EIB World Trade Headlines

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

October 15, 2016 - Volume 8, Issue 19

FINAL Revisions to the Export Administration Regulations (EAR): and ITAR CAT XII Fire Control, Laser, Imaging, and Guidance Equipment, effective Dec 31, 2016

10/12/16
81 FR 70320
Revisions to the Export Administration Regulations (EAR): Control of Fire Control, Laser, Imaging, and Guidance Equipment the President Determines No Longer Warrant Control Under the United States Munitions List (USML) This final rule describes how articles the President determines no longer warrant control under Category XII (Fire Control, Laser, Imaging, and Guidance Equipment) of the United States Munitions List (USML) of the International Traffic in Arms Regulations (ITAR) will be controlled under the Commerce Control List (CCL) of the Export Administration Regulations (EAR) by amending Export Control Classification Number (ECCN) 7A611 and creating new ''600 series'' ECCNs 7B611, 7D611, and 7E611. In addition, for certain dual-use infrared detection items, this final rule expands controls for certain software and technology, eliminates the use of some license exceptions, revises licensing policy, and expands license requirements for certain transactions involving military end users or foreign military commodities. This final rule also harmonizes provisions within the EAR by revising controls related to certain quartz rate sensors. This rule is effective December 31, 2016.
http://www.bis.doc.gov/index.php/regulations/federal-register-notices#fr70320

NEWSLETTER NOTES

National Manufacturing & Supply Chain Conference & Exhibition 31st January 2017

2017 National Manufacturing Conference & Exhibition on the 31st of January 2017 to hear from an impressive line-up of manufacturing leaders, academics and government agencies who will engage in a stimulating blend of key note addresses and debates. http://www.manufacturingevent.com

Creating an Innovative Manufacturing & Supply chain Ecosystem

New approaches and technology have been introduced in recent years that have created significant organisational and process improvements. The aim of the conference is to showcase such innovative approaches and to disseminate the cutting edge research that underpins them.

The conference will be of interest to senior management, established practicing engineers and researchers together with those that are much earlier in their careers.

Delegates have registered from leading food, pharmaceutical, medical, chemical, electronics and engineering manufacturing sectors.

Manufacturing on this island of Ireland has some of the best people, products, brands and innovation. We deserve nothing less than the best business environment to chart a new economic course to growth. But government needs to set the climate and conditions to allow this to happen.

Manufacturers small and large from across the country will gather to challenge political decision makers to deliver a business environment which manufacturing deserves. Delegates attending the conference will:

- gain industry insights to help their business plan ahead
- share good practice and learn from each other's experience
- connected with senior business leaders to find new business opportunities
- meet with key technology providers in the dedicated exhibition area

Washington

WASHINGTON (AP) — U.S. manufacturing rebounded in September after contracting in August. New orders and production at factories increased, although employment fell — a sign that manufacturers have yet to fully stabilize after a difficult year.

The Institute for Supply Management said Monday that its manufacturing index rose to 51.5 in September from 49.4 in August. Any reading above 50 signals expansion.

Government contractor secretly arrested for allegedly removing classified materials

The contractor, Harold Thomas Martin III of Glen Burnie, Md., was arrested on Aug. 27. A criminal complaint unsealed in federal court today says authorities recovered highly classified information from his home and car, including six sensitive documents dating to 2014.

DEPARTMENT OF STATE

22 CFR Parts 120 and 126 [Public Notice: 9602] RIN 1400–AD95
Amendment to the International Traffic in Arms Regulations: Tunisia, Eritrea, Somalia, the Democratic Republic of the Congo, Liberia, Coˆ te d'Ivoire, Sri Lanka, Vietnam, and Other Changes
Federal Register/Vol. 81, No. 189/Thursday, September 29, 2016/Rules and Regulations **66805**

AGENCY: Department of State. **ACTION:** Interim final rule.

SUMMARY: The Department of State is amending the International Traffic in Arms Regulations (ITAR) to designate Tunisia as a major non-NATO ally (MNNA); reorganize the content in several paragraphs to clarify the intent of the ITAR; update defense trade policy regarding Eritrea, Somalia, the Democratic Republic of the Congo, Liberia, and Coˆte d'Ivoire to reflect resolutions adopted by the United Nations Security Council; update defense trade policy regarding Sri Lanka to reflect the Consolidated Appropriations Act, 2016; and update defense trade policy regarding Vietnam to reflect a determination made by the Secretary of State.

DATES: The rule is effective on September 29, 2016. The Department of State will accept comments on this interim final rule until October 31, 2016.

*(*Continued On The Following Page)*

ADDRESSES: Interested parties may submit comments within 30 days of the date of publication by one of the following methods:

• *Email:* DDTCPublicComments@state.gov with the subject line, ''ITAR Amendment— Section 126.1 Re-organization.''

• *Internet:* At *www.regulations.gov,* search for docket number DOS–2016– 0059. Comments received after that date may be considered, but consideration cannot be assured. Those submitting comments should not include any personally identifying information they do not desire to be made public or information for which a claim of confidentiality is asserted because those comments and/or transmittal emails will be made available for public inspection and copying after the close of the comment period via the Directorate of Defense Trade Controls Web site at *www.pmddtc.state.gov.* Parties who wish to comment anonymously may do so by submitting their comments via *www.regulations.gov,* leaving the fields that would identify the commenter blank and including no identifying information in the comment itself. Comments submitted via *www.regulations.gov* are immediately available for public inspection.

FOR FURTHER INFORMATION CONTACT: Mr. C. Edward Peartree, Director, Office of Defense Trade Controls Policy, U.S. Department of State, telephone (202) 663–2792, or email *DDTCResponseTeam@state.gov.* ATTN: Regulatory Change, ITAR Section 126.1 Update 2016.

SUPPLEMENTARY INFORMATION: In Presidential Determination No. 2015– 09, on July 10, 2015, President Obama exercised his authority under § 517 of the Foreign Assistance Act of 1961 (FAA) to designate Tunisia as a MNNA for the purposes of the FAA and the Arms Export Control Act (AECA). The Department of State amends ITAR § 120.32 to reflect this change.

Paragraphs (a), (c), and (d) of § 126.1 of the ITAR are updated to enhance their clarity. The fundamental content of the aforementioned paragraphs is not changing, but is reorganized in this rule by subject matter. The lists of proscribed countries were previously in multiple

paragraphs, but are now consolidated in paragraph (d). Provisions relevant to the rationale for defense trade sanctions, previously located in paragraphs (a), (c), and (d) are now consolidated in paragraph (c). Section 126.18 of the ITAR is amended to maintain conformity with revised paragraph (d) of ITAR § 126.1.

Recent actions by the United Nations (UN), Congress, and the Executive require the Department to amend ITAR § 126.1 to reflect the change in policy towards individual nations identified in that section.

*(*Continued On The Following Column)*

On October 23, 2015, the United Nations Security Council (UNSC) adopted United Nations Security Council Resolution (UNSCR) 2244, which reaffirmed the arms embargoes on Eritrea and Somalia. Exemptions from the arms embargo on Somalia are set forth in paragraphs 6 through 11 of UNSCR 2111 and paragraphs 2 through 9 of UNSCR 2142. Thus subparagraphs (1) and (2) of § 126.1(m) of the ITAR have been revised to reflect this change, and subparagraphs (3) through (6) are added to reflect new exceptions for Somalia as enumerated in UNSCR 2111. The revised control text follows the language as published in the aforementioned UNSCRs.

Exemptions from the arms embargo on Eritrea are set forth in paragraphs 12 and 13 of UNSCR 2111; consequently, Eritrea will be moved to paragraph (h) of § 126.1. The revised control text follows the language as published in the aforementioned UNSCRs. The Department modifies paragraph (h) of ITAR § 126.1 accordingly.

On June 23, 2016, the UNSC adopted Resolution 2293, which expanded the exemptions from the arms embargo on the Democratic Republic of the Congo. Exemptions from the arms embargo are set forth in paragraph 3 of the UNSCR. The revised control text follows the language as published in the aforementioned UNSCR. The Department modifies paragraph (i) of ITAR § 126.1 accordingly.

On May 25, 2016, the UNSC adopted Resolution 2288, which terminated the sanctions regime against Liberia, including restrictions on exports to Liberia of arms and related materiel. The Department reserves paragraph (o) to remove Liberia from ITAR § 126.1.

On April 28, 2016 the UNSC adopted Resolution 2283, which terminated the sanctions regime against Coˆte d'Ivoire, including restrictions on exports to Coˆte d'Ivoire of arms and related materiel. The Department reserves paragraph (q) to remove Coˆte d'Ivoire from ITAR § 126.1.

Licensing restrictions relating to Sri Lanka articulated in section 7044(e) of the Consolidated Appropriations Act, 2015, Public Law 113–235, and in previous appropriations acts, were not carried forward in section 7044(e) of the Consolidated Appropriations Act, 2016, Public Law 114–113. Therefore, the Department reserves paragraph (n) to remove Sri Lanka from ITAR § 126.1.

The Secretary of State lifted the ban on lethal weapons sales to Vietnam in May 2016. Accordingly, the Department reserves paragraph (l) and the associated note to remove Vietnam from ITAR § 126.1.

For more information, please visit the Directorate of Defense Trade Controls (DDTC) internet Web site at *https:// www.pmddtc.state.gov/.*

Hack-A-Jeep 101: Renowned Security Expert Will Explain How He Did It

Charlie Miller security engineer for Uber Technologies, Inc., told *Design News*. "If someone hacks into your computer, they can steal your photos and maybe even get your credit card numbers, so you have a bad day. But if they can hack into your car and crash it while you're driving with your family, that's another matter."

The chilling story behind Miller's Jeep hack is proof that the potential dangers are real. With a writer from *Wired* at the wheel in 2015, Miller and fellow hacker Chris Valasek remotely operated the vehicle's radio, climate system, and windshield wipers. Then, with the writer rolling down I-64 in Missouri, they disabled the accelerator. The hackers accomplished those feats from a laptop computer located 10 miles away.

"We were sending messages to these computer systems, pretending to be other computers on the vehicle network," Miller explained. "We would tell them to do things, like disabling the brakes. From end to end, we could remotely attack the car and control physical systems, and that's really scary."

Within days of Miller's widely-reported hack, Fiat Chrysler Automobiles recalled a host of its vehicles, including various modes of the Jeep Grand Cherokee, Dodge Viper, Dodge Durango, Chrysler 200, Chrysler 300, Dodge Challenger, and Ram.

Miller, who holds a Ph.D. in mathematics from the University of Notre Dame, isn't formally trained in automotive engineering. He's a cyber security expert who spent five years at the National Security Agency and later became notable for compromising a variety of consumer products. In 2008, he won a $10,000 cash prize at a hacker conference in Vancouver, Canada, for being the first to find a bug in the MacBook Air. In 2009, he won $5,000 for cracking a Safari web browser. In 2011, he found a security hole in Apple's iPhone and iPad products that would let malicious hackers install unauthorized apps to steal consumers' data.

Miller's work on the Jeep has been his most notable to date, however. He told *Design News* that he and Valasek did it by accessing the Jeep's Uconnect service, going through its radio-navigation computer in the head unit, and then linking to its CAN bus. "We were trying to find the shortest path from the computers that talked to the outside world to the computers that affected physical safety," he said. The key was the Jeep's park assist and lanekeeping systems, both of which were accessible, he added.Although Chrysler has since fixed the bugs, Miller believes hackers will conjure up new ways to remotely access vehicles. "We have these features that make our lives easy and protect us," he said. "But those same features are also a way for a hacker to take advantage and gain control of our cars."

THE CIPHER BRIEF

August 28, 2016

In the wake of a series of hacks against government and private networks, it is clear that Russia and China are among the most active and proficient nations in regards to cyber operations. One needs to only review the most high-profile breaches to see that many of them are believed to be the work of one of these countries. China is thought to be behind the OPM hack and has been hacking a large number of American businesses to steal trade secrets and intellectual property. Russia almost certainly hacked the DNC and has breached networks at both the White House and the State Department. Clearly, both China and Russia are finding value in cyber operations as a means of achieving their foreign policy goals, and this is likely to create a more perilous cyber environment moving forward.

Simply put, cyber-operations provide too many advantages for either Russia or China to decrease their reliance upon them. As The Cipher Brief has previously reported, cyber-operations are very difficult to conclusively attribute to any given nation. Even in the cases of the OPM hack and the DNC hack, most experts will only say that the code was developed by Chinese or Russian speakers, and that the attacks were launched from within their territory. However, that is not enough in and of itself for formal charges of blame to be levied against either country.

Cyber operations are also an essentially asymmetric tool, in that they level the playing field between nations that may have wide disparities in terms of the effectiveness of their conventional forces. However, this cuts both ways, as the United States also conducts a considerable number of cyber operations in support of intelligence collection. This leads into the third primary advantage of cyber as it relates to espionage, which is that cyber-capabilities make exfiltrating large volumes of information much, much easier than would be the case otherwise. These advantages translate directly into gains towards foreign policy goals for both Russia and China. Leo Taddeo, Chief Security Officer at Cryptzone, told The Cipher Breif that "while both of them are engaged in both types of activity, I think the emphasis by the Russians is on diplomatic and military information and the emphasis for the Chinese is on business information." Russia wants access to military and diplomatic information in order to influence events in Europe in a way that is advantageous to its interests.

In contrast, China needs access to foreign intellectual property in order to keep their economy going. According to Justin Harvey, Chief Security Officer at Fidelis Cybersecurity, the Chinese "have reached a point with technology and their economy where it's been boosted and injected full of our commercial intellectual property, but to sustain that technological advancement requires a lot more infrastructure, education, and people that they don't have yet."

(*Continued On The Following Page)

Cyber operations have proven to be an extremely subtle and flexible tool that nations can use to pursue their objectives while minimizing the chances of any given action escalating tensions into outright war. For this reason, it is reasonable to assume that Russia will continue to exploit cyber vulnerabilities to aid in intelligence collection and battlefield preparation efforts. There is no incentive for Russia to stop doing either, as both support their goal of countering the United States' ability to challenge them in Europe.
Likewise, the Chinese will continue to use cyber to gain advantage in terms of economic growth. While there is evidence that China has backed off from cyber-enabled economic espionage against the United States, it has plenty of other targets to pick from in Europe and Asia. And, despite their focus on meeting economic objectives, China will likely continue to engage in traditional espionage as well.
Both nations will almost certainly continue to grow in sophistication and will work to make their actions even harder to attribute, as this will expand the usefulness of their cyber operations. The United States will need to work to keep pace in terms of detection and cyber-forensics if there is to be any hope of establishing credible deterrence against these adversaries.

ARRESTS, TRIALS AND CONVICTIONS

Department of Justice
Office of Public Affairs
FOR IMMEDIATE RELEASE
Monday, September 26, 2016
Four Chinese Nationals and China-Based Company Charged with Using Front Companies to Evade U.S. Sanctions Targeting North Korea's Nuclear Weapons and Ballistic Missile Programs
Company Allegedly Violated Sanctions by Facilitating U.S. Dollar Transactions on Behalf of a North Korean Bank with Ties to Weapons of Mass Destruction Proliferators
Four Chinese nationals and a trading company based in Dandong, China, were charged by criminal complaint unsealed today with conspiring to evade U.S. economic sanctions and violating the Weapons of Mass Destruction Proliferators Sanctions Regulations (WMDPSR) through front companies by facilitating prohibited U.S. dollar transactions through the United States on behalf of a sanctioned entity in the through U.S. financial institutions.

Assistant Attorney General Leslie R. Caldwell of the Justice Department's Criminal Division, Assistant Attorney General for National Security John P. Carlin, U.S. Attorney Paul J. Fishman of the District of New Jersey and Assistant Director E.W. Priestap of the FBI's Counterintelligence Division made the announcement.

*(*Continued On The Following Column)*

On Aug. 3, 2016, a U.S. Magistrate Judge Joseph A. Dickson of the District of New Jersey signed a criminal complaint charging Ma Xiaohong (Ma) and her company, Dandong Hongxiang Industrial Development Co. Ltd. (DHID), and three of DHID's top executives, general manager Zhou Jianshu (Zhou), deputy general manager Hong Jinhua (Hong) and financial manager Luo Chuanxu (Luo), with conspiracy to violate the International Emergency Economic Powers Act (IEEPA) and to defraud the United States; violating IEEPA; and conspiracy to launder monetary instruments.
Today, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) also imposed sanctions on DHID, Ma, Zhou and Hong for their ties to the government of North Korea's weapons of mass destruction proliferation efforts.
In addition, the department filed a civil forfeiture action for all funds contained in 25 Chinese bank accounts that allegedly belong to DHID and its front companies. The department has also requested tha the federal court in the District of New Jersey issue a restraining order for all of the funds named in the civil forfeiture action, based upon the allegation that the funds represent property involved in money laundering, which makes them forfeitable to the United States. There are no allegations of wrongdoing by the U.S. correspondent banks or foreign banks that maintain these accounts.
"The charges and forfeiture action announced today allege that defendants in China established and used shell companies around the world, surreptitiously moved money through the United States and violated the sanctions imposed on North Korea in response to, among other things, its nuclear weapons program," said Assistant Attorney General Caldwell. "The actions reflect our efforts to protect the integrity of the U.S. banking system and hold accountable those who seek to evade U.S. sanctions laws."
"The charges unsealed today reflect our nation's commitment to using all tools to deter and disrupt weapons of mass destruction proliferators," said Assistant Attorney General Carlin. "One of the strengths of our sanctions programs is that they prevent sanctioned wrongdoers from engaging in U.S. dollar transactions. Denying the use of the U.S. financial system can greatly curtail illegal activities and disrupt efforts to provide weapons of mass destruction to terrorists and rogue nations. Those who seek to evade our financial sanctions will be fully prosecuted, and we will be unflagging in our efforts to bring them to justice."
"The FBI takes violations of these laws extremely seriously and will not hesitate to use our full investigative resources to stop this type of illegal activity," said Assistant Director Priestap. "In this case agents, analysts and forensic accountants from field offices in Phoenix and Newark, as well as FBI Headquarters, all contributed to a successful investigation."

*(*Continued On The Following Page)*

According to criminal and civil complaints, DHID is primarily owned by Ma and is located near the North Korean border. DHID allegedly openly worked with North Korea-based Korea Kwangson Banking Corporation (KKBC) prior to Aug. 11, 2009, when the OFAC designated KKBC as a Specially Designated National (SDN) for providing U.S. dollar financial services for two other North Korean entities, Tanchon Commercial Bank (Tanchon) and Korea Hyoksin Trading Corporation (Hyoksin). President Bush identified Tanchon as a weapons of mass destruction proliferator in June 2005, and OFAC designated Hyoksin as an SDN under the WMDPSR in July 2009. Tanchon and Hyoksin were so identified and designated because of their ties to Korea Mining Development Trading Company (KOMID), which OFAC has described as North Korea's premier arms dealer and main exporter of goods and equipment related to ballistic missiles and conventional weapons. The United Nations (UN) placed KOMID, Tanchon and Hyoksin on the UN Sanctions List in 2006. In March 2016, KKBC was added to the UN Sanctions List.

In August 2009, Ma allegedly conspired with Zhou, Hong and Luo to create or acquire numerous front companies to conduct U.S. dollar transactions designed to evade U.S. sanctions. The complaints allege that from August 2009 to September 2015, DHID used these front companies, established in offshore jurisdictions such as the British Virgin Islands, the Seychelles and Hong Kong, and opened Chinese bank accounts to conduct U.S. dollar financial transactions through the U.S. banking system when completing sales to North Korea. These sales transactions were allegedly financed or guaranteed by KKBC. These front companies facilitated the financial transactions to hide KKBC's presence from correspondent banks in the United States, according to the allegations in the complaints.

As a result of the defendants' alleged scheme, KKBC was able to cause financial transactions in U.S. dollars to transit through the U.S. correspondent banks without being detected by the banks and, thus, were not blocked under the WMDPSR program.

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

The FBI is investigating the case. Trial Attorneys Jennifer Wallis and Michael Parker of the Criminal Division's Asset Forfeiture and Money Laundering Section, Trial Attorney Christian Ford of the National Security Division's Counterintelligence and Export Control Section and Chief Barbara Ward and Assistant U.S. Attorneys Joyce Malliet and Sarah Devlin of the District of New Jersey are prosecuting the case. The Criminal Division's Office of International Affairs provided valuable assistance in this matter.

CYBER, HACKING, DATA THEFT, COMPUTER INTRUSIONS & RELATED

PSA: Ransomware Victims Urged to Report Infections to Federal Law Enforcement

The FBI has reported that ransomware attacks amassed more than $200 million during the first three months of 2016, signaling that cyber-criminals are on track to gain more than $1 billion through ransomware by the end of the year.

FBI Internet Crime Complaint Center (IC3) WWW.IC3.GOV

September 15, 2016

The FBI urges victims to report ransomware incidents to federal law enforcement to help us gain a more comprehensive view of the current threat and its impact on U.S. victims. LINK: https://www.ic3.gov/media/2016/160915.aspx)

What Is Ransomware?

Ransomware is a type of malware installed on a computer or server that encrypts the files, making them inaccessible until a specified ransom is paid. Ransomware is typically installed when a user clicks on a malicious link, opens a file in an e-mail that installs the malware, or through drive-by downloads (which does not require user-initiation) from a compromised Web site.

Why We Need Your Help

New ransomware variants are emerging regularly. Cyber security companies reported that in the first several months of 2016, global ransomware infections were at an all-time high. Within the first weeks of its release, one particular ransomware variant compromised an estimated 100,000 computers a day.

Ransomware infections impact individual users and businesses regardless of size or industry by causing service disruptions, financial loss, and in some cases, permanent loss of valuable data. While ransomware infection statistics are often highlighted in the media and by computer security companies, it has been challenging for the FBI to ascertain the true number of ransomware victims as many infections go unreported to law enforcement.

Victims may not report to law enforcement for a number of reasons, including concerns over not knowing where and to whom to report; not feeling their loss warrants law enforcement attention; concerns over privacy, business reputation, or regulatory data breach reporting requirements; or embarrassment. Additionally, those who resolve the issue internally either by paying the ransom or by restoring their files from back-ups may not feel a need to contact law enforcement. The FBI is urging victims to report ransomware incidents regardless of the outcome. Victim reporting provides law enforcement with a greater understanding of the threat, provides justification for ransomware investigations, and contributes relevant information to ongoing ransomware cases.

*(*Continued On The Following Page)*

Threats to Users

All ransomware variants pose a threat to individual users and businesses. Recent variants have targeted and compromised vulnerable business servers (rather than individual users) to identify and target hosts, thereby multiplying the number of potential infected servers and devices on a network. Actors engaging in this targeting strategy are also charging ransoms based on the number of host (or servers) infected. Additionally, recent victims who have been infected with these types of ransomware variants have not been provided the decryption keys for all their files after paying the ransom, and some have been extorted for even more money after payment. This recent technique of targeting host servers and systems could translate into victims paying more to get their decryption keys, a prolonged recovery time, and the possibility that victims will not obtain full decryption of their files.

What to Report to Law Enforcement

The FBI is requesting victims reach out to their local FBI office and/or file a complaint with the Internet Crime Complaint Center, at www.IC3.gov, with the following ransomware infection details (as applicable):

· Date of Infection
· Ransomware Variant (identified on the ransom page or by the encrypted file extension)
· Victim Company Information (industry type, business size, etc.)
· How the Infection Occurred (link in e-mail, browsing the Internet, etc.)
· Requested Ransom Amount
· Actor's Bitcoin Wallet Address (may be listed on the ransom page)
· Ransom Amount Paid (if any)
· Overall Losses Associated with a Ransomware Infection (including the ransom amount)
· Victim Impact Statement

Defense

The FBI recommends users consider implementing the following prevention and continuity measures to lessen the risk of a successful ransomware attack.

· Regularly back up data and verify the integrity of those backups. Backups are critical in ransomware incidents; if you are infected, backups may be the best way to recover your critical data.
· Secure your backups. Ensure backups are not connected to the computers and networks they are backing up. Examples might include securing backups in the cloud or physically storing them offline. It should be noted, some instances of ransomware have the capability to lock cloud-based backups when systems continuously back up in real-time, also known as persistent synchronization.

(*Continued On The Following Column

"Teamwork makes the dream work"

· Scrutinize links contained in e-mails and do not open attachments included in unsolicited e-mails.
· Only download software – especially free software – from sites you know and trust. When possible, verify the integrity of the software through a digital signature prior to execution.
· Ensure application patches for the operating system, software, and firmware are up to date, including Adobe Flash, Java, Web browsers, etc.
· Ensure anti-virus and anti-malware solutions are set to automatically update and regular scans are conducted.
· Disable macro scripts from files transmitted via e-mail. Consider using Office Viewer software to open Microsoft Office files transmitted via e-mail instead of full Office Suite applications.
· Implement software restrictions or other controls to prevent the execution of programs in common ransomware locations, such as temporary folders supporting popular Internet browsers, or compression/decompression programs, including those located in the AppData/LocalAppData folder.

Training

Registration is still open for the 29th Annual Update Conference on Export Controls and Policy in Washington, D.C., October 31-November 2, 2016. This major outreach activity draws business and government representatives from around the world to learn and exchange ideas about export control issues. It is one of the Commerce Department's most notable international trade events. A conference room rate is offered at the Washington Hilton Hotel, 1919 Connecticut Avenue, N.W., Washington, D.C. 20009, subject to room availability, until October 11 only. This date represents an extension of the special conference room rate availability.

http://www.bis.doc.gov/index.php/component/content/article/222-update-2016/1124-update-2016-details