EIB World Trade Headlines

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

April 15, 2016 - Volume 8, Issue 7

Webinar - "Specially Designed"

Please join the Bureau of Industry and Security on Wednesday, April 27 at 2:30 p.m. Eastern Time for a ninety-minute session on the definition of "specially designed and its application in different contexts. Kevin Wolf, Assistant Secretary of Commerce for Export Administration, and other subject matter experts from the Bureau of Industry and Security will discuss the framework of the definition, including the 'catch' and 'release' construct, provide an overview of the application of "specially designed" in different contexts, and highlight key things learned by BIS and industry from applying "specially designed" since the revised definition became effective on October 15, 2013.

Participants will be able to submit questions for answers by the BIS presenters during the session. There will be a $50 charge for this webinar. For detailed instructions on registration and payment, and on how to join the webinar on the day of the broadcast, please use the following link: https://www.webcaster4.com/Webcast/Page/914/14449

Please register as soon as possible for this webinar, as we will not be able to accept registrations after Tuesday, April 26. Once you have registered and paid, you will receive information to enable you to log in on the day of the webinar. You are strongly encouraged to test your connection before the webinar by using the link provided for that purpose.

*(*Continued On The Following Page)*

NEWSLETTER NOTES

Visa Waiver Program

http://www.cbp.gov/travel/international-visitors/visa-waiver-program

The Visa Waiver Program (VWP), administered by the Department of Homeland Security (DHS) in consultation with the State Department, permits citizens of 38 countries to travel to the United States for business or tourism for stays of up to 90 days without a visa. In return, those 38 countries must permit U.S. citizens and nationals to travel to their countries for a similar length of time without a visa for business or tourism purposes.

IMPORTANT NOTICE!

Travelers in the following categories are no longer eligible to travel or be admitted to the United States under the Visa Waiver Program (VWP):

- Nationals of VWP countries who have traveled to or been present in Iran, Iraq, Sudan, or Syria on or after March 1, 2011 (with limited exceptions for travel for diplomatic or military purposes in the service of a VWP country).
- Nationals of VWP countries who are also nationals of Iran, Iraq, Sudan, or Syria.

In addition, **as of April 1, 2016, you must have an e-passport to use the VWP**. An e-Passport is an enhanced secure passport with an embedded electronic chip. You can readily identify an e-Passport, because it has a unique international symbol on the cover.

Electronic System for Travel Authorization (ESTA)

ESTA is an automated system that determines the eligibility of visitors to travel to the United States under the Visa Waiver Program (VWP). Authorization via ESTA does not determine whether a traveler is admissible to the United States. U.S. Customs and Border Protection officers determine admissibility upon travelers' arrival. The ESTA application collects biographic information and answers to VWP eligibility questions. ESTA applications may be submitted at any time prior to travel, though it is recommended that travelers apply as soon as they begin preparing travel plans or prior to purchasing airline tickets.

Other Visa Information

- Frequently Asked Questions about the VWP and the VWP Improvement and Terrorist Travel Prevention Act of 2015
- Frequently Asked Questions about the VWP and the ESTA
- VWP Signatory Carriers List
- Guam- CNMI Visa Waiver Program
- Guam-CNMI VWP Signatory Carriers

Travel by Pleasure Boats or Ferries

*(*Continued On The Following Column)*

FLYING TO CANADA? ENTRY RULES HAVE CHANGED

Canada has introduced a new entry requirement, known as Electronic Travel Authorization (eTA), for visa-exempt foreign nationals traveling to Canada by air. Exceptions include U.S. citizens and travelers with a valid visa. Apply online today: Canada.ca/eTA

Announces the Electronic Visa Update System

Release Date:
March 15, 2016

Nationals of the People's Republic of China with a 10-year visa will update their information every two years using EVUS

WASHINGTON—U.S. Customs and Border Protection (CBP) announced today the anticipated establishment of the Electronic Visa Update System (EVUS), a new platform under development designed to enhance border security in accordance with the bilateral arrangement with China to issue 10-year validity tourist and business visas. Beginning in November 2016, nationals of the People's Republic of China holding 10-year visas B1/B2, B1 and B2 visas will be required to complete an online form to update certain biographic information. Travelers will need to have a valid EVUS enrollment prior to traveling to the United States. An EVUS enrollment is valid for two years or until the traveler obtains a new passport, whichever comes first.

"More than 2.7 million nationals of the People's Republic of China are part of the 10-year visa program, a milestone in diplomatic relations between the U.S. and China," said Commissioner R. Gil Kerlikowske. "The Electronic Visa Update System will enable CBP to enhance the security of the program while facilitating legitimate travel."

In addition to having valid 10-year visas, such travelers will be required to complete EVUS enrollments, prior to their first travel to the United States and at least once every two years, to be admitted into the United States. A nominal fee will be charged at the time of the EVUS enrollment and subsequent updates. This update will generally be valid for two years and will help to facilitate entry into the United States. EVUS will go-live in November 2016. Travelers will be asked to update/verify the following fields: name, address, date of birth, passport number, and other basic biographic information needed to expedite entry into the United States. Visa holders do not need to do anything until the platform has officially launched.

The EVUS process is similar to the process that travelers from 38 other countries must follow before traveling to the United States. If Chinese travelers do not update their information at

*(*Continued On The Following Page)*

least every two years, or upon obtaining a new passports after EVUS becomes effective, they will not be able to use their 10-year visas.

U.S. Customs and Border Protection is the unified border agency within the Department of Homeland Security charged with the management, control and protection of our nation's borders at and between the official ports of entry. CBP is charged with keeping terrorists and terrorist weapons out of the country while enforcing hundreds of U.S. laws.

Join *The Nation* for a week of educational and cultural exchange in Havana, Cuba! October 8-15th, 2016

Join us in Havana, Cuba, during this historic period of change, for a unique trip specially curated for fellow *Nation* travelers. The experience is certain to offer a unique opportunity not only to visit the island but also to experience its people, politics, culture, and history in a way few ever have.

After our chartered flight from Tampa arrives at Havana's historic José Martí International Airport, we will attend private seminars and concerts featuring prominent Cuban professors, government officials, urban planners, journalists, musicians, artists, dancers, and community activists. We'll also tour museums with renowned art historians, wander through the artist's markets of Old Havana, experience the hospitality of local residents in small country towns, and savor traditional Cuban food and spirits at the island's finest restaurants and markets.

The all-inclusive cost of this weeklong tour is $5,585 to $5,990 per person (double/single occupancy) and includes round-trip chartered airfare between Tampa and Havana, six nights at the Hotel NH Capri La Habana, one night in a private guesthouse in Pinar del Río Province, all transportation within Cuba, tours, seminars, lectures, concerts, most of your meals, and many other captivating events.

Complete the appropriate registration form and submit it, with a $1000 deposit, to *The Nation* by email, fax (212-982-9000 – Attn: Kelsea), or mail (*The Nation*, Cuba Trip, 33 Irving Place, New York, NY 10003). Once you are approved for travel to Cuba (Cuba and the US have a simple application process that all travelers must follow) *The Nation* will contact you regarding further payments.

October Registration Form

For additional information or to register, contact Charles Bittner at charles@thenation.com or 617-833-1435

U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage First Time Criminal Charges Are Filed Against Known State Actors for Hacking

A grand jury in the Western District of Pennsylvania (WDPA) indicted five Chinese military hackers for computer hacking, economic espionage and other offenses directed at six American victims in the U.S. nuclear power, metals and solar products industries.

The indictment alleges that the defendants conspired to hack into American entities, to maintain unauthorized access to their computers and to steal information from those entities that would be useful to their competitors in China, including state-owned enterprises (SOEs). In some cases, it alleges, the conspirators stole trade secrets that would have been particularly beneficial to Chinese companies at the time they were stolen. In other cases, it alleges, the conspirators also stole sensitive, internal communications that would provide a competitor, or an adversary in litigation, with insight into the strategy and vulnerabilities of the American entity.

"This is a case alleging economic espionage by members of the Chinese military and represents the first ever charges against a state actor for this type of hacking," U.S. Attorney General Eric Holder said. "The range of trade secrets and other sensitive business information stolen in this case is significant and demands an aggressive response. Success in the global market place should be based solely on a company's ability to innovate and compete, not on a sponsor government's ability to spy and steal business secrets. This Administration will not tolerate actions by any nation that seeks to illegally sabotage American companies and undermine the integrity of fair competition in the operation of the free market."

"For too long, the Chinese government has blatantly sought to use cyber espionage to obtain economic advantage for its state-owned industries," said FBI Director James B. Comey. "The indictment announced today is an important step. But there are many more victims, and there is much more to be done. With our unique criminal and national security authorities, we will continue to use all legal tools at our disposal to counter cyber espionage from all sources."

"State actors engaged in cyber espionage for economic advantage are not immune from the law just because they hack under the shadow of their country's flag," said John Carlin, Assistant Attorney General for National Security. "Cyber theft is real theft and we will hold state sponsored cyber thieves accountable as we would any other transnational criminal organization that steals our goods and breaks our laws."

*(*Continued On The Following Page)*

"This 21st century burglary has to stop," said David Hickton, U.S. Attorney for the Western District of Pennsylvania. "This prosecution vindicates hard working men and women in Western Pennsylvania and around the world who play by the rules and deserve a fair shot and a level playing field."

Summary of the Indictment

Defendants : Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui, who were officers in Unit 61398 of the Third Department of the Chinese People's Liberation Army (PLA). The indictment alleges that Wang, Sun, and Wen, among others known and unknown to the grand jury, hacked or attempted to hack into U.S. entities named in the indictment, while Huang and Gu supported their conspiracy by, among other things, managing infrastructure (e.g., domain accounts) used for hacking.

Victims : Westinghouse Electric Co. (Westinghouse), U.S. subsidiaries of SolarWorld AG (SolarWorld), United States Steel Corp. (U.S. Steel), Allegheny Technologies Inc. (ATI), the United Steel, Paper and Forestry, Rubber, Manufacturing, Energy, Allied Industrial and Service Workers International Union (USW) and Alcoa Inc.

Time period : 2006-2014.

Crimes : Thirty-one counts as follows (all defendants are charged in all counts).

Count(s)	Charge	Statute	Maximum Penalty
1	Conspiring to commit computer fraud and abuse	18 U.S.C. § 1030(b).	10 years.
2-9	Accessing (or attempting to access) a protected computer without authorization to obtain information for the purpose of commercial advantage and private financial gain.	18 U.S.C. §§ 1030(a)(2)(C), 1030(c)(2)(B)(i)-(iii), and 2.	5 years (each count).
10-23	Transmitting a program, information, code, or command with the intent to cause damage to protected computers.	18 U.S.C. §§ 1030(a)(5)(A), 1030(c)(4)(B), and 2.	10 years (each count).
24-29	Aggravated identity theft.	18 U.S.C. §§ 1028A(a)(1), (b), (c)(4), and 2	2 years (mandatory consecutive).
30	Economic espionage.	18 U.S.C. §§ 1831(a)(2), (a)(4), and 2.	15 years.
31	Trade secret theft.	18 U.S.C. §§ 1832(a)(2), (a)(4), and 2.	10 years.

*(*Continued On The Following Column)*

Summary of Defendants' Conduct Alleged in the Indictment

Defendant	Victim	Criminal Conduct
Sun	Westinghouse	In 2010, while Westinghouse was building four AP1000 power plants in China and negotiating other terms of the construction with a Chinese SOE (SOE-1), including technology transfers, Sun stole confidential and proprietary technical and design specifications for pipes, pipe supports, and pipe routing within the AP1000 plant buildings. Additionally, in 2010 and 2011, while Westinghouse was exploring other business ventures with SOE-1, Sun stole sensitive, non-public, and deliberative e-mails belonging to senior decision-makers responsible for Westinghouse's business relationship with SOE-1.

(*Continued On The Following Page)

Wen	SolarWorld	In 2012, at about the same time the Commerce Department found that Chinese solar product manufacturers had "dumped" products into U.S. markets at prices below fair value, Wen and at least one other, unidentified co-conspirator stole thousands of files including information about SolarWorld's cash flow, manufacturing metrics, production line information, costs, and privileged attorney-client communications relating to ongoing trade litigation, among other things. Such information would have enabled a Chinese competitor to target SolarWorld's business operations aggressively from a variety of angles.
Wang and Sun	U.S. Steel	In 2010, U.S. Steel was participating in trade cases with Chinese steel companies, including one particular state-owned enterprise (SOE-2). Shortly before the scheduled release of a preliminary determination in one such litigation, Sun sent spearphishing e-mails to U.S. Steel employees, some of whom were in a division associated with the litigation. Some of these e-mails resulted in the installation of malware on U.S. Steel computers. Three days later, Wang stole hostnames and descriptions of U.S. Steel computers (including those that controlled physical access to company facilities and mobile device access to company networks). Wang thereafter took steps to identify and exploit vulnerable servers on that list.
Wen	ATI	In 2012, ATI was engaged in a joint venture with SOE-2, competed with SOE-2, and was involved in a trade dispute with SOE-2. In April of that year, Wen gained access to ATI's network and stole network credentials for virtually every ATI employee.

*(*Continued On The Following Column)*

Sun	Alcoa	About three weeks after Alcoa announced a partnership with a Chinese state-owned enterprise (SOE-3) in February 2008, Sun sent a spearphishing e-mail to Alcoa. Thereafter, in or about June 2008, unidentified individuals stole thousands of e-mail messages and attachments from Alcoa's computers, including internal discussions concerning that transaction.
Huang		Huang facilitated hacking activities by registering and managing domain accounts that his co-conspirators used to hack into U.S. entities. Additionally, between 2006 and at least 2009, Unit 61398 assigned Huang to perform programming work for SOE-2, including the creation of a "secret" database designed to hold corporate "intelligence" about the iron and steel industries, including information about American companies.
Gu		Gu managed domain accounts used to facilitate hacking activities against American entities and also tested spearphishing e-mails in furtherance of the conspiracy.

An indictment is merely an accusation and a defendant is presumed innocent unless proven guilty in a court of law.

The FBI conducted the investigation that led to the charges in the indictment. This case is being prosecuted by the U.S. Department of Justice's National Security Division Counterespionage Section and the U.S. Attorney's Office for the Western District of Pennsylvania.

Challenge Air France & Airbus Bizlab

Air France Starttech Factory and Airbus BizLab jointly propose this challenge to start-up.
According to the thematic, new technologies like augmented or virtual reality, robotics, IOT, big data, … might be taken into account in the projects analysis. The aircraft connectivity is also an enabler.

*(*Continued On The Following Page)*

Magnify the customer experience in the air travel:
• Connect with customer senses to generate dream, well-being etc
• Address different typologies of customers
• Address specific needs: families, passenger with reduce mobility, kids, seniors, specific cultural needs

Modify the airline business model. As illustration:
• Create new products and services concepts, new business models and sales tools and modes: collaborative economy, gamification, "billetic"
• Optimize interfaces using new multilingual technologies (gestures or voice control ..)
• Create new loyalty tools or approaches,
• Seek for processes fluidity (from booking to onboard service)
• Reinvent cabin modularity• Optimize interfaces using new multilingual technologies (gestures or voice control ..)
• Create new loyalty tools or approaches,
• Seek for processes fluidity (from booking to onboard service)
• Reinvent cabin modularity
• Optimize resources allocation: aircraft usage, kerosene, network management, simplify processes between actors..

• Reduce emissions and in particular CO2 emissions
• Use of renewable energies
• Waste management and circular economy
• Water consumption optimization

Your applications will be welcome until the 22nd of April at the latest. At the end of a first selection process, the jury will select a batch of 10 projects to participate to a Bootcamp on the 30th & 31st of May where Airbus and AirFrance experts will help to dig deeper your concept.

The Bootcamp will aim to select 4 startups :
• AirFrance to co-develop with 3 oh them : coaching from experts to build experiments
• Airbus BizLab will offer to one project the opportunity to integrate its Season #2 and to benefit from a 6 month acceleration program.

This Bootcamp will take place in Toulouse at the Airbus **BizLab.**

US Navy signs Deal with BAE Systems for Manufacturing FSSR

A deal has been signed between US Navy and BAE Systems under which, a new warning system will be made to deliver high level of coverage and responsiveness. The system is called the Full-Spectrum Staring Receiver (FSSR), which will be used to gather information regarding near-instantaneous battle-space situation, emitter tracking, threat warning, and countermeasure cueing.

The BAE Systems received $11 million funds to develop next-generation electronic warfare (EW) technology from Office of Naval Research (ONR). The technology will quickly detect, locate, and identify sources of radio frequency signals. "The program integrates a complementary array of innovative technologies into a comprehensive capability that addresses a critical need for full spectrum awareness, ensuring the Navy's ships and aircraft are best prepared for future missions," said Steve Hedges, FSSR principal investigator at BAE Systems.
By using FSSR, US Navy ships will constantly keep record of threat emitters over a very broad span of the electromagnetic spectrum. The new technology will integrate a number of electronic warfare technologies that have been advanced by ONR-funded efforts. Not only the Navy, but the entire Department of Defense community will be benefited as talents of researchers from academia, industry, and the government will be brought together for the project.

The organizations to take part in efforts to make FSSR by BAE Systems are the S2 Corporation, University of Colorado Boulder, Montana State University, Purdue University, HRL Laboratories, and the Naval Research Laboratory. The work will start in Nashua, New Hampshire from October 6, 2018. The US Navy is obligating $2.8 million from fiscal 2015 research, development, tests and evaluation funds.

*(*Continued On The Following Column)*

U.S. curbs China's ZTE exports over Iran business allegations

REUTERS
March 8, 2016
A new U.S. export restriction against China's ZTE Corp (000063.SZ) for alleged Iran sanctions violations is likely to disrupt the telecom manufacturer's sprawling global supply chain and could create substantial parts shortages, according to sanctions experts.
Under the measure announced by the Commerce Department on Monday, U.S. manufacturers will be banned from selling components to ZTE, which is a major global supplier of telecom-networking equipment. In addition, foreign manufacturers will be prohibited from selling products containing a significant amount of U.S.-made parts to the Chinese company.
The Commerce Department, confirming the decision that was first reported by Reuters on Saturday, said ZTE planned to use a series of shell companies "to illicitly reexport controlled items to Iran in violation of U.S. export control laws." It said ZTE acted "contrary to the national security or foreign policy interests of the United States."

*(*Continued On The Following Page)*

While ZTE suppliers can apply for an export license to ship any American-made equipment or parts, the Commerce Department said such license applications generally will be denied.
The export restriction, which does not stop ZTE from selling handsets in the United States, is expected to have a global impact.
“It is going to have a large ripple effect. It’s very significant to many companies both in the U.S. and (outside the) U.S.,” said Doug Jacobson, an export attorney at law firm Jacobson Burton Kelley PLLC, who said he has been fielding calls from clients who supply ZTE since Reuters broke news of the impending export restrictions.
For example, a Taiwanese chipmaker that uses American-made components to make processors for ZTE handsets would likely have to cut off those sales. If the Taiwanese supplier only procures components from outside the United States it can continue to sell to ZTE, experts said.
“I am telling all my clients today that anything (for ZTE)not already on board an airplane going to China, you cannot ship it starting tonight. They have to scrub and screen their customers lists – pending orders and future orders – to make sure that any transactions with ZTE are flagged and stopped.”
ZTE, which has annual sales of more than $15 billion and is the only Chinese smartphone maker with a meaningful presence in the U.S. market, can appeal the decision.
ZTE is among the largest companies that the Commerce Department has hit with a near-total export ban, according to public records. In 2014, the department restricted exports to Russian energy companies Lukoil OAO and Gazprom OAO, but those restrictions only stopped American companies from supplying certain types of oil-production projects, such as Arctic offshore and deepwater drilling.

EFFECT ON HANDSET PRODUCTION
ZTE is the No. 4 smartphone vendor in the United States, with a 7 percent market share, behind Apple Inc (AAPL.O), Samsung Electronics Co (005930.KS) and LG Electronics Inc (066570.KS), according to research firm IDC. It sells handset devices to three of the four largest U.S. mobile carriers - AT&T (T.N), T-Mobile US (TMUS.O) and Sprint Corp (S.N).
Although ZTE is not being banned from selling handsets in the United States, the restriction could disrupt handset production if ZTE sources U.S.-made parts to manufacture its handsets, experts said.
AT&T declined to comment, and T-Mobile and Sprint did not respond to requests for comment.
A ZTE website states that several leading U.S. technology companies, including Microsoft (MSFT.O), Intel Corp (INTC.O), IBM (IBM.N) and Honeywell International Inc (HON.N), are "key strategic partners."
Intel and Qualcomm confirmed they were ZTE suppliers, but did not elaborate on specific products sold to the Chinese company or how sanctions would affect their businesses.
Texas Instruments (TXN.O), which has also said it provides processors for the Chinese company, did not immediately respond to a request for comment.
The impact of the new restrictions on these three companies was not immediately clear as most of them produce components both in the United States and overseas.
Microsoft, in an emailed statement, said, "We follow U.S. law and will review new U.S. restrictions."
A spokeswoman for Microsoft said the company had a licensing agreement with ZTE but could not confirm if ZTE purchases other products, such as software.
The other U.S. companies did not respond to requests for comment.

The U.S. decision could even prompt suppliers to halt sales of non-U.S. components that are still allowed, said Kay Georgi, an export attorney at law firm Arent Fox LLP.
"When you get placed on one of these lists nobody wants to do business with you at all," Georgi said.
The United States has long banned the sale of U.S.-made technology products to Iran as part of its sanctions, even as China maintains close diplomatic, economic, trade and energy ties with Tehran. Last year, the United States and major world powers reached a deal with Iran to loosen economic sanctions in exchange for Tehran curbing its nuclear program.
"We hope this sends a strong message to ZTE, to China, and to other Chinese telecommunications companies who present serious national security risks not only by evading export controls, but by purposefully compromising supply chain security," said Representative Adam Schiff of California, the top Democrat on the House of Representatives Intelligence Committee.

*(*Continued On The Following Column)*

Eavesdropping on 3D Printers Allows Reverse Engineering of Sensitive Designs

Nick Lavars
March 3, 2016
A new UCI study has found that 3D printers emit sounds, vibrations and other signals that present opportunities for industrial espionage (Credit: Daniel Anderson/UCI). View gallery (2 images)
3D printers have opened up all kinds of possibilities when it comes to turning digital blueprints into real word objects, but might they also enable new ways to pilfer intellectual property? Amid all that mechanical whirring, these machines emit acoustic signals that give away the motion of the nozzle, new research has found. And by discreetly recording these sounds, scientists say it is possible for sneaky characters to deduce design details and reverse engineer printed objects at a later date.
While the source code for 3D printed designs can be guarded through encryption and regular means, once the machine is swung into action that sensitive information may be compromised, researchers at the University of California Irvine (UCI) have discovered.

*(*Continued On The Following Page)*

Led by Mohammad Al Faruque, director of the Advanced Integrated Cyber-Physical Systems lab, the team found that placing a smartphone alongside the machine as it printed objects layer-by-layer enabled them to capture the acoustic signals. It says that these recordings contain information about the precise movement of the nozzle, and that information can later be used to reverse engineer the item being printed.
Using this technique, Al Faruque and his team were able to reproduce a key-shaped object with almost 90 percent accuracy.

"In many manufacturing plants, people who work on a shift basis don't get monitored for their smartphones, for example," he says. "If process and product information is stolen during the prototyping phases, companies stand to incur large financial losses. There's no way to protect these systems from such an attack today, but possibly there will be in the future."
One of the possible ways engineers could stonewall would-be thieves might be to confuse the acoustic signals through additional white noise, Al Faruque says. His discovery has attracted interest from other researchers at UCI and at various government agencies. The team are preparing to present their findings at the International Conference on Cyber-Physical Systems in Vienna in April.
Source: University of California Irvine

DIA: Russian Software Could Threaten U.S. Industrial Control Systems

THE WASHINGTON FREE BEACON
March 1, 2016
The Defense Intelligence Agency warned this month that Russian government hackers could penetrate U.S. industrial control networks using commercial security software.

The agency stated in a recent notice circulated within the Pentagon that security software being developed by Kaspersky Lab, a Russian-origin company, will create vulnerabilities for U.S. industrial control systems and so-called supervisory control and data acquisition software, or SCADA, systems, if purchased and deployed by American utilities.
A DIA spokesman declined to comment on the report.
Kaspersky Lab, in a statement, denied its security products could be used against U.S. infrastructure.
In a related development, two U.S. military commanders urged Defense Secretary Ash Carter earlier this month to do more to defend critical infrastructure from cyber attacks against industrial control systems.
“We respectfully request your assistance in providing focus and visibility on an emerging threat that we believe will have serious consequences on our ability to execute assigned missions if not addressed – cyber security of [Defense Department] critical infrastructure Industrial Control Systems,” Northern Command’s Adm. William Gortney and Pacific Command’s Adm. Harry Harris stated in a Feb. 11 letter to Carter.

*(*Continued On The Following Column)*

On the potential Russian government exploitation of security software, defense officials familiar with the DIA report said the agency fears U.S. electrical and water utilities, as well as other critical industrial sectors, will purchase and use the Kaspersky security software.
The agency said the software could permit Russian government hackers, considered among the most advanced nation-state cyber spies, to gain access to industrial control software, specifically remote-controlled SCADA programs that run the electrical grid, oil and gas networks, water pipelines and dams, and wastewater systems.
U.S. officials have said hackers from both Russia and China have been detected conducting cyber reconnaissance of industrial control networks in apparent preparation for future cyber attacks during a conflict.
Kaspersky Lab strongly rejected the DIA claims.
“The alleged claims are meritless as Kaspersky Lab’s products and solutions are designed to protect against cybercriminals and malicious threat actors, not enable attacks against any organization or entity,” the statement said.
“We are not developing any offensive techniques and have never helped, or will help, any government in the world in their offensive efforts in cyberspace.”
Kaspersky Lab plans to release what it describes as “a complete security solution” later this year designed to help protect industrial control systems and networks around the world from cyber attacks.

“The systems controlling important operations involving electricity, water and manufacturing have been widely publicized as being extremely vulnerable to cyber threats, and our solution will help manufacturers and critical infrastructure operators, including those in the U.S, to prevent a crippling cyber attack against these sensitive systems that we rely upon every day,” the statement said.
The company said it is “proud to work with governments around the world to protect their infrastructure and networks, and also to collaborate with the authorities of many countries and international law enforcement agencies in fighting cybercrime.”
The statement said Kaspersky Lab “has no political ties to any government.”

Gortney and Harris, the military commanders, stated in their letter that the threat to U.S. industrial control systems is serious and should be included on the Pentagon’s automated cyber “scorecard”—an electronic system being developed to outline key vulnerabilities of defense computer networks to cyber attack.

(*Continued On The Following Page)

"We must establish clear ownership policies at all levels of the department, and invest in detection tools and processes to baseline normal network behavior from abnormal behavior," the four-star admirals said.

Once that is accomplished, "we should be able to track progress for establishing acceptable cyber security for our infrastructure [industrial control systems," they added.
The letter said the Department of Homeland Security had detected a seven-fold increase in cyber attacks between 2010 and 2015 on critical infrastructure. The attacks were carried out against what the Pentagon calls "platform information technology"—critical national security hardware and software, including industrial controls and SCADA.
"Many nefarious cyber payloads, e.g., Shamoon, Shodan, Havex and BlackEnergy, and emerging ones, have the potential to debilitate our installations' mission critical infrastructure," the admirals said.
"As geographic combatant commanders with homeland defense responsibilities and much at stake in this new cyber connected world, we request your support," they added. The letter was first disclosed by FCW.com on Feb. 25.
BlackEnergy is malware that researchers have linked to Russian government hacking. BlackEnergy malware was detected during investigations of recent cyber attacks against Ukraine's electrical grid that were believed to be carried out by Russian hackers.
Shamoon was linked to the 2012 cyber attack against the state-run Saudi Aramco oil company that damaged 30,000 computers and was believed to have been carried out by Iran.
Havex malware has been linked to cyber attacks on industrial control systems, and Shodan is a search engine that is believed to have helped foreign hackers map remote industrial control networks for possible attacks.

Asked about the letter, a Northcom spokeswoman said in a statement that the Pentagon's Industrial Control Systems, or ICS, cyber security "is vital to command preparedness and our ability to execute assigned missions."
"The eight-star letter from Adms. Harris and Gortney demonstrates our combatant commands' commitment to defend against emerging threats against DoD critical infrastructure ICS," said a joint statement from the two commands.
"We recognize the risks associated with attacks on critical infrastructure [industrial control systems] and we are engaging with the secretary of defense to actively combat these risks," the statement added.
Russia was linked to SCADA attacks by Director of National Intelligence James Clapper in congressional testimony last September.
Clapper disclosed that Russian cyber warfare specialists are developing the capability to remotely access industrial control systems used in managing critical infrastructure.

(*Continued On The Following Column)

"Unknown Russian actors successfully compromised the product supply chains of at least three [industrial control system] vendors so that customers downloaded malicious software designed to facilitate exploitation directly from the vendors' websites along with legitimate software updates," Clapper stated in Sept. 10 testimony before the House Permanent Select Committee on Intelligence.
The *Washington Free Beacon* disclosed in 2014 that Russian hackers were suspected of using malware, including BlackEnergy, to map U.S. industrial control systems since 2011.
A former intelligence official said threats to industrial control systems from Kaspersky software has been an "NSA myth" for years.
"Kaspersky wanted to do it and still is developing something but it's never going to be public and they know that," the former official said, adding that NSA has overreacted to the threat.
However, the former official said that industrial control systems remain vulnerable to cyber attacks because the architecture of the systems allow intruders to gain access to multiple devices once inside a network.
"There are some serious vulnerabilities," the former official said, including remote access capabilities. "You have to watch those because in an ICS once you gain access, you have everything, there is no 'root' on the [programmable logic controller], you have it by default."
"The biggest problem is that most of the software is made insecure by default. That's what we have to address."
Securing industrial control networks will require producing more secure hardware and software and increasing the monitoring of current networks, many of which run Windows operating software.
"We need to patch the Windows infrastructure because it's defendable but we shouldn't waste resources patching systems internal to the ICS that aren't remotely accessible because it's very, very costly in an operational environment with very little return on investment," the former official said.
Kaspersky Lab founder Eugene Kaspersky was asked earlier this month what involvement, if any, he and his company have with the Russian government and security services.
"We are working with governments in many nations – in Europe, in Asia, in the Middle East, in Russia," he said in an interview with the Dubai-based GulfBusiness.com.
"We are very good friends with the cyber police and the agencies responsible for cyber security," he said. "But we stay away from the intelligence services and the espionage agencies; we keep our distance from them and from the politicians. We are a security company so we must stay independent and neutral. It is not possible to be linked to any political party, for instance. It would be a conflict of interest.
National Public Radio reported in August that Kaspersky worked for a few years in a Soviet military research institute but left for the private sector in 1991.
Kaspersky has cooperated with Russian security services in seeking out cyber criminals, NPR said. Critics have pointed out that while Kaspersky Lab has exposed malware from Western governments, it has not pursued Russian government hacking efforts with the same vigor.

SINGAPORE MAN EXTRADITED TO UNITED STATES IN CONNECTION WITH PLOT INVOLVING EXPORTS TO IRAN OF U.S. COMPONENTS LATER FOUND IN BOMBS IN IRAQ

WASHINGTON – Lim Yong Nam, aka Steven Lim, 42, a citizen of Singapore, has been extradited from Indonesia to stand trial in the District of Columbia on charges of taking part in a conspiracy that allegedly caused thousands of radio frequency modules to be illegally exported from the United States to Iran, at least 16 of which were later found in unexploded improvised explosive devices (IEDs) in Iraq.

The extradition was announced by Assistant Attorney General for National Security John P. Carlin, U.S. Attorney Channing D. Phillips of the District of Columbia, Director Sarah Saldaña of the Department of Homeland Security's U.S. Immigration and Customs Enforcement (ICE), Executive Assistant Director Michael Steinbach of the FBI's National Security Branch, and Under Secretary of Commerce Eric L. Hirschhorn.

Lim had been detained in Indonesia since October 2014 in connection with a U.S. request for extradition. He is to make his initial appearance at 1:30 p.m. today in federal court in the District of Columbia, where he was indicted on June 23, 2010. Lim faces one count of conspiracy to defraud the United States, one count of smuggling, one count of illegal export of goods from the United States to Iran, one count of making false statements to the United States government and one count of making false statements to law enforcement.

"The indictment alleges that Lim conspired to defraud the United States and defeat our export controls by sending U.S.-origin components to Iran instead of their stated final destination of Singapore," said Assistant Attorney General Carlin. "Several of those components ultimately ended up in unexploded improvised devices in Iraq. This case, including the successful extradition of Lim, demonstrates our efforts to vigorously pursue and bring to justice those who threaten our national security."
"Thanks to the efforts of law enforcement here and abroad, Lim Yong Nam will now appear in an American courtroom to face charges involving the illegal export of sensitive technology," said U.S. Attorney Phillips. "As alleged in the indictment, the parts at issue here wound up in Iran and then on the battlefields in Iraq. The extradition of this defendant demonstrates our commitment to aggressively investigating and prosecuting those who violate our export controls and threaten our nation's security."

"Improvised explosive devices (IEDs) have injured or killed thousands of military service members overseas. The U.S.-made products Mr. Lim is accused of illegally exporting were

*(*Continued On The Following Column)*

found in several of the devices used against America's warfighters," said ICE Director Saldaña. "After a long investigative process, Mr. Lim is back on U.S. soil to answer for his actions."

"The illegal export of restricted U.S. technology is extremely harmful to our national security," said Executive Assistant Director Steinbach of the FBI's National Security Branch. "In this case the technology had lethal applications and was used in improvised explosive devices in Iraq which endangered U.S. and coalition forces. This investigation was a coordinated effort by many agency partners and shows our determination to identify and bring to justice all those who steal sensitive technology."

"The extradition of Lim Yong Nam highlights the significant cooperation of U.S. law enforcement agencies and our international partners to pursue and prosecute those who pose a threat to our national security, especially to U.S. service members overseas," said Under Secretary Hirschhorn. "I commend the outstanding efforts of all of the agencies involved in the case."

According to a superseding indictment that was returned against Lim and other defendants on Sept. 15, 2010, IEDs were the major source of American combat casualties in Iraq. The conspiracy alleged in the indictment involved radio frequency modules that have several commercial applications, including in wireless local area networks connecting printers and computers in office settings. These modules include encryption capabilities and have a range allowing them to transmit data wirelessly as far as 40 miles when configured with a high-gain antenna. These same modules also have potentially lethal applications. Notably, during 2008 and 2009, coalition forces in Iraq recovered numerous modules made by the Minnesota firm that had been utilized as part of the remote detonation system for IEDs.

The superseding indictment alleges that between June 2007 and February 2008, Lim and others caused 6,000 modules to be purchased and illegally exported from the Minnesota-based company through Singapore, and later to Iran, in five shipments, knowing that the export of U.S.-origin goods to Iran was a violation of U.S. law. In each transaction, Lim and others made misrepresentations and false statements to the Minnesota firm that Singapore was the final destination of the goods. Similarly, according to the superseding indictment, Lim and others caused false documents to be filed with the U.S. government, in which they claimed that Singapore was the ultimate destination of the modules. At the time of these activities, Lim and others were allegedly communicating with one another about U.S. laws prohibiting the export of U.S.-origin goods to Iran. However, in November 2009, Lim told U.S. authorities that he had never participated in illicit exports to Iran, the superseding indictment alleges.

(*Continued On The Following Page)

The superseding indictment alleges that several of the 6,000 modules the defendants routed from Minnesota to Iran were later discovered by coalition forces in Iraq, where the modules were being used as part of IED remote detonation systems. In May 2008, December 2008, April 2009 and July 2010, coalition forces found at least 16 of these modules in unexploded IEDs recovered in Iraq, the indictment alleges.

An indictment is merely a formal charge that a defendant has committed a violation of criminal law and is not evidence of guilt. Every defendant is presumed innocent until, and unless, proven guilty. This investigation was jointly conducted by ICE agents in Boston and Los Angeles; FBI agents in Minneapolis, and Department of Commerce's Bureau of Industry and Security agents in Chicago and Boston. Substantial assistance was provided by the U.S. Department of Defense, U.S. Customs and Border Protection, the State Department's Directorate of Defense Trade Controls, the Treasury Department's Office of Foreign Assets Control and the Justice Department's Office of International Affairs, particularly the Justice Department Attaché in the Philippines, as well as the FBI and ICE Attachés in Jakarta and Singapore.

U.S. law enforcement authorities thanked the governments of Singapore and Indonesia for the substantial assistance that was provided in the investigation of this matter.
The prosecution is being handled by Assistant U.S. Attorney Ari Redbord of the District of Columbia and Trial Attorney Julie Edelstein of the National Security Division's Counterintelligence and Export Control Section.

Announcing Full Scholarship for Spouses of Wounded Veterans

Northeastern University's Center for the Advancement of Veterans and Servicemembers is pleased and honored to announce a unique scholarship opportunity for the spouses of wounded veterans/servicemembers in Massachusetts. I ask for your assistance in sharing this throughout your network.

Through the generosity of the Ruby Linn Foundation, Northeastern is prepared to award **Two Full Scholarships** covering the cost of any program in our Lowell Institute School degree portfolio. This includes the following degrees:

- BS Biological Science
- BS Biotechnology
- BS Environmental Studies
- BS Health Management
- BS Health Management – Fast-Track
- BS Information Technology
- BS Information Technology – Fast-Track

*(*Continued On The Following Column)*

- BS Psychology
- BS Technical Communication
- BSET Computer Engineering Technology
- BSET Electrical Engineering Technology
- BSET Mechanical Engineering Technology
- BSHS Health Science
- Post-Baccalaureate Pre-Medical

Spouses of wounded veterans are asked to complete a scholarship essay (described below). Proof of spouse's military service (DD214, VA Certificate of Eligibility, military/veteran ID card, etc.) and proof of spousal relationship (marriage certificate, dependent ID card, etc.) are required. Optional letters of recommendation will be strongly considered. Essays and supporting documents should be sent in a single email to NUvets@neu.edu for consideration. Receipt of the scholarship is contingent upon the awardee's admission into one of the LIS degree programs above. Deadline for submission is May 15, 2016. Degree programs would begin in the fall 2016 semester.

Scholarship Essay

Please respond to the following prompt:

The Lowell Institute School is a unique community of enterprising students focused on completing their studies, mastering new knowledge and skills, and graduating prepared to pursue promising careers in industries at the core of our innovation economy. While students come to the Lowell Institute School from diverse backgrounds and experiences, they share a common goal of achieving their full career potential and building a better future for themselves and their families.

Please describe how receiving this scholarship from the Ruby Linn Foundation and completing your bachelor's degree within the Lowell Institute School will support your educational goals, as well as your current or future career aspirations. Please do so in a minimum of two pages, double spaced (approximately 500 words).