattan U.S. Attorney Preet Bharara said: "As he admitted in court, Ali Reza Parsa conspired to purchase high-tech electronic components – some used in the production of rockets and missiles – from American companies for eventual delivery to Iran through Canada. He has now been sentenced to three years in prison for his violation of federal law."

Assistant Attorney General John P. Carlin said: "Over the course of six years, Parsa repeatedly violated export control laws and aided Iranian entities in procuring high-tech electronic components that have both commercial and military uses. With this sentence, he will be held accountable for circumventing important U.S. laws designed to protect our national security interests. One of our top national security priorities remains safeguarding our national assets from those who may wish to do us harm."

According to the Indictment filed against PARSA and other court documents publicly filed in this case and statements made in court proceedings, including Friday's sentencing:

Between approximately 2009 and 2015, PARSA conspired to obtain high-tech electronic components from American companies for transshipment to Iran and other countries for clients of PARSA's procurement company in Iran, Tavan Payesh Mad, in violation of U.S. economic sanctions. To accomplish this, PARSA used his Canadian company, Metal PM, to place orders with U.S. suppliers and typically had the parts shipped to him in Canada or to a freight forwarder located in the United Arab Emirates, and then transshipped from these locations to Iran or to the location of his Iranian company's client. PARSA provided the U.S. companies with

*(*Continued On The Following Column)*

false destination and end-user information about the components in order to conceal the illegality of these transactions.

PARSA's criminal scheme targeted numerous American technology companies. The components that PARSA attempted to procure included cryogenic accelerometers, which are sensitive components that measure acceleration at very low temperatures. Cryogenic accelerators have both commercial and military uses, including in applications related to ballistic missile propellants and in aerospace components such as liquid-fuel rocket engines.

In addition, following his arrest and while incarcerated at the Metropolitan Detention Center, PARSA continued to violate the IEEPA and the ITSR by conducting business for Metal PM and Tavan Payesh Mad, including by ordering parts from German and Brazilian companies for Iranian customers. PARSA subsequently directed a relative to delete email evidence of his ongoing business transactions while in jail, emphasizing the need for secrecy in their dealings.

Neither PARSA nor any other individual or entity involved in transactions that gave rise to his conviction applied for or obtained a license from the U.S. Department of the Treasury's Office of Foreign Assets Control for the transactions.

In addition to the 36-month prison term, PARSA, 45, was ordered to pay a $100 special assessment.

Mr. Bharara praised the outstanding investigative work of the FBI and BIS. He also thanked the U.S. Department of Justice's National Security Division's Counterintelligence and Export Control Section.

This prosecution is being handled by the Office's Terrorism and International Narcotics Unit. Assistant United States Attorneys Michael D. Lockard and Anna Skotko are in charge of the prosecution.

High-powered British drone-freezing ray to trial in US airports

A high-powered ray gun that can jam drone signals and stop them mid-flight is being tested out by the US government's Federal Aviation Administration (FAA). The tech is desirable as it's expected to clear and secure airspace around airports. It has the potential to detect small, unmanned aerial vehicles that are flying around the airport and may potentially be owned and operated by terrorists and smugglers.

(*Continued On The Following Page)

Deemed the Anti-UAV Defense System (Auds), the drone-freezing ray was developed by three British companies – Enterprise Control Systems, Blighter Surveillance Systems, and Chess Dynamics.

But how exactly does the drone-freezing ray work? First, a thermal imaging camera allows the Auds operator to target a particular drone. Once the drone has been located, a very high-powered radio signal is then activated, jamming the drones' signals, making them unresponsive.

Auds operators have the ability to freeze drones and warn pilots if they think something is wrong with the device. It can also crash devices by installing drones in the air for as long as the battery lasts.

In addition to the Auds, the US Army also has weapons able to destroy larger drones. Projectiles can be launched and steered to drones using ground-based radars.

The drone-freezing ray is set to be tested at several airports to be selected by the FAA. Two other US-based firms – Gryphon Sensors LLC and Sensofusion – will also take part.

ARRESTS, TRIALS AND CONVICTIONS
Navy Lt. Cmdr. Edward Lin Pleads Not Guilty to Spying Charges

WAVY.COM May 17, 2016
NORFOLK, Va (WAVY) — Navy Lt. Cmdr. Edward Lin has pleaded not guilty to espionage charges and has requested a trial by jury.
Court documents claim Lin illegally shared information with a foreign government and falsified records. The government has never named the country for which he's accused of spying for, 10 On Your Side has learned it's likely Taiwan, where Lin was born.
In newly unredacted charge sheets released Tuesday, it was learned that Lin's espionage charges revolve around incidents in Washington, D.C.
The paperwork asserts that while in the nation's capital from, September 2012 – December 2013 and April 2012 – May 2014, Lin gave information classified as "secret" with "intent or reason to believe it would be used to the advantage of a foreign nation."
"Secret" information is one step below "Top Secret." Top secret is the military's most guarded information.
According to biographical data released from the Navy, Lin worked at the Pentagon from late February 2012 through the end of November 2013. He was a staffer working for the Assistant Secretary of the Navy for Financial Management and Comptroller.

*(*Continued On The Following Column)*

Lin also faces two counts of purposefully lying about his travel in October 2014 and April 2015. The Navy says that both times, Lin listed his final destination as Alexandria, Virginia, when he was actually traveling to a foreign destination. That destination was not disclosed in the documentation.
In 2014, until his arrest in 2015, Lin was stationed in Pearl Harbor where he oversaw several Navy spy planes.
The newly unredacted documents also show that Lin's three counts of attempted espionage and five counts of communicating defense information, charges less severe than espionage or attempted espionage, allegedly occurred in Pearl Harbor.
According to audio from his preliminary hearing in April, the government found a notebook and emails at his home with secret intelligence. NCIS investigators say Lin spoke with a FBI informant in Mandarin, his native language.
The military goes on to say he passed on the intelligence he gathered to a prostitute in Hawaii. Lin originally faced counts of soliciting a prostitute and adultery, but those charges were dropped.
Investigators took Lin into custody at the Honolulu airport in September 2015, and questioned him for two days. There is video of the 11 hours of interrogations. The government says Lin admitted to all the charges. Lin's defense lawyers argue undercover agents forced him to make those alleged confessions. They also maintain the information he allegedly gave was no longer classified.
Lin's missteps date back to 2011. That's when he's accused of failing to report foreign travel. During that time he was a student at the Naval War College in Newport, RI.
Lin's next hearing is scheduled for early June. His attorneys say that's when they'll petition to have him released from the Brig.

http://wavy.com/navy-lt-cmdr-edward-lin-to-stand-trial-on-spying-charges

CYBER, HACKING, DATA THEFT, COMPUTER INTRUSIONS & RELATED
FBI Warns against Wireless Keystroke Loggers Disguised as USB Chargers
Alert is for companies that use wireless Microsoft keyboards

SOFTPEDIA May 24, 2016
At the end of April, the FBI issued a public alert regarding KeySweeper, a piece of custom hardware created by security researcher Samy Kamkar as a proof-of-concept project, capable of stealing keystrokes from wireless Microsoft keyboards by intercepting nearby radio signals and decrypting the keyboard's protocol.

*(*Continued On The Following Page)*

The device works on top of an Arduino board, which is small enough to fit inside the case of a USB charger. Since USB chargers have become commonplace with the proliferation of mobile devices such as smartphones and tablets, seeing one such device plugged into a wall socket and abandoned in an office is not out of the ordinary these days.
The FBI warns companies to limit the number of outlets available for device charging, to instruct employees to recognize whose chargers are currently plugged in, and not to leave any charger plugged into the wall if not used.
Additionally, companies were also instructed to limit the usage of wireless keyboards, either by switching to wired keyboards or to ones that use Bluetooth for communications. However, if companies use Bluetooth keyboards, the FBI also recommends using encryption, along with a strong PIN.
KeySweeper is not effective against all keyboards
KeySweeper cannot harvest keystrokes from Bluetooth keyboards, with Kamkar only designing it for RF-based wireless keyboards created and sold by Microsoft. Of course, with the documentation out there in the open, anyone can very easily adapt it to other platforms and manufacturers.
While it was doing damage control after Kamkar's announcement last year, Microsoft also said that keyboards that operate on the 2.4GHz frequency and manufactured after 2011 are also safe because they use Advanced Encryption Standard (AES) encryption for securing keystrokes between the keyboard and the computer.
Kamkar released the device in January 2015, but the FBI has only recently issued this alert, which means that it investigated at least one case where someone used a KeySweeper device to log keystrokes.

FBI Warns Nation-State Cyber Attacks Are Continuing

Chinese soldiers browse online news on desktop computers at a garrison of the PLA / AP
Foreign government hackers are continuing to target U.S. government and private sector computer networks in sophisticated cyber attacks, the FBI warned in an alert sent this week.
“Advanced Persistent Threat (APT) cyber actors continue to target sensitive information stored on U.S. commercial and government networks through cyber espionage,” the FBI said in the May 11 notice.
The term “APT actor” is a euphemism for state-sponsored or highly sophisticated cyber attackers, usually involving connections to foreign militaries or intelligence services.
Two cyber security researchers who examined the FBI notice listing details of the cyber attacks said the tactics appeared similar to those used in the past by Chinese hackers, including the suspects behind the massive theft of records on 22 million federal workers from the Office of Personnel Management.

*(*Continued On The Following Column)*

The FBI listed seven major Internet server software types hacked in the past year, including two Adobe ColdFusion security flaws. ColdFusion software is used with large databases.
Other attacks involved Apache Tomcat, JBoss, and Cacti, software used for remote data logging. Drupal servers used to operate a large number of websites around the world, including corporate and government sites, also were compromised. Joomla content-management software also was compromised, the FBI said.
A seventh compromise affected Oracle’s E-Business Suite software, used for customer management and supply-chain management.
State-sponsored hackers exploited vulnerabilities in all seven types of software, and “some of these vulnerabilities are also exploited by cyber criminals in addition to state-sponsored operators,” the FBI said.
“The compromises were [used] to build infrastructure and for exploitation,” the notice states.

Only two of the compromises took place last year, an indication that software patches applied last year to close entry holes have not stopped the attacks and that older vulnerabilities continue to be used by cyber spies, the notice says.
The FBI warned network administrators to engage in “proactive patch management” as the main line of defense for protecting publicly accessible computer servers from attack.
One indicator that China may have been behind the cyber espionage was the use of spear-phishing emails containing links to documents or compromised systems.
The technique is said to be a favorite of Chinese military hackers, including those part of Shanghai-based Unit 61398 that has been traced to widespread cyber attacks against U.S. government and private networks over the past several years.
“A general consensus is it is Chinese [tactics, techniques and procedures],” said one security researcher, who spoke on condition of anonymity.
The FBI said the recent government-sponsored hacking continued to use fraudulent emails to lure unsuspecting users into providing remote computer access. The hackers also were able to navigate widely once inside a network.
“Previous spear-phish emails sent by these actors contained decoy documents, such as a U.S. letter fax test page and an office monkeys video,” the notice states.
“Once on computer networks, the actors utilizing these exploits are extremely adept at lateral movement through the enterprise, to include the ability to gain administrative access, including domain-level access, within a short time frame.”
Like the hackers linked to OPM attack, the recent hackers also used a program called Mimikatz for “credential harvesting” from remote users. Another program called LogonUI allowed the hackers to maintain their presence inside a hacked network.

*(*Continued On The Following Page)*

Additionally, the hackers used public data storage sites for storing the stolen data and delivering malware, including Google Drive, Microsoft OneDrive, and Dropbox.
In a relatively new technique, the hackers used a Tor software called Meek that allows online users to evade detection and tracking and also to hide data theft.
If the recent cyber espionage is confirmed as Chinese in origin, it would be a setback for the Obama administration.
The administration was set to impose sanctions on Chinese hackers in September in respond to Beijing's role in the large-scale OPM data theft.
However, the sanctions were dropped during the summit in Washington in exchange for a pledge from Chinese leader Xi Jinping to halt cyber economic espionage.
A White House National Security Council spokesman had no immediate comment.

Senior U.S. intelligence officials, including Director of National Intelligence James Clapper and Cyber Command commander Adm. Mike Rogers, told Congress earlier this year they could not confirm China had halted the practice of stealing data through cyber espionage.
Clapper said in March it "remains to be seen" whether China will halt cyber spying.
Contrary to the Xi pledge, however, Rogers said, "cyber operations from China are still targeting and exploiting U.S. government, defense industry, academic, and private computer networks." The comments were made in prepared testimony to a House Armed Services subcommittee on March 16.
Missile Defense Agency Director Vice Adm. James Syring also told a House hearing May 14 that Chinese military cyber attacks on his agency's networks were a daily occurrence.
"My biggest concern remains in our cleared defense contractor base and their protections," Syring said.
China's cyber espionage and attack operations have included compromises of major U.S. weapons systems, including the F-35 and F-22 jet fighters, the B-2 stealth bomber, and the space-based laser.
A National Security Agency document made public by former contractor Edward Snowden revealed that the Chinese stole radar design and engine schematics for the new F-35.
FBI spokeswoman Nora Scheland declined to comment on the alert but said the FBI routinely advises private industry on various cyber threat indicators gained from investigations.

http://freebeacon.com/issues/fbi-warns-nation-state-cyber-attacks-continuing

DEPARTMENT OF COMMERCE
Bureau of Industry and Security
Revisions to Definitions in the Export Administration Regulations

ACTION: Final rule.
SUMMARY: This final rule is part of the Administration's Export Control Reform (ECR) Initiative. The Initiative will enhance U.S. national and economic security, facilitate compliance with
export controls, update the controls, and further the goal of reducing unnecessary regulatory burdens on U.S. exporters. As part of this effort, the Bureau of Industry and Security (BIS), in publishing this
rule, makes revisions to the Export Administration Regulations (EAR) to include certain definitions to enhance clarity and consistency with terms also
found in the International Traffic in Arms Regulations (ITAR), which is administered by the Department of State, Directorate of Defense Trade
Controls (DDTC), or that DDTC expects to publish in proposed rules. This final rule also revises the Scope part of the EAR to update and clarify application of controls to electronically transmitted
and stored technology and software, including by way of cloud computing. DDTC is concurrently publishing comparable amendments to certain
ITAR definitions for the same reasons. Finally, this rule makes conforming changes to related provisions.

DATES: This rule is effective September 1, 2016.

SEE 81 fr 35568 for complete info.

Revisions to Definitions in the Export Administration Regulations: Frequently Asked Questions (FAQs) Effective September 1, 2016

Effective September 1, 2016 1

Not Subject to the EAR: Information released by Instruction in a Catalog Course or Associated Teaching Laboratory of an Academic Institution (§ 734.3)(b)(3))
Q.1: I teach a university graduate course on design and manufacture of very high-speed integrated circuitry. Many of the students are foreigners. Do I need a license to teach this course?
A: No. Release of information by instruction in catalog courses and associated teaching laboratories of academic institutions is not subject to the EAR.

*(*Continued On The Following Page)*

Q.1.2: Would it make any difference if some of the students were from countries to which export licenses are generally required for these items?
A: No.
Q.1.3: Would it make any difference, in teaching this course, if I talk about recent and as yet unpublished results from my laboratory research?
A: No.
Q.1.4: Even if that research is funded by the government?
A: Even then the information would not be subject to the EAR. However, you would not be released from any obligations imposed by any other law or your grant or contract.
Q.1.5: Would it make any difference if I were teaching at a foreign university?
A: No.
Q.2: My company teaches proprietary courses on design and manufacture of high-performance machine tools. Is the instruction in our classes subject to the EAR?
A: That instruction is most likely subject to the EAR, because it would not qualify as "released by instruction in a catalog course or associated teaching laboratory of an academic institution" under § 734.3(b)(3) because your proprietary business does not qualify as an "academic institution" within the meaning of § 734.3(b)(3). Conceivably, however, the instruction might qualify as "unlimited distribution at a conference, meeting, seminar, trade show, or exhibition, generally accessible to the interested public" under § 734.7(a). The conditions that would have to be satisfied are that such a seminar or gathering qualify as "open," including a fee reasonably related to costs (of the conference, not of producing the data), and that there is an intention that all interested and technically qualified persons be able to attend.
Published Technology and Software (§ 734.7)
Q.1: Are libraries with access controls in place for physical security reasons (e.g., to guard against theft of written materials or to keep the users safe) "open and available to the public?"
A: Yes. **Revisions to Definitions in the Export Administration Regulations: Frequently Asked Questions (FAQs) Effective September 1, 2016**

Q.2: My Ph.D. thesis is on technology, which is listed in the EAR as requiring a license to all destinations except Canada and has never been published for general distribution. However, the thesis is available at the institution from which I took the degree. Do I need a license to send another copy to a colleague overseas?
A: That may depend on where in the institution your thesis is available. If it is not readily available in the university library, it is not "published" and its export or reexport would be subject to the EAR on that ground. If your Ph.D. research qualified as "fundamental research" under § 734.8, it would not be subject to the EAR. If not, however, you will either need to obtain a license or qualify for a license exception (if a license requirement applies) or use the No License Required (NLR)
*(*Continued On The Following Column)*

designation (if a license requirement does not apply) before you can send a copy of your thesis out of the U.S.
Q.3: What does "unclassified" mean in § 734.7?
A: Unclassified information" refers to information not classified in accordance with Executive Order 13526, 75 FR 707; 3 CFR 2010 Comp., p. 298, or a comparable predecessor or successor order.
Q.4: Are copyright protections or generic property rights in the underlying physical medium "restrictions upon … further dissemination" that make information not "published?"
A: No. Copyright protections or generic property rights in the underlying physical medium are not such restrictions.
Q.5: I plan to publish in a foreign journal a scientific paper describing the results of my research, which is in an area listed in the EAR as requiring a license to all countries except Canada. Do I need a license to send a copy of the paper to my publisher abroad? Would the answer differ depending on where I work or where I performed the research?
A: No. This export transaction is not subject to the EAR. The EAR do not cover technology that is already published or technology that is made public by the transaction in question (§§ 734.3 and 734.7). Your research results would be made public by the planned publication. The answer would not differ depending on where you work or performed the research.
Q.5.1: Would I need a license to send the paper to the editors of a foreign journal for review to determine whether it will be accepted for publication?
A: No. This export transaction is not subject to the EAR because you are submitting the paper to the editors with the understanding that the paper will be made available to the public (published) if favorably received (§ 734.7(a)(5)). This answer is applicable to submissions to either U.S. or foreign journals.
Q.6: I have been invited to give a paper at a prestigious international scientific conference on a technology listed as requiring a license under the EAR to all countries, except Canada. Scientists in the field are given an opportunity to submit applications to attend. Invitations are given to those judged to be the leading researchers in the field, and attendance is by Revisions to Definitions in the Export Administration Regulations: Frequently Asked Questions (FAQs) Effective September 1, 2016

invitation only. Attendees will be free to take notes, but not make electronic or verbatim recordings of the presentations or discussions. Some of the attendees will be foreigners. Do I need a license to give my paper?
A: No. Release of information at an open conference and information that has been released at an open conference are not subject to the EAR (see § 734.7(a)(3)). A conference or gathering is "open" (see also § 734.7(a)(5)(iii)) if all technically qualified members of the public are eligible to attend and attendees are permitted to take notes or otherwise make a personal record (not necessarily a recording) of the proceedings and presentations. All technically qualified
*(*Continued On The Following Page)*

members of the public may be considered eligible to attend a conference or other gathering notwithstanding a registration fee reasonably related to cost and reflecting an intention that all interested and technically qualified persons be able to attend, or a limitation on actual attendance, as long as attendees either are the first who have applied or are selected on the basis of relevant scientific or technical competence, experience, or responsibility.

Q.6.1: Would it make any difference if there were a prohibition on taking notes or other personal record of what transpires at the conference?

A: Yes. To qualify as an "open" conference, attendees must be permitted to take notes or otherwise make a personal record (although not necessarily a recording). If note taking or the making of personal records is altogether prohibited, the conference would not be considered "open."

Q.6.2: Would it make any difference if there were also a registration fee?

A: That would depend on whether the fee is reasonably related to costs of the conference and reflects an intention that all interested and technically qualified persons should be able to attend.

Q.6.3: Would it make any difference if the conference were to take place in another country?

A: No.

Q.6.4: Must I have a license to send the paper I propose to present at such a foreign conference to the conference organizer for review?

A: No. A license is not required under the EAR to submit papers to foreign organizers of open conferences or other open gatherings with the understanding that the papers will be delivered at the conference, and so be published, if favorably received. The submission of the papers is not subject to the EAR (§ 734.7(a)(5)).

Q.6.5: Would the answers to any of the foregoing questions be different if my work were supported by the federal government?

A: No. You may export and reexport the papers, even if the release of the paper violates any agreements you have made with your government sponsor. However, nothing in the EAR relieves you of responsibility for conforming to any controls you have agreed to in your Federal grant or contract.

Fundamental Research (§ 734.8) Revisions to Definitions in the Export Administration Regulations: Frequently Asked Questions (FAQs) Effective September 1, 2016

Effective September 1, 2016 4

Q.1: What is considered fundamental research under the EAR?

A: The role of the EAR is not to regulate fundamental research as such; it is to regulate the transfer of technology and software. Technology or software that arises during or results from fundamental research is generally not subject to the EAR (see § 734.8 for specific criteria). (Please note: Section 734.8 does not apply to physical objects such as pathogens or equipment.) Fundamental research is described in the EAR as

*(*Continued On The Following Column)*

as "research in science, engineering, or mathematics, the results of which ordinarily are published and shared broadly within the research community, and for which the researchers have not accepted restrictions for proprietary or national security reasons." The techniques used during the research are normally publicly available or are part of the published information.

- Example: There is a joint U.K./U.S. university-based research project on vector identification for Marburg virus with no restrictions on publication of the results of the research or of any technology released to the researchers. The research would be considered fundamental and the information resulting from this research, such as the results and methods, are not subject to the EAR. There would be no "deemed export" required for foreign nationals working at the U.S. university and no export license required for discussing research methods and outcomes between the two universities. An export license would be required for the export of the Marburg virus samples to the U.K. university.

Q.2: What types of research are NOT considered fundamental research under the EAR?

A: Research is not considered fundamental research when the laboratory, company, university or researcher restricts the publication of the outcome of the research or restricts the publication of the methods used during the research. The following are examples of research that is not considered fundamental and information that becomes subject to the EAR:

· Proprietary research.

· Any research methods or outcomes of government-funded research that have been specifically restricted from publication. Only the information that is thus restricted would become subject to the EAR; the remainder of the research methods and outcomes that have not been subject to restriction would be considered information resulting from fundamental research.

· Any research methods or outcomes of government-funded research that have been communicated in violation of any condition that may exist in the funding instrument that requires prepublication security review of the research communication.

· Research methods or outcomes that an investigator voluntarily decides should not be communicated widely because of security concerns and therefore self-redacts from publication. Only the information that is redacted would become subject to the EAR; the remainder of the research methods and outcomes that have not been subject to self-redaction would be considered information resulting from fundamental research.

Revisions to Definitions in the Export Administration Regulations: Frequently Asked Questions (FAQs) Effective September 1, 2016

Effective September 1, 2016 5

*(*Continued On The Following Page)*

- Example: Government-funded researchers studying *Bacillus anthracis* accept national security prepublication review of their research. If the group complies with the review requirement and does not communicate this research without the required reviews, their research remains fundamental research. However, any of the information resulting from this research that is restricted from publication becomes subject to the EAR. Research methods and outcomes from the same project that are not subject to restriction would remain information resulting from fundamental research and not subject to the EAR.

Decisions to restrict publication, regardless of the source of the decision, would mean that the technology not intended to be published is technology subject to the EAR. This decision is not retroactive, so it would not impose a license requirement for exports of the information that have already taken place, but may impose a license requirement for future exports of the information and future deemed export licenses as necessary.

Q.3: Our internal compliance program uses a slightly different definition of "fundamental research" from the one in the EAR. We use the exact wording found in National Security Decision Directive (NSDD)-189. Do we need to revise our program materials to match the EAR definition?

A: No. The scope of EAR definition is fully consistent with the scope of NSDD-189 definition.

Q.4: Does BIS presume that research conducted by scientists, engineers, or students at an accredited institution of higher education located in the United States will be considered fundamental research?

A: Yes, but, as with all rebuttable presumptions, it is rebutted if the research is not within the scope of technology and software that arises during, or results from, fundamental research as described in § 734.8.

Q.5: My research sponsor will review the results of my research before I publish. Does this review affect whether my results are subject to the EAR?

A: It depends on the nature of the prepublication review. (See 734.8(b).) Prepublication review by a sponsor of university research to ensure that the publication would not compromise patent rights or would not inadvertently divulge proprietary information that the sponsor has furnished to the researchers does not change the status of the research as fundamental research. If the result of the review is to restrict publication, the EAR applies to that information for which publication is restricted. For example, university-based research is not considered "fundamental research" if the university or its researchers accept, at the request of an industrial sponsor, other restrictions on publication of scientific and technical information resulting from the project or activity. Scientific and technical information resulting from the research will nonetheless qualify as fundamental research once all such restrictions have expired or have been removed.

*(*Continued On The Following Column)*

Q.6: Is information given to researchers by a sponsor subject to the EAR? Revisions to Definitions in the Export Administration Regulations: Frequently Asked Questions (FAQs) Effective September 1, 2016
Effective September 1, 2016 6

A: The initial transfer of information from an industry sponsor to university researchers is subject to the EAR where the parties have agreed that the sponsor may withhold from publication some or all of the information so provided.

Q.7: What if our research is government-funded and the government imposes access and dissemination controls on it?

A: Technology or software resulting from U.S. government funded research that is subject to government-imposed access and dissemination or other specific national security controls qualifies as technology or software resulting from fundamental research, provided that all government-imposed national security controls have been satisfied and the researchers are free to publish the technology or software contained in the research without restriction.

Q.8: My research is not subject to government-imposed access and dissemination or other specific national security controls. Do I need a license for a foreign graduate student to work in my laboratory?

A: Not if the research on which the foreign student is working is "fundamental research" under § 734.8 and any information released to the researchers is also intended to be published.

Q.9: Our company has entered into a cooperative research arrangement with a research group at a university. One of the researchers in that group is a national of the People's Republic of China (PRC). We would like to share some of our proprietary information with the university research group. We have no way of guaranteeing that this information will not be released to the Chinese scientist. Do we need to obtain a license to protect against that possibility?

A: If the cooperative research arrangement authorizes the university to freely publish the proprietary information, then the sharing of the information is not a transaction to which the EAR applies. However, if your company and the researchers have agreed to a prohibition on publication, then you must determine whether a license is necessary and, if necessary, obtain a license or qualify for a license exception before transferring the information to the university. It is important that you as the corporate sponsor determine the proper classification and discuss with the university the nationality of any foreign nationals that will have access to the information, so that you may obtain any necessary authorization prior to transferring the information to the research team.

Q.10: My university will host a prominent scientist from the PRC who is an expert on research in engineered ceramics and composite materials. Do I require a license before telling our visitor about my latest, as yet unpublished, research results in those fields?

A: Probably not, provided the research results meet the criteria of "fundamental research" in § 734.8. Specifically, if

*(*Continued On The Following Page)*

you performed your research at the university, you intend to publish it, and you were subject to no contract controls on release of the research, your research would be "fundamental research." Information arising during or resulting from such research is not subject to the EAR (§ 734.3(b)(3)). You should probably assume, however, that your visitor will be debriefed later about anything of potential military value he learns from you. **Revisions to Definitions in the Export Administration Regulations: Frequently Asked Questions (FAQs) Effective September 1, 2016**
Effective September 1, 2016 7

Q.10.1: Would it make any difference if I were proposing to talk with a Chinese national in China?
A: No, if the information in question arose during or resulted from the same "fundamental research." You still should probably assume, however, that the Chinese national in China will be debriefed later about anything of potential military value he learns from you.
Q.10.2: Could I properly do some work with him in his research laboratory inside China?
A: If you release technology subject to the EAR that requires a license under the EAR, you must obtain a license or qualify for a license exception prior to releasing the technology. If the technology that you release is "published" (see § 734.7) or it arose during or is a result of "fundamental research" (see § 734.8), then it is not subject to the EAR.
Q.11: I would like to correspond and share research results, which deal with technology that requires a license to all destinations except Canada, with an Iranian expert in my field. Do I need a license to do so?
A: Not as long as it is information that arose during or resulted from "fundamental research" as described in § 734.8. If that is not the case – meaning the information is subject to the EAR – then that would be a deemed export and most likely would require a license from BIS prior to releasing the technology to the Iranian national.
Q.11.1: Suppose the research in question were funded by a corporate sponsor and I had agreed to prepublication review of any paper arising from the research?
A: Whether your research would be "fundamental" for purposes of the EAR would depend on the nature and purpose of the prepublication review. If the review is intended solely to ensure that your publications will neither compromise patent rights nor inadvertently divulge proprietary information that the sponsor has furnished to you, the research could still qualify as "fundamental." But if the sponsor will consider as part of its prepublication review whether it wants to hold your new research results as trade secrets or otherwise proprietary information (even if your voluntary cooperation would be needed for it to do so), your research would no longer qualify as "fundamental." For purposes of the EAR, it is whether the research results are ordinarily published and shared broadly that primarily determines whether the research counts as "fundamental" and so is not subject to the EAR.

*(*Continued On The Following Column)*

Q.12: In determining whether research is ordinarily published and shared broadly and therefore counts as "fundamental," does it matter where or in what sort of institution the research is performed?
A: In principle, no. "Fundamental research" is performed in industry, federal laboratories, or other types of institutions, as well as in universities. It remains the type of research, and particularly the intent and freedom to publish it that identifies "fundamental research," not the institutional locus.
Q.13: I am doing research on high-powered lasers in the central basic-research laboratory of an industrial corporation. I am required to submit the results of my research for prepublication review before I can publish them or otherwise make them public. I would Revisions to Definitions in the Export Administration Regulations: Frequently Asked Questions (FAQs) Effective September 1, 2016
Effective September 1, 2016 8

like to compare research results with a scientific colleague from Vietnam and discuss the results of the research with her when she visits the United States. Do I need a license to do so?
A: You may need a license. The information will be subject to the EAR if the prepublication review is intended to allow your sponsor to withhold the results of the research from publication. However, if the only restriction on your publishing any of that information is a prepublication review solely to ensure that publication would not compromise any patent rights or proprietary information provided by the company to the researcher, your research may be considered "fundamental research," in which case you may be able to share information because it is not subject to the EAR. Note that the information will be subject to the EAR if the prepublication review is intended to allow your sponsor to withhold the results of the research from publication.
Q.13.1: Suppose I have already cleared my company's review process and am free to publish all the information I intend to share with my colleague, though I have not yet published?
A: If the clearance from your company means that you are free to publish all the information without restriction, and you intend to publish it, the information is not subject to the EAR.
Q.14: I work as a researcher at a government-owned, contractor-operated research center. May I share the results of my unpublished research with foreign nationals without concern for export controls under the EAR?
A: That is up to the sponsoring agency and the center's management. If your research is designated "fundamental research" as defined in the EAR within any appropriate system devised by your agency or management to control release of information by scientists and engineers at the center, it will be treated as such by the Commerce Department, and the research will not be subject to the EAR. Otherwise, you would need to obtain a license or qualify for a license exception, except to publish or otherwise make the information public.

*(*Continued On The Following Page)*

Q.15: In a contract for performance of research entered into with the Department of Defense (DOD), we have agreed to specific national security controls. DOD is to have ninety days to review any papers we proposed before they are published and must approve assignment of any foreign nationals to the project. The work in question would otherwise be "fundamental research" under § 734.8. Is the information arising during or resulting from this sponsored research subject to the EAR?

A: Any export or reexport of information resulting from government-sponsored research that is inconsistent with any specific contract controls that you have agreed to will not be "fundamental research" and any such export or reexport would be subject to the EAR. The EAR does not restrict exports or reexports that are consistent with the specific national security controls. Thus, if you abide by the specific controls you have agreed to, you need not be concerned about violating the EAR. If you violate those controls and export or reexport information as "fundamental research" under § 734.8, you may subject yourself to the sanctions provided for under the EAR, including criminal sanctions, in addition to administrative and civil penalties for breach of contract under other laws. **Revisions to Definitions in the Export Administration Regulations: Frequently Asked Questions (FAQs) Effective September 1, 2016**
Effective September 1, 2016 9

Q.16: Do the Export Administration Regulations restrict my ability to publish the results of my research?

A: No, the Export Administration Regulations are not the means for enforcing the national security controls you have agreed to for such research that is not subject to the EAR; they do not restrict your ability to publish information. If such publication violates the underlying applicable contract entered into with the federal government, however, you may be subject to administrative, civil, and possible criminal penalties under other laws.

Patents (§ 734.10)

Q: Is the export or reexport of patented information fully disclosed on the public record subject to the EAR?

A: Information to the extent it is disclosed on the patent or an open (published) patent application available from or at any patent office is not subject to the EAR. The export or reexport of the information is not subject to the EAR because any person can obtain the technology from the public record and further disseminate or publish the information. For that reason, it is impossible to impose export controls that would restrict access to the information.

Definitions of Export and Reexport (§§ 734.13 and 734.14)

Q.1: Is performing a service on behalf of or for the benefit of a foreign person, whether in the United States or abroad, an export under the EAR?

A: Except for the proliferation-related controls in Part 744 and certain activities in Part 764, or as related to a denied person, the EAR do not control the provision of services as such. Rather, the EAR control the export, reexport, release,

*(*Continued On The Following Column)*

or transfer of items, regardless of whether in the performance of a service. Thus, if technology subject to the EAR will be released as part of performing the service, then authorization may be required for that release.

Q.2: I understand that a release in the United States of technology subject to the EAR to a foreign person is called a "deemed export" because it is deemed to be an export to the foreign person's most recent country of citizenship or permanent residency. I also understand that U.S. citizens, protected individuals as defined by 8 U.S.C. 1324b(a)(3), and lawful permanent residents of the United States are not foreign persons as defined in § 772.1. A release outside of the United States of technology subject to the EAR to a foreign person of another country (*i.e.*, a country different from the one in which the release takes place) is a deemed reexport to the foreign person's most recent country of citizenship or permanent residency (except as described in § 734.20). How do I determine the "permanent residency" status of a person in a foreign country?

A: This can be difficult, and some countries may not have an equivalent status. Factors to be considered include whether the individual (i) has the right to reside in the country indefinitely, (ii) is authorized to be employed by any employer in the country, and (iii) is eligible for unlimited entry and exit to/from the country without a visa. BIS recognizes concerns that may arise in instances where a foreign national maintains dual citizenship or multiple permanent **Revisions to Definitions in the Export Administration Regulations: Frequently Asked Questions (FAQs) Effective September 1, 2016**
Effective September 1, 2016 10

residence relationships. If the status of a foreign national is not certain, exporters can request the assistance of BIS to determine where the stronger ties lie, based on the facts of the specific case. In response to such a request, BIS will look at the foreign national's country, family, professional, financial, and employment ties.

Q.3: Is sending an item back to the United States a reexport?

A: No. Sending an item to the United States does not meet the definition of "reexport." Authorization under the EAR is not required to bring an item into the United States.

Q.4: When is transfer of ownership of a satellite not considered an export or reexport?

A: The mere transfer of ownership to an entity outside of a Country Group D:5 country (*e.g.*, as part of an on orbit transfer of ownership to an entity outside a D:5 country) of satellites subject to the EAR that are eligible for License Exception STA is not an export or reexport.

Release (§ 734.15)

Q.1: Does merely providing foreign persons in the United States with access to controlled equipment, software, or technology trigger a requirement to get a license or determine whether a license exception is available in order to be compliant with the EAR?

A: No. The question in such circumstances is whether

*(*Continued On The Following Page)*

"technology" is actually "released," as defined in § 734.15, during the provision of such access.

Q.2: I am a professor at a U.S. university, with expertise in design and creation of submicron devices. I have been asked to be a consultant for a foreign company that wishes to manufacture such devices. Do I need a license to do so?

A: Possibly. If you release technology that requires a license under the EAR, you will need to obtain a license or the release would need to qualify for a license exception. This guidance applies whether the release occurs in the U.S. or elsewhere.

Q.3: The manufacturing plant where I work is planning to begin admitting groups of the general public to tour the plant facilities. We are concerned that a license might be required if the tour groups include foreign nationals. Would such a tour constitute an export? If so, is the export subject to the EAR?

A: While the tour itself is not an export, visual inspection by foreign nationals of items subject to the EAR that reveals technology or source code is a "release" of that technology or source code. However, not all visual inspection results in such a release. Merely seeing an item briefly is not necessarily sufficient to constitute a release of the technology required, for example, to develop or produce it. Even if technology is released, if the tour is truly open to all members of the public, including your competitors, and you do not charge a fee that is not reasonably related to the cost of conducting the tours, any technology or source code released may be "published" (§ 734.7). Otherwise, you will have to obtain a license, the release would have to qualify for a license exception, or the release would have to be able to use the NLR designation, prior to permitting foreign nationals to tour your facilities.

Activities That Are Not Exports, Reexports, or Transfers (§ 734.18)

Q.1: What does "unclassified" mean in § 734.18?

A: Unclassified information" refers to information not classified in accordance with Executive Order 13526, 75 FR 707; 3 CFR 2010 Comp., p. 298, or a comparable predecessor or successor order.

Q.2: What is the "encryption carve-out"?

A: The export control "carve-out for encrypted data" results from a number of changes in technology and software controls implemented as part of Export Control Reform. The changes affect export controls on cross-national transmission of technical data in the Export Administration Regulations, and also release of such data to foreign persons. While not referencing cloud applications directly, these changes will have a major positive effect on the management and use of many cloud services. Most applicable provisions may be found in EAR §734.18 of the EAR, "Activities that are not exports, reexports or transfers."

*(*Continued On The Following Column)*

Q.3: Why is FIPS 140-2 specified for the carve-out?

A: The Federal Information Processing Standards Publication 140-2 ("FIPS 140-20") is a well-known set of cryptographic standards used for government procurement in the U.S and Canada. It is intended to set a baseline for the quality of encryption eligible for the carve-out. Specifically, hardware and software modules (and by extension, algorithms) certified as compliant by the National Institute of Standards and Technology (NIST) would qualify. FIPS 140-2 can be found at the NIST website:
http://csrc.nist.gov/groups/STM/cmvp/standards.html

Q.4: What level of security would qualify?

A: While FIPS 140-2 features four levels of security, § 734.18 does not specify what level is appropriate for a particular business environment. Moreover, the section references NIST publications as guidance for dimensions of cryptographic execution, such as key management that are not referenced in the FIPS 140-2 itself. The exporter is responsible for ensuring that modules and procedures implemented are sufficient to ensure protection of data within the context in which he or she operates.

Q.5: Is FIPS 140-2 the only cryptographic standard or approach that can be used for the carve-out?

A: No, and in fact the EAR specifically state that equally or more effective cryptographic means can be used. BIS recognizes that there are circumstances, such as cryptography developed for internal company use, that may be effective but that have never been subject to the NIST certification process. However, exporters must be sure that whatever standard and procedures are used are effective within the context in which the firm operates.

Q.6: How is "end-to-end" encryption defined for the purpose of this final rule? Revisions to Definitions in the Export Administration Regulations: Frequently Asked Questions (FAQs) Effective September 1, 2016
Effective September 1, 2016 12

A: "End-to-end" encryption is defined as cryptographic protection of data such that the data are not in unencrypted form between the originator or the originator's in-country security boundary and an intended recipient or the recipient's in-country security boundary.

Q.7: What is the significance of the in-country security boundary?

A: With certain applications, encryption/reencryption is not permitted at any point between the originator and the intended recipient. While applications that meet this criterion (like PGP) are common and well understood, such solutions are typically used by individuals, are not scalable to large organizations, and risk loss of keys, as key management is accomplished by the individuals at either end. Moreover, any services, such as malware screening, have to be done on clear text, which means the typical practice of providing them at an organizational level would be impossible.

*(*Continued On The Following Page)*

To address these concerns, the definition of end-to-end encryption prohibits decryption/re-encryption only between the in-country security boundaries of the originator and the recipient. This is consistent with the common practices in both the government and industry, and allows for desired or necessary services to be performed within security boundaries while meeting the security objective of the rule.

The "in-country" provision is intended to prevent exports of controlled data in unencrypted form resulting from defining security boundaries to include multiple countries. Any release of controlled data to non-U.S. nationals within the security boundary of a corporate intranet (as an example) would be treated as a deemed export requiring appropriate authorization, as is the case today.

Q.8: Is decryption/re-encryption permitted for data eligible for the carve-out?

A: Not in transit between security boundaries. Protected technology and code must not be in unencrypted form (i.e., in clear text) from the security boundary of the originator to the security boundary of the recipient. Decryption/re-encryption within the security boundary would be allowed in order to provide services such as anti-malware screening. Also, decryption/re-encryption would be allowed for data that is "super-encrypted" (that is encryption of data that has already been encrypted previously), provided that data under protection was not in the clear at any point between the security boundaries. Such multiple encryption is used in some VPN applications.

Q.9: My U.S. company needs to send technology to one of our employees in the U.K. The employee is a U.S. national, and we are securing the technology according to the criteria in § 734.18(a)(5). The technology in question would normally require a license to the U.K. Do we need a license? What if our U.S. national employee in the U.K. needs remote access to a server in the U.S. and we secure that access according to the criteria in § 734.18(a)(5)? What if another employee who is a U.K. national needs the same access?

A: Sending the technology secured according to the criteria in § 734.18(a)(5) is not an export. The recipient is a U.S. national, so the technology is not "released" (see § 734.15). The U.S. national's similarly secured remote access to the data on a U.S. server is also not an export. **Revisions to Definitions in the Export Administration Regulations: Frequently Asked Questions (FAQs) Effective September 1, 2016**
Effective September 1, 2016 13

Access by the U.K. national is a release of the technology to a foreign person that will need the same authorization as the export of the same technology to the U.K.

Q.10: Is giving someone remote access the same as "sending" for purposes of § 734.18(a)(5)?

A: Yes.

Q.11: What is the legal status of wholly non-U.S. technology that would be stored encrypted on a server in the U.S.?

A: While it is stored in the U.S., it is subject to the EAR. Storage of encrypted foreign-origin technology on a server in the U.S.

*(*Continued On The Following Column)*

is not sufficient to render it U.S.-origin technology, which is subject to the EAR wherever located.

Q.12: What if I don't encrypt my data to the standards in § 734.18(a)(5)?

A: Transmission of data not encrypted to the standards in § 734.18(a)(5) across a border is an export or reexport.

Activities That Are Not Deemed Reexports (§ 734.20)

Q.1: Do the list of activities in § 734.20 that do not constitute "deemed reexports" affect License Exception TSR?

A: No. If an activity is not a deemed reexport, then one doesn't need to consider whether TSR applies. If an activity is a deemed reexport, then one may still consider whether the technology at issue may be released under TSR pursuant to § 740.6.

Q.2: Does the term "entity," when used in § 734.20, refer to entities located outside of the U.S.?

A: Yes.

Q.3: Section 734.20(c)(5) describes situations that are not deemed reexports involving releases to persons who are not Country Group A:5 nationals. There are six situations listed, and some of them refer to information that is not in the EAR. Where can I find the information that is referenced?

A: The U.S.-U.K. Exchange of Notes regarding § 126.18 of the ITAR referred to in paragraph (c)(5)(iii) and the U.S.-Canadian Exchange of Letters regarding § 126.18 of the ITAR referred to in paragraph (c)(5)(iii) may be found at the following link: http://test.pmddtc.state.gov/licensing/agreement.html
The Agreements Guidelines referred to in paragraphs (c)(5)(v) and (vi) may be found at the following link: http://www.pmddtc.state.gov/licensing/documents/agreement_guidelinesv4.2.pdf **Revisions to Definitions in the Export Administration Regulations: Frequently Asked Questions (FAQs) Effective September 1, 2016**
Effective September 1, 2016 14

Definition of Technology (§ 772.1)

Q.1: For technology to be "use" technology, must it include all six elements of the definition of "use" in § 772.1, *i.e.*, operation, installation (including on-site installation), maintenance (checking), repair, overhaul and refurbishing technology?

A: Yes. If, however, an ECCN specifies one or more of the six elements of "use" in the heading or control text, each element specified is classified under that ECCN.

Q.2: Does information on the basic function or purpose of an item constitute "technology?"

A: No. Such information does not meet the definition of technology.

Q.3: My technology is not on the U.S. Munitions List, but it is not on the CCL either – what is it?

A: Technology not elsewhere specified on the CCL is designated as EAR99, unless the technology is subject to the exclusive jurisdiction of another U.S. government agency (see § 734.3(b)(1)) or is otherwise not subject to the EAR (see § 734.3(b)(2) and (b)(3) and §§ 734.7 through 734.10).

(*Continued On The Following Page)

Q.4: Are Build/Design-to-Specifications excluded from the definition of technology?
A: Such specifications are not per se outside the scope of the EAR's definition of "development" or "production" technology. Depending on the particular situation, it is theoretically possible that such specifications could constitute technology. A technical specification that conveys size, weight and performance requirements and does not include "build-to-print technology" likely would not meet the definition.
Q.5: The definition of technology contains the following note: "The modification of the design of an existing item creates a new item, and technology for the modified design is technology for the development or production of the new item." What does this mean?
A: BIS created this note to address the fact that multiple variations of a product are usually created by one or more companies, and companies often struggle with how to classify the technology that is and is not common to the variations. Consider, for example, a company that makes a civil aircraft switch controlled under ECCN 9A991.d. It later modifies the switch so that it would work in a military aircraft. The modified switch – the "dash one" model – is, in this example, specially designed for a military aircraft and thus controlled under ECCN 9A610.x. The technology that is common to both switches is 9E991, but the delta in technology to make the 9A610.x switch is controlled under 9E610. That is, whatever the technology is that is required to make the 9A991.d commercial aircraft switch into a 9A610.x switch is the technology for the new, modified item.
Issuance of Licenses (§ 750.7) Revisions to Definitions in the Export Administration Regulations: Frequently Asked Questions (FAQs) Effective September 1, 2016 Effective September 1, 2016 15

Q.1: The scope of § 750.7 states that a BIS license authorizing the release of technology to an entity also authorizes release of the same technology to the "entity's foreign nationals who are permanent and regular employees (and who are not proscribed persons…)." Is the entity receiving the technology responsible for screening its employees? Does the applicant have to confirm that the screening has been conducted prior to releasing the technology to the entity?
A: The entity receiving the technology is responsible for screening its foreign nationals who are permanent and regular employees, as consistent with local laws, and

*(*Continued On The Following Column)*

"When you feel like quitting think about why you started."

regular employees, as consistent with local laws, and must not release any technology authorized by the BIS license to employees who are "proscribed persons." The applicant is not required to confirm that the entity has screened its employees prior to releasing the technology to the entity.
Q.2: Do the expiration dates on BIS and DDTC licenses and other authorizations (e.g., BIS-748Ps, DSP-5s, TAAs, MLAs, and WDAs) apply only to the initial export, reexport, or transfer authorized or do they apply to all subsequent transactions that are otherwise within the scope of the authorization?
A: The expiration dates apply only to the initial export, reexport, or transfer authorized in the license or other authorization. That is, the initial export, reexport, or transfer must take place before the expiration date for it to be authorized. The expiration date does not apply to subsequent transactions involving the items at issue to the end users, destinations, and end uses described in the license or other authorization. Such transactions continue to be authorized so long as no condition or proviso to the license or other authorization limits such transactions and the U.S. government has not subsequently imposed additional controls on the end uses, end users, or destinations at issue, such as through the Entity List, the Debarred Parties List, or the Specially Designated Nationals List.
Temporary Exports of Technology (TMP)(§ 740.9)(a)(3)
Q.1: Can TMP be used for remote access to U.S. servers?
A: Yes, provided the other terms of paragraph (a)(3) are met.
Q.2: Is taking an encrypted device out of the U.S. an export?
A: Yes. Paragraph (a)(3) may authorize the technology on the device, but the device itself is a commodity that, if it requires a license to its destination, would need to be authorized by another provision in the EAR, *e.g.*, by paragraph (a)(1)(Tools of trade).
Q.3: Can obfuscation/tokenization be used to protect data? (Tokenization is a process through which data or documents are obfuscated by replacing underlying clear text with a surrogate value called a "token.")
A: Done properly, yes, this is an effective security measure.

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