EIB World Trade Headlines

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

January 1, 2017 - Volume 10, Issue 1

CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics

WASHINGTON—U.S. Customs and Border Protection released today an update to the agency's Directive governing Border Searches of Electronic Devices. This Directive, which supersedes the previous directive released in August 2009, enhances the transparency, accountability and oversight of electronic device border searches performed by CBP.

"In this digital age, border searches of electronic devices are essential to enforcing the law at the U.S. border and to protecting the American people," said Deputy Executive Assistant Commissioner, Office of Field Operations, John Wagner. "CBP is committed to preserving the civil rights and civil liberties of those we encounter, including the small number of travelers whose devices are searched, which is why the updated Directive includes provisions above and beyond prevailing constitutional and legal requirements. CBP's authority for the border search of electronic devices is and will continue to be exercised judiciously, responsibly, and consistent with the public trust."

*(*Continued On The Following Page)*

NEWSLETTER NOTES

Noting the evolution of the operating environment since the 2009 directive was issued, advances in technology and continuing developments, along with the requirements of the Trade Facilitation and Trade Enforcement Act of 2015, codified at 6 U.S.C. § 211(k), Acting Commissioner Kevin McAleenan directed the review and update of the Directive.

In FY17, CBP conducted 30,200 border searches, both inbound and outbound, of electronic devices. Approximately 0.007 percent of arriving international travelers processed by CBP officers (more than 397 million) had their electronic devices searched (more than 29,200). In FY16, 0.005 percent of arriving international travelers (more than 390 million) had their electronic devices searched (more than 18,400).

The need for border searches of electronic devices is driven by CBP's mission to protect the American people and enforce the nation's laws in this digital age. As the world of information technology evolves, techniques used by CBP and other law enforcement agencies must also evolve to identify, investigate, and prosecute individuals who use new technologies to commit crimes. CBP border searches of electronic devices have resulted in evidence helpful in combating terrorist activity, child pornography, violations of export controls, intellectual property rights violations, and visa fraud.

CBP is responsible for securing our nation's borders, to include, among other things, ensuring the interdiction of persons and goods illegally entering or exiting the United States; enforcing the customs and trade laws of the United States; detecting, responding to, and interdicting terrorists, drug smugglers and traffickers, human smugglers and traffickers, and other persons who may undermine the security of the United States; and safeguarding the border of the United States to protect against the entry of dangerous goods. In furtherance of these critical responsibilities, CBP exercises its border search authority judiciously and in a manner that preserves the public trust.

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.

Last published: January 9, 2

Below is a month-to-month comparison for FY16 and FY17.

*(*Continued On The Following Column)*

International Travelers (Inbound and Outbound) Processed with Electronic Device Search

	FY 2016	FY 2017
October	857	2,561
November	1,208	2,379
December	1,486	2,404
January	1,656	2,760
February	1,484	2,303
March	1,709	2,605
April	1,578	2,275
May	1,626	2,537
June	1,487	2,304
July	1,656	2,359
August	2,385	3,133
September	1,919	2,580
Total	**19,051**	**30,200**

Facial Scans at U.S. Airports Violate Americans' Privacy, Report Says

WASHINGTON — A new report concludes that a Department of Homeland Security pilot program improperly gathers data on Americans when it requires passengers embarking on foreign flights to undergo facial recognition scans to ensure they haven't overstayed visas.

The report, released on Thursday by researchers at the Center on Privacy and Technology at Georgetown University's law school, called the system an invasive surveillance tool that the department had installed at nearly a dozen airports without going through a required federal rule-making process.

The report's authors examined dozens of Department of Homeland Security documents and raised questions about the accuracy of facial recognition scans. They said the technology had high error rates and were subject to bias, because the scans often fail to properly identify women and African-Americans.

"It's telling that D.H.S. cannot identify a single benefit actually resulting from airport face scans at the departure gate," said Harrison Rudolph, an associate at the center and an author of the report.

"D.H.S. doesn't need a face-scanning system to catch travelers without a photo on file," he added. "It's alarming that D.H.S. still hasn't supplied evidence for the necessity of this $1 billion program."Homeland security officials said the program was necessary and fulfilled a decades-old congressional requirement to prevent foreign visitors from overstaying their visas.

John Wagner, deputy executive assistant commissioner for field operations at Customs and Border Protection, said American travelers could ask to be inspected other than by a facial scan before boarding flights. He said that at least 90 percent of the scans had correctly identified faces, and that the agency had not encountered gender or racial bias problems with the technology.

"Our job is to meet the mandate and build the system," Mr. Wagner said. "The fact that Congress felt strong enough to set aside a billion dollars to get it done speaks to its need."

The report comes as homeland security officials begin to roll out a biometric exit system that uses facial recognition scanning in 2018 at all American airports with international flights.

*(*Continued On The Following Column)*

Customs and Border Protection has been testing a number of biometric programs, teaming up with several airlines in Atlanta, Boston, New York and Washington. It will cost up to $1 billion, raised from certain visa fee surcharges over the next decade.

Customs officials say the biometric system has also produced some successes in the pilot testing and has helped catch people who have entered the United States illegally and are traveling on fake documents. They noted that facial scans and fingerprints — unlike travel documents — cannot be forged or altered and therefore give agents an additional tool to ensure border security.

But Senators Edward J. Markey, Democrat of Massachusetts, and Mike Lee, Republican of Utah, expressed concerns about the report's findings. In a letter to Kirstjen Nielsen, the homeland security secretary, the senators urged the department to delay rolling out the facial scans until it addressed the privacy and legal concerns identified in the report.

In 1996, Congress ordered the federal government to develop a tracking system for people who overstayed their entry visas. After the Sept. 11, 2001, attacks, an entry- and exit-tracking system was seen as a vital national security and counterterrorism tool. The 9/11 Commission recommended in 2004 that the newly-developed Department of Homeland Security complete a system "as soon as possible." Congress has since passed seven separate laws requiring biometric entry-exit screening.

But for years, officials have struggled to put a biometric exit system in place because the technology to collect the data was slow to take hold. And many American airports, unlike those in Europe and elsewhere, do not have designated international terminals, leaving little space for additional scanning equipment.

The biometric system being tested by the Department of Homeland Security can be used either with a small portable hand-held device or a kiosk equipped with a camera.

The system snaps a picture of a passenger leaving the United States and checks the person's face with a gallery of photos maintained by Customs and Border Protection or the State Department. It also checks the person's citizenship or immigration status against various homeland security and intelligence databases. For American citizens, the facial scans are checked against photos from State Department databases.

(*Continued On The Following Page)

While the system does take facial scans of American citizens, officials at Customs and Border Protection said, the information is used in a very limited way. The officials said scans of Americans were only used to verify identity — not to collect new information.

Mr. Wagner said Customs and Border Protection would comply with a federal process to address concerns before the face scanning system was used at all international terminals at American airports.

Laura Moy, who helped write the report, said the Customs and Border Protection assurances were not sufficient.

“They can change their minds on how they use this data at any time, because they haven’t put policies in place that govern how it’s supposed to be used,” said Ms. Moy, the deputy director of the Privacy and Technology Center at Georgetown Law. “This invasive system needs more transparency, and homeland security officials need to address the legal and privacy concerns about this system, before they move forward.”

An executive order signed in January by President Trump calls for homeland security officials to speed up the deployment of the biometric system to airports.

The United States continues to trail other nations in adopting the technology to collect biometric information. Nearly three dozen countries, including in Europe, Asia and Africa, collect fingerprints, iris scans, and photographs that can be used for facial recognition of people leaving their countries.

President Delegates Magnitsky ACT export controls to Secretary of the Treasury, in consultation with the Secretary of State

Dec 21, 2017

DEPARTMENT OF THE TREASURY
Office of Foreign Assets Control

31 CFR Part 584

Magnitsky Act Sanctions Regulations

ACTION: Final rule.

*(*Continued On The Following Column)*

FOR FURTHER INFORMATION CONTACT: The Department of the Treasury’s Office of Foreign Assets Control: Assistant Director for Licensing, tel.: 202-622-2480, Assistant Director for Regulatory Affairs, tel.: 202-622-4855, Assistant Director for Sanctions Compliance & Evaluation, tel.: 202-622-2490; or the Department of the Treasury’s Office of the Chief Counsel (Foreign Assets Control), Office of the General Counsel, tel.: 202-622-2410.

Background

On December 14, 2012, the President signed into law the Sergei Magnitsky Rule of Law Accountability Act of 2012, Public Law 112-208, title IV, 126 Stat. 1502 (2012) (the “Act”). The Act provides authority for the identification of and imposition of sanctions on certain persons related to the detention, abuse, and death of Sergei Magnitsky or responsible for certain gross violations of human rights in the Russian Federation.

Section 404(a) of the Act requires the President to submit to certain congressional committees a list of each person the President has determined meets certain criteria set forth in

the Act. Section 406 of the Act requires the President, with certain exceptions, to exercise powers granted by the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) to the extent necessary to freeze, and prohibit all transactions in, all property and interests in property that are in the United States, that come within the United States, or that are or come within the possession or control of any United States person of persons on the list required by Section 404(a) of the Act.

Section 404(a) of the Act sets out criteria for inclusion on the list, namely, certain persons who the President determines:

(1) Are responsible for the detention, abuse, or death of Sergei Magnitsky, participated in efforts to conceal the legal liability for the detention, abuse, or death of Sergei Magnitsky, financially benefitted from the detention, abuse, or death of Sergei Magnitsky, or were involved in the criminal conspiracy uncovered by Sergei Magnitsky;

(2) Are responsible for extrajudicial killings, torture, or other gross violations of internationally recognized human rights committed against individuals seeking: to expose illegal activity carried out by officials of the Government of the Russian Federation; or to obtain, exercise, defend, or promote internationally recognized human rights and freedoms, such as the freedoms of religion, expression, association, and assembly, and the rights to a fair trial and democratic elections, in Russia; or

*(*Continued On The Following Page)*

(3) Acted as agents of or on behalf of a person in a matter relating to an activity described in paragraph (1) or (2).

Pursuant to Presidential Memorandum of April 5, 2013: Delegation of Functions Under Section 404 and 406 of Public Law 112-208 (78 F.R. 22761, April 16, 2013), the President delegated certain functions and authorities, including the functions and authorities set forth in section 404(a) of the Act, with respect to the determinations provided for therein, and section 406(a)(1) of the Act, with respect to the freezing, and prohibiting all transactions in, property, to the Secretary of the Treasury, in consultation with the Secretary of State.

Apple, Amazon Said in Talks to Set Up in Saudi Arabia

Apple and Amazon are in licensing discussions with Riyadh on investing in Saudi Arabia, two sources told Reuters, part of Crown Prince Mohammed bin Salman's push to give the conservative kingdom a high-tech look.

A third source confirmed that Apple was in talks with SAGIA, Saudi Arabia's foreign investment authority.

Both companies already sell products in Saudi Arabia via third parties but they and other global tech giants have yet to establish a direct presence.

Amazon's discussions are being led by cloud computing division Amazon Web Services (AWS), which would introduce stiff competition in a market currently dominated by smaller local providers like STC and Mobily.

Riyadh has been easing regulatory impediments for the past two years, including limits on foreign ownership which had long kept investors away, since falling crude prices highlighted the need to diversify its oil-dependent economy.

Luring Apple and Amazon would further Prince Mohammed's reform plans and raise the companies' profile in a young and relatively affluent market, which already boasts some of the highest internet and smartphone use in the world.

About 70 percent of the Saudi population is under 30 and frequently glued to social media.

A licensing agreement for Apple stores with SAGIA is expected by February, with an initial retail store targeted for 2019, said two sources familiar with the discussions.

*(*Continued On The Following Column)*

Amazon's talks are in earlier stages and no specific date has been set for investment plans, they said.

Apple already holds second place in the Saudi mobile phone market behind Samsung, according to market researcher Euromonitor.

Amazon acquired Dubai-based online retailer Souq.com earlier in 2017, opening access for Amazon retail goods to be sold in the kingdom.

Both companies declined to comment, while SAGIA was not immediately available to answer questions about the discussions.

LENGTHY COURTSHIP

While Saudi reform plans call for luring foreign investment broadly across sectors, officials have courted Silicon Valley players especially strongly over the past two years to complement their high-tech ambitions.

Prince Mohammed is an avowed technophile and has styled himself a disrupter in the model of Steve Jobs, Mark Zuckerberg and Bill Gates.

During an official visit to the United States last year he met executives at Facebook, Microsoft and Uber, in which the sovereign wealth fund he chairs later took a $3.5 billion stake.

Since then, he has also set up a $45 billion technology investment fund with Japan's SoftBank and announced plans to create a futuristic $500 billion mega-city with more robots than humans.

Apple and Amazon have both been on a Saudi priority list of foreign firms which officials hope to attract to further their reforms, one of the sources said.

"Many tech multinationals now in Saudi Arabia are either vendors to the Saudi government or, in the case of Uber, have benefited from a sizable Saudi investment," said Sam Blatteis, who heads Dubai-based tech advisory MENA Catalysts Inc.

"Amazon entering the Saudi market would be a step-change."

For Amazon, the move underscores how AWS is looking to take an early lead in selling data storage and computing services to customers in the Middle East.

AWS, the world's biggest cloud business by revenue, has embarked on a slower global expansion than No.2 Microsoft, which now offers cloud services in twice as many regions.

(*Continued On The Following Page)

However, Microsoft has yet to announce plans for data centers in the Middle East, with three regions in India serving as its closest operations.

AWS said in September it would set up data centers for the region in neighboring Bahrain.

The kingdom has been streamlining its many overlapping laws which could apply to cloud computing for more than a year in order to attract service providers.

If completed, a cloud deal could pave the way for an expansion of Amazon retail warehouses in Saudi Arabia.

Although Amazon operates its diverse business units separately, it has rolled out its near-full suite of retail, third-party marketplace and cloud services in countries of operation over time.

Apple stores would raise the profile of the company's products and offer repairs and community events in line with its strategy to brand its stores as "town squares."

Cybersecurity Dangers Will Spike in 2018

While the cyber danger increases for industrial networks, holistic security is gaining ground.

by: Rob SpiegelAutomation & Motion ControlCyber SecurityDecember 22, 2017

In 2018, we're likely to see hackers build on the success of brutal attacks such as WannaCry ransomware. On the defense side, companies are beginning to take a holistic approach to security. With corporate leadership increasingly backing efforts to bolster security protections, companies are committing to security as continuous improvement.

In many cases, the roadrunner is outsmarting the cyber-attacking coyote. Some cybersecurity experts note that you don't necessarily have to outrun the coyote – you just have to outrun the roadrunner next to you, since cyber attackers seek the least-protected companies. In all, we'll watch 2018 play out with attacks getting more creative while companies – with the financial blessing from the c-suite – will become more adept at protection.

*(*Continued On The Following Column)*

The Attackers Are Getting Smarter

The 2017 ransomware attacks set the scene for 2018 protections. Yet it's the next wave beyond ransomware the worries cybersecurity experts. "The impact of WannaCry was pivotal. Attackers became empowered by WannaCry, since it resulted in at least a million dollars in public loss. I fear we're going to see a pivot from ransom to more IoT and IT attacks," Kevin Tambascio, manager of the Cybersecurity Office at Rockwell Automation, told Design News. "On the positive side, I'm seeing more empowered security that is better founded. There are more and more tools to help companies detect anomalous behavior in their organizations."

Tambascio is concerned about a possible shift from PCs to network attacks. "Even after the ransomware attacks, the landscape continues to change. Attackers are pivoting from PCs to newer platforms where they feel they'll have better success. In 2018, we'll see new generations of attacks that we won't be able to defend," said Tambascio. "There is not a single technology or network design that will offer all the protection an organization needs. We need security depth and a risk-based approach."

Where Are the Weaknesses?

It's in the nature of hackers to be step ahead of cyber protection. Companies don't always know where they're vulnerable until the attack hits. "The implementation of security in many IoT products will not match the pace of advancement of cyberattacks," Alan Grau, president and co-founder at Icon Labstold Design News. "Many companies are focused on security at the cloud and on secure communication. There is far less emphasis on security at the device level and ensuring that IoT devices are protected from attack."

While companies beef up their cloud, network, and device security, there is one weakness that can't be defended without ongoing personnel education. "You have to understand the risk that is present. We're talking about firewalls, antivirus, but in the background, you have people, and they're still a weakness in security," said Tambascio. "That means educating your people. People have to evolve."

While people in the organization may be the weakest link, many companies are slow to identify this problem and commit to an ongoing education strategy. "In most cases, the biggest problem is lack of education and understanding around cybersecurity," said Grau. "While some companies have dedicated cybersecurity staff, many don't. They have bright, talented engineers but lack the depth of understanding of cybersecurity."

*(*Continued On The Following Page)*

Has IT Won the Battle for Network Ownership?

For a couple decades, there has been conflict between the IT department who wants all patches updated right now, and the operational tech team (OT) who live and die by uptime. "The challenge is the request for high availability. On the IT side the most important thing is the integrity of the network. So, that means patch management," Josh Kass, product manager of networks at Rockwell Automation, told Design News. "In the industrial space, it's very difficult for the OT people to take a system down to do a patch. They're developing the process internally to do the patch."

For many years, the OT team won the argument – the patch can wait; we need uptime. But cyber threats have tipped the scale in favor of the IT department's warnings about the importance of patches. "The days of not doing a patch because of up time are coming to an end," said Kass. "The organization says we're going to do patches every 30 or 90 days depending on acceptable downtime, but there has to be more patch management."

2018 Will See the Holistic Approach to Cybersecurity

One of the changes we're likely to see in 2018 is the shift to a broader approach to cybersecurity. Protection will become an assortment of defense efforts inside and outside the network. "A few forward-looking companies are beginning to address security in a holistic fashion. These companies are developing products that include strong built-in security, and they are also addressing security at all levels – cloud, network and device," said Grau. "Many companies, however, are deferring security until a later release or they are enabling a few, minimal security features provided by the hardware or OS. These companies are not necessarily insuring that all main attack vectors are being protected."

The holistic solution will take security down to the device level. "I think advances is the underlying security technology will continue to provide strong protections," said Grau. "Examples include new hardware-based security solutions and secure MCUs for IoT devices."

One of the ongoing dangers comes from hackers who can build on previous successful attacks to create new attacks. One odd way to avoid an attack is to create protection that is simply better than the next company's protection. While this might ward off the net attack, it's a weak approach to security.

"Too often, vulnerabilities that have been known for years are still present in industrial devices. Attackers are able to recycle old attacks with success against these targets," said Grau. "Hackers often target the weakest devices they find.

*(*Continued On The Following Column)*

As a result, companies that have security that is weak but 'not as bad as the other guy' often feel a false sense of security. While many hackers simply target the weakest devices they can find, there is a growing threat from more sophisticated attacks. Companies need to be far more proactive, building security into IoT devices and taking a holistic approach to security."

DDTC Leadership Change: (12.26.17)

Deputy Assistant Secretary Brian Nilsson is retiring after a distinguished career of 31 years. Effective December 23, 2017, Mr. Mike Miller will temporarily assume the duties of Acting Deputy Assistant Secretary for Defense Trade Controls. Mr. Miller, a career member of the Senior Executive Service, is currently the Director for Regional Security and Arms Transfers (RSAT) within the Bureau of Political-Military Affairs and is already well known in the defense trade sector.

As a reminder, the following DDTC Acting positions are still effective:

Anthony Dearth, Acting Chief of Staff, Directorate of Defense Trade Controls Front Office.

Sarah Heidema, Acting Director of Defense Trade Controls Policy.

Terry Davis, Acting Director of Defense Trade Controls Licensing.

The Director of Defense Trade Controls Compliance position is vacant. As announced December 10, 2017, the leadership responsibilities are being shared by the team chiefs during the transition period until a new Director is identified.

Germany's Export Machine Draws Both Envy And Ire

This is the third and final report in John Ydstie's series on Germany's manufacturing strength.

You've probably never heard of Beko Technologies. Headquartered in Neuss, Germany, it makes filters and other products for compressed air systems, which are used in manufacturing, food processing and countless other applications. Beko may not be well known outside Neuss, but it's an excellent example of what makes Germany a manufacturing and export powerhouse.

And that strength has captured the attention of the Trump administration. Year after year, Germany runs huge trade surpluses. The U.S. hasn't seen a trade surplus in decades. President Trump has accused the Germans of cheating, without offering much in the way of specifics.

A look at Beko helps explain why Germany is such an exporting juggernaut.

The company's shipping area is a busy place. Boxes filled with filters, condensers or monitoring devices for compressed air systems are headed to workshops and factories all over the world.

Rainer Stutzel, who works in Beko's marketing department, says compressed air is used everywhere from gas stations and paint shops to hospitals. In 1982, the company's founder developed a condensate drain that removes corrosive moisture from compressed air systems. Beko later developed filters and other products that eliminate impurities from compressed air.

"If you leave the condensate inside a compressed air system, and the compressed air goes to a paint job place, like painting cars with spray guns, not only would the paint come out of the spray gun, but lots of drops of air and oil and water and dirt and your car would look like hell," Stutzel explains.

That's why the world wants Beko's products. Stutzel says about half of what the company manufactures ends up outside Germany, through marketing subsidiaries in Asia and North America.

*(*Continued On The Following Column)*

While the world knows all about the export prowess of German industrial giants like Daimler-Benz and Siemens, thousands of small and mid-sized companies like Beko Technologies are also big exporters. They helped push the German surplus in the export of goods to $280 billion in 2016. Meanwhile, the U.S. had a deficit of $750 billion.

Martin Baily, an economist at the Brookings Institution, says Germany's strength is partly the result of a strategy following World War II to rebuild its economy by focusing on manufacturing and exporting. Baily also says German firms are very motivated to export.

"Partly because it is a smaller economy, so their companies are much more oriented towards exporting, whereas our companies are much more oriented towards selling in the domestic market," Baily says.

The big domestic market in the U.S. is an advantage in many ways, says Baily.
"But from a trade point of view, it means that most companies are like, 'Oh yeah, exports. Why would we export?' "

German exports also have benefited from China's rapid industrialization. German companies provided many of the high-quality machines that Chinese factories needed.

So in part, German companies have simply out-competed other manufacturers.

What about President's Trump's claim that Germany is cheating on trade?

"It's not cheating," says Jeromin Zettelmeyer, a former economic official in the German government and now a fellow at the Peterson Institute for International Economics in Washington.

Germany does have an advantage, he says, but "the only sense in which I think Germany could be accused of 'cheating' is by being a member of the [eurozone]. There is no question that if Germany were to exit the [eurozone] today, this would lead to a pretty substantial appreciation of the German currency."

The euro has been Germany's currency since 1999. But if Germany still had the deutsche mark, its products would almost certainly be more expensive and less competitive in global markets. That's because the deutsche mark would reflect the real strength of the German economy. The euro doesn't. It reflects the less robust economy of the whole euro area and therefore German products, priced in euros, are less expensive and more competitive.

*(*Continued On The Following Page)*

But Germany doesn't control the value of euro. Its value is tied to the health of the whole eurozone economy. So the Trump administration's claim that Germany is cheating by holding the value of the euro down is misguided, according to Baily of the Brookings Institution and other economists.

There is another force that supports Germany's big trade surpluses. It saves far more than the U.S. The clearest sign of that is that the German government balances its federal budget or runs surpluses, while the U.S. government runs huge budget deficits. In other words, the U.S. borrows massively, instead of saving like the Germans do, says Baily.

"They are very disciplined on that, so they don't run those deficits," he says. "Their savings is high so they get the conditions right so they can have a trade surplus."

The U.S. has urged Germany to spend more on its infrastructure and other programs, which could draw more imports into Germany and lower its surplus. Baily and Zettelmeyer both agree that could be good for Germany and its trading partners. But many Germans are proud that what they produce is in demand around the world, and they're not inclined to save less or spend more to mollify their critics.

Robust Apprenticeship Program Key To Germany's Manufacturing Might

Manufacturing accounts for nearly a quarter of Germany's economy. In the U.S., it's about half that. A key element of that success is Germany's apprenticeship training program.

Every year, about half a million young Germans enter the workforce through these programs. They provide a steady stream of highly qualified industrial workers that helps Germany maintain a reputation for producing top-quality products.

Henrik Tillmann is among the current crop of young apprentices. The 19-year-old is training at Hebmuller Aerospace to be an industrial clerk, which qualifies him to do a variety of jobs from materials purchasing to marketing. Each week he spends three-and-a-half days at the company's production center, and a day and a half at a government-funded school. Before he can become a clerk, though, Tillmann must first learn how to build the valves Hebmuller sells to aerospace companies.

He will be a better clerk, says his boss, Axel Hebmuller, because he'll know the valves inside out when he describes them for customers.

*(*Continued On The Following Column)*

"I think it's much easier for young people to understand what they're doing, what they're learning, when they get a little practical work with it because then they can see what they learn at school," he says.

Hebmuller, a co-founder of this firm located near Dusseldorf, says small companies like his rely on apprentices. In fact, that's how he started his career: He was an apprentice at the local bank. "This is where I got my economy degrees," Hebmuller says.

He later went to university, too. But Hebmuller says only 3 of the 16 people who work for his company went to university.

"Even in some of the big, big companies in Germany, in the upper management levels you have people who only have an apprentice and don't even have any university degree," he says.

Apprenticeships are one of the foundations of Germany's manufacturing strength, and Felix Rauner, a professor at the University of Bremen, says U.S. presidents have taken notice.

"Every president of the United States [in] the last 30 years, after becoming elected, said, 'Oh, we should implement the apprenticeship system'," says Rauner.

Donald Trump is no exception.

Last June, at the White House, Trump signed an executive order aimed at boosting the number of U.S. apprenticeships by nearly tenfold to 5 million. But, experts doubt the goal will be realized because funding is inadequate.

Rauner, one of the world's leading authorities on apprenticeships and vocational education, says historically, the U.S. approach to vocational education has been ineffective partly because it's often not directly connected to specific jobs at real companies.

Also, says Rauner, U.S. society has stigmatized vocational education, so most American parents see college as the only path to status and a good career for their children. Rauner says there's a troubling trend in that direction in Germany, too. But, in Germany there's still lots of prestige attached when someone, trained through apprenticeship, achieves master status.

"If, for example, someone gets a meister title, it would be published in the local newspaper and there's a huge celebration. It is an important event," Rauner says. "No one in Germany is interested if someone gets a master degree in a university."

(*Continued On The Following Page)

Ludger Deitmer, Rauner's colleague at the University of Bremen, says his son is an example of the benefits of an apprentice system.

"He started as an engineer, but after four semesters he gave it up and said no this is not really what I want," Deitmer says.

His son is now a tradesman who prefers to learn things by doing them and enjoys looking back after a hard days work and seeing what he has accomplished.

Deitmer is international research coordinator at the Institute of Technology and Education at the University of Bremen and has also studied apprenticeships extensively. He suggests the failure of the U.S. to widely provide this kind of training has hurt U.S. manufacturing, something President Trump says he wants to remedy.

"Vocational training should be one of the medicines, the key medicines, in how to make America great again," Deitmer says. "Why not? This is exactly what the country needs."

One barrier to apprenticeships in the U.S. is getting American companies to buy in, because of the cost of training. In Germany, a firm trains the apprentice and pays them a modest wage.

"But in the second year, they're already doing 60 percent of the workload of a fully skilled worker," Deitmer says. "So, there is a return."

Cheap apprentice labor reduces the net training cost to the company to a little over $10,000, Deitmer says. And, the real pay-off for companies, he says, is that after three years they've got a highly-skilled worker.

U.S. firms often complain about a lack of skilled workers, but the U.S. has struggled to create widespread apprentice programs. Felix Rauner says growing a viable American apprenticeship system will be difficult. Partly because the U.S. has historically had a barrier between schools and business, and partly because of the fractured nature of U.S. education, with 50 states in charge.

NEW KIND OF 3D PRINTING..."VOLUMETRIC"

Although additive manufacturing (AM), commonly known as 3D printing, lets engineers, scientists, and hobbyists alike build parts in configurations and designs never before possible, it is still a slow process unsuited to mass production. The layer-based technology can take up to hours or days to build three-dimensional parts, depending on their complexity.

However, researchers at Lawrence Livermore National Laboratory (LLNL), along with collaborators at UC Berkeley, the University of Rochester, and the Massachusetts Institute of Technology, have developed a method they have named volumetric printing that prints parts all at once. It uses laser-generated, hologram-like 3D images flashed into photosensitive resin from three different axes.

Each of the three laser beams define an object's geometry from a different direction (x, y, or z), creating a 3D image suspended in the vat of resin. The laser light is relatively low in intensity, but where the three beams intersect, the intensity is enough to harden the photo-sensitive resin in about 10 sec. Excess resin is drained out of the vat, and researchers are left with a fully formed 3D part.

This approach, the scientists say, results in parts built many times faster than other polymer-based methods, and most (if not all) commercial AM methods used today. Due to its low cost, flexibility, speed, and geometric versatility, the researchers expect the framework to open a major new direction of research in rapid 3D printing.

"This is a demonstration of what the next generation of additive manufacturing may be," says LLNL engineer Chris Spadaccini, head of Livermore Lab's 3D printing effort. "Most 3D printing and additive manufacturing technologies consist of either a one-dimensional or two-dimensional unit operation. This moves fabrication to a fully 3D operation, which has not been done before. The potential impact on throughput could be enormous, and if you can do it well, you can still have a lot of complexity."

With this process, the LLNL team has printed beams, planes, struts at arbitrary angles, lattices, and complex and uniquely curved objects. And although conventional 3D printing has difficulty with spanning structures that might sag without support, volumetric printing has no such constraints or need for supports. Another major advantage is that many curved surfaces can be produced without layering artifacts. This should reduce post-processing and make for smoother parts. Because volumetric printing does not involve layering, mechanical properties are more likely to be homogenous rather than based on the direction the layers were laid down.

*(*Continued On The Following Page)*

The team also hopes the process can be accelerated by using higher-powered light sources. They also hope the process will work on extra-soft materials such as hydrogels to make parts which would otherwise be damaged or destroyed by fluid motion in traditional layer-by-layer printers. Volumetric 3D printing also is the only additive manufacturing technique that works better in zero gravity, expanding the possibility of space-based production.

The technique does have limitations, the researchers say. Because each laser beam propagates through space without changing, there are restrictions on part resolution and on the kinds of geometries that can be formed. Extremely complex structures would require lots of intersecting laser beams, which would limit the process, they explain.

Spadaccini adds that additional polymer chemistry and engineering also would be needed to improve the resin properties and fine-tune them to make better structures. “If you leave the laser on too long, it starts to cure everywhere, so there’s a timing game,” Spadaccini said. “A lot of the science and engineering is figuring out how long you can keep it on and at what intensity, and how that couples with the chemistry.”

Training

Registration is open for BIS export control seminars in Texas, California, Florida, and Oregon. Reserve your space before the programs fill up! Details below.

■ Complying with U.S. Export Controls – 2 Days

January 23-24, 2018
Houston, TX
Registration: $575

■ Technology and Software Controls – 1 Day

January 25, 2018
Houston, TX
Registration: $300

■ Complying with U.S. Export Controls – 2 Days

February 6-7, 2018
San Diego, CA
Registration: $495

*(*Continued On The Following Column)*

■ Complying with U.S. Export Controls – 2 Days

February 21-22, 2018
Miami, FL
Registration: $499

■ Complying with U.S. Export Controls – 2 Days

March 7-8, 2018
Portland, OR
Registration: $355 before February 20, 2018 and $455 after that date

“Complying with U.S. Export Controls” is a two-day program led by BIS's professional counseling staff and provides an in-depth examination of the Export Administration Regulations (EAR). The program will cover the information exporters need to know to comply with U.S. export control requirements under these regulations. We will focus on what items and activities are subject to the EAR; steps to take to determine the export licensing requirements for your item, how to determine your export control classification number (ECCN), when you can export or reexport without applying for a license, export clearance procedures and record keeping requirements, and real life examples in applying this information. Presenters will conduct a number of "hands-on" exercises that will prepare you to apply the regulations to your own company's export activities.

“Technology and Software Controls” is a one-day program that will offer a comprehensive look at how to comply with the U.S. export and reexport controls relating to technology and software. Discussion will focus on the regulatory requirements relating to technology and software, including what is considered an export or reexport of technology or software; the kinds of technology and software subject to the EAR; how to determine the Export Control Classification Number; license exceptions; and the unique application requirements of technology and software. Recommended prerequisite: Essentials of Export Controls or Complying with U.S. Export Controls or equivalent experience.
For additional details about the seminars, please visit the BIS Current Seminar Schedule page at:https://www.bis.doc.gov/index.php/compliance-a-training/current-seminar-schedule

For general information about the BIS Seminar Program contact the Outreach and Educational Services Division at OESDSeminar@bis.doc.gov or (202) 482-6031, (949) 660-0144, or (408) 998-8806.

Settlement Agreement between the U.S. Department of the Treasury's Office of Foreign Assets Control and Richemont North America, Inc. d.b.a. Cartier

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) today announced a $344,800 settlement with Richemont North America, Inc., d.b.a. Cartier ("Richemont"), headquartered in New York, New York, to settle Richemont's potential civil liability for four apparent violations of the Foreign Narcotics Kingpin Sanctions Regulations, 31 C.F.R. Part 598 (FNKSR). Between the approximate dates of October 5, 2010 and April 21, 2011, Richemont appears to have violated § 598.203 of the FNKSR when it exported four shipments of jewelry to Shuen Wai Holding Limited in Hong Kong ("Shuen Wai"), an entity OFAC added to the List of Specially Designated Nationals and Blocked Persons on November 13, 2008. OFAC determined that Richemont did not voluntarily self-disclose the apparent violations to OFAC, and that the apparent violations constitute a non-egregious case.

Web Notice: The Directorate of Defense Trade Controls (DDTC) is currently in the process of modernizing its IT systems. During this time period, we anticipate there may be delays in response times and time to resolve IT related incidents and requests. We apologize for any inconvenience, and appreciate your patience while we work to improve DDTC services. If you need assistance, please contact the DDTC Service Desk at (202) 663-2838, or email at DtradeHelpDesk@state.gov (06.28.16)

"Nothing worth having comes easy."

Publication of Amended Iraq Stabilization and Insurgency Sanctions Regulations

The Department of the Treasury's Office of Foreign Assets Control (OFAC) is amending the Iraq Stabilization and Insurgency Sanctions Regulations, to implement Executive Order 13668 of May 27, 2014 ("Ending Immunities Granted to the Development Fund for Iraq and Certain Other Iraqi Property and Interests in Property Pursuant to Executive Order 13303, as Amended."). The amendments also implement certain technical and conforming changes. This amendment will take effect upon publication in the Federal Register on Wednesday, December 27, 2017.