EIB World Trade Headlines

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

July 1, 2017 - Volume 9, Issue 13

WHAT IS MANUFACTURING DAY?

Manufacturing Day℠ is a celebration of modern manufacturing meant to inspire the next generation of manufacturers. Manufacturing Day occurs on the first Friday in October — this year Manufacturing Day is Oct 6, 2017.

While Manufacturing Day is officially Oct. 6, companies and community organizations should plan their events on the date in October that works best for them. No matter the date, events should be registered on the site and can be marked as public or invitation-only events.

Registered event hosts have access to free event planning and execution resources and toolkits to make planning a Manufacturing Day event easy

*(*Continued On The Following Page)*

NEWSLETTER NOTES

THE MANUFACTURING DAY MISSION

Manufacturing Day addresses common misperceptions about manufacturing by giving manufacturers an opportunity to open their doors and show, in a coordinated effort, what manufacturing is — and what it isn't. By working together during and after MFG DAY, manufacturers will begin to address the skilled labor shortage they face, connect with future generations, take charge of the public image of manufacturing, and ensure the ongoing prosperity of the whole industry.

MFG DAY is designed to amplify the voice of individual manufacturers and coordinate a collective chorus of manufacturers with common concerns and challenges. The rallying point for a growing mass movement, MFG DAY empowers manufacturers to come together to address their collective challenges so they can help their communities and future generations thrive.

WHO'S BEHIND MANUFACTURING DAY?

Created by Founding Partner Fabricators and Manufacturers Association, International in 2012, MFG DAY has enjoyed support from many organizations aligned with its mission of positively changing the public perception of modern manufacturing. Organizations that have played a vital role in working with FMA to successfully grow this national celebration of all things manufacturing include the National Association of Manufacturers (NAM), the Manufacturing Institute (MI), and the National Institute of Standards and Technology's (NIST) Hollings Manufacturing Extension Partnership (MEP).

MFG DAY is now produced annually by the NAM with key contributions and support from the MEP and the MI.

ABOUT THE NAM

The NAM is the preeminent U.S. manufacturers association, as well as the nation's largest industrial trade association, representing small and large manufacturers in every industrial sector and in all 50 states.

The National Association of Manufacturers

733 10th Street NW, Suite 700
Washington, DC 20001
(1-800) 814-8468

manufacturing@nam.org
www.nam.org

The PENSAR from Aerialtronics is Released at Commercial UAV Expo Europe

At Commercial UAV Expo Europe, Aerialtronics released a fully integrated computer vision platform with deep learning capabilities. PENSAR is a stand-alone twin sensor platform that utilizes the GPU-accelerated computing power to enable real-time video processing and immediate augmented insights.

The product is the first to integrate the new and powerful FLIR Boson thermal IR camera into a drone application, and additionally contains a 30x zoom Sony daylight camera. It's designed to change the way operators perform aerial tasks in search and rescue, inspections, documenting assets, surveying, mapping and public privacy.

One of the most revolutionary features of the PENSAR is how it leverages deep learning networks in real-time to detect, recognize, track, classify and annotate certain objects or deviations of interest and conversely, to blur out and mask objects for privacy reasons. Users have access to deep learning methods and machine vision developers can automate dynamic decision-making systems quickly and easily. What's really exciting though is that the way in which someone actually uses this product is totally up to them.

The benefits of a single platform that has a thermal camera along with a daylight camera into a drone will create opportunities for emergency and inspection professionals, but the deep learning methods and machine vision will allow for countless possibilities. One of the most exciting questions professionals who are using drones can ask is, "wouldn't it be great if…", and with the ability to develop custom apps, this product is a perfect example of that potential. It allows users to not only ask this question regarding how they want to be using drones, but to answer it as well.

Full specs of the PENSAR are below…

- FLIR Boson thermal IR view / Radiometric measurements 1/1 (3:2)
- Day Vision with 30x zoom (HD 1920*1080) 1/1 (16:9)
- Side by side view (vision / IR) (HD 1920*1080) 1/2 (16:9)
- Sensor fusion (IR overlay on vision image stream)
- Dual-stream parallel onboard recording
- Image capturing
- AI-powered object detection, tracking & classification
- Real-time masking
- Optical character recognition (OCR)
- GPU-accelerated computing
- Ability to run unlimited computer vision powered algorithms

The Trump administration is preparing to delay the launch of a new startup visa

The Trump administration is preparing to delay the launch of a new startup visa set to go into effect next month, and may ultimately kill it altogether, the San Francisco Chronicle reports, citing an unnamed source.

In January, as his term entered its final days, President Barack Obama signed the International Entrepreneur Rule, which grants a 30-month visa to entrepreneurs who have raised $250,000 in American venture capital or more. The rule is set to take effect July 17

Critics of the new startup visa say Obama unfairly expanded immigration laws, which grant temporary visas for people who come to the country for humanitarian reasons, or provide a "significant public benefit." The Obama administration argued that early-stage startups provide a significant public benefit — something critics of the law aren't as convinced of.

U.S. Citizenship and Immigration Services will only say it's reviewing the rule.

"We cannot speculate on the outcome of the review of the rule," a department spokesman told the Chronicle. "When the review is final, we will make the decision public."

Earlier this week, Republican senators Jerry Moran, Orrin Hatch, Jeff Flake and John McCain wrote a letter to the U.S. Department of Homeland Security in support of the startup visa.

"There is little benefit to losing any ground in attracting entrepreneurs and their investments," the senators wrote, according to a copy of the letter obtained by the Chronicle.

The move comes as Canada and France step up efforts to attract foreign-born entrepreneurs and scientists. Canada's startup visa is open to any entrepreneur who raises $200,000 or more from a Canadian venture capitalist, or at least $75,000 from a Canadian angel investor. The French startup visa asks, among other things, for entrepreneurs to get accepted to one of the country's startup incubators.

Join the conversation: Follow @SVbizjournal on Twitter, "Like" us on Facebookand sign up for our free email newsletters.

ENFORCEMENT INFORMATION FOR June 26, 2017

Information concerning the civil penalties process is discussed in OFAC regulations governing the various sanctions programs and in 31 C.F.R. Part 501. On November 9, 2009, OFAC published as Appendix A to part 501 Economic Sanctions Enforcement Guidelines. See 74 Fed. Reg. 57,593 (Nov. 9, 2009). The Economic Sanctions Enforcement Guidelines, as well as recent final civil penalties and enforcement information, can be found on OFAC's website at http://www.treasury.gov/ofac/enforcement.

ENTITIES – 31 C.F.R. 501.805(d)(1)(i)

American International Group, Inc. Settles Potential Liability for Apparent Violations of Multiple Sanctions Programs: American International Group, Inc. (AIG) of New York, NY, an international insurance and financial services organization incorporated in Delaware and headquartered in New York, has agreed to remit $148,698 to settle its potential civil liability for 555 apparent violations of the following OFAC sanctions programs: the Iranian Transactions and Sanctions Regulations, 31 C.F.R. Part 560 (ITSR); the Weapons of Mass Destruction Proliferators Sanctions Regulations, 31 C.F.R. Part 544 (WMDPSR); the Sudanese Sanctions Regulations, 31 C.F.R. Part 538 (SSR); and the Cuban Assets Control Regulations, 31 C.F.R. Part 515 (CACR), (collectively, the "Apparent Violations").

OFAC has determined that AIG did voluntarily self-disclose the Apparent Violations, and that the Apparent Violations constitute a non-egregious case. The total base penalty amount for the apparent violations was $198,266.

From on or about November 20, 2007, to on or about September 3, 2012, AIG engaged in a total of 555 transactions totaling approximately $396,530 in premiums and claims for the insurance of maritime shipments of various goods and materials destined for, or that transited through, Iran, Sudan, or Cuba, and/or that involved a blocked person. While most of the Apparent Violations occurred under global insurance policies, dozens of apparent violations occurred under single shipment policies. OFAC identified 455 apparent violations totaling $274,463.64 in which AIG extended insurance coverage to parties that were engaging in a voyage, shipment, or transshipment to, from, or through Iran, and/or accepted premium payments or paid claims arising from that insurance coverage, in apparent violation of § 560.204 of ITSR. In addition, OFAC identified 38 apparent violations of § 538.205 of the SSR, all of which pertained to global insurance policies that provided insurance coverage for shipments going to or from Sudan, with premiums received totaling $13,321.44.

*(*Continued On The Following Page)*

Moreover, OFAC identified 33 apparent violations of § 544.201 of the WMDPSR, all of which involved shipments aboard blocked Islamic Republic of Iran Shipping Lines vessels, with premiums received totaling $105,065.94. Finally, OFAC identified 29 apparent violations of § 515.201 of the CACR, all of which pertained to AIG's provision of insurance coverage in connection with shipments to or from Cuba, or its processing of premiums or claims arising from this coverage or that involved a Cuban entity, with premiums received totaling $3,679.

AIG's OFAC compliance program in place at the time of the Apparent Violations included recommendations for when to use exclusion clauses in the policies it issued regarding coverage or claims that implicated U.S. economic sanctions. While a majority of the policies were issued with exclusionary clauses, most were too narrow in their scope and application to be effective. In addition, some of the policies were issued without such clauses. Separately, some insureds, mindful of existing exclusionary clauses in their open cargo or worldwide master policies, sought single shipment policies that had no exclusionary clauses.

The settlement amount reflects OFAC's consideration of the following facts and circumstances, pursuant to the General Factors under OFAC's Economic Sanctions Enforcement Guidelines, 31 C.F.R. Part 501, app. A. The following were considered aggravating factors: AIG engaged in a pattern or practice that spanned multiple years in which it issued and maintained insurance policies and processed claims and premium payments in apparent violation of multiple U.S. sanctions programs; AIG issued policies and insurance certificates, and/or processed claims and other insurance-related transactions, that conferred economic benefit to sanctioned countries or persons and undermined the policy objectives of several U.S. economic sanctions programs; and AIG is a large and commercially sophisticated financial institution.

The following were considered mitigating factors: AIG has not received a penalty notice or Finding of Violation from OFAC in the five years preceding the earliest date of the transactions giving rise to the Apparent Violations; AIG had an OFAC compliance program in place at the time of the Apparent Violations that included, in most instances, the use of sanctions exclusion clauses to try to prevent the company from issuing policies or processing claims that implicated U.S. economic sanctions; AIG took remedial action in response to the apparent violations; and AIG cooperated with OFAC's investigation, including by voluntarily self-disclosing the Apparent Violations, submitting detailed and well-organized information to OFAC, and signing tolling agreements that tolled the statute of limitations.

*(*Continued On The Following Column)*

This enforcement action highlights the important role that properly executed exclusionary clauses and robust compliance controls play in the global insurance industry's efforts to comply with U.S. economic sanctions programs. As outlined in OFAC's Frequently Asked Questions regarding Compliance for the Insurance Industry, the best and most reliable approach for insuring global risks without violating U.S. sanctions law is to insert in global insurance policies an explicit exclusion for risks that would violate U.S. sanctions laws.

For more information regarding OFAC regulations, please visit: http://www.treasury.gov/ofac.

AUTONOMOUS VEHICLES

Design News June 29

We've reached the point where the hype is galloping past the reality. And it's partly because the word "autonomous" is losing its meaning. So for clarity's sake, let's recap: Today's "autonomous" cars have drivers; the 2020 versions will operate in limited domains; and SAE Level 5 (real autonomy) is still a decade or more away.

Most important, though, is this: Autonomous cars, even those driven by governors, will never be foolproof.

7 Simple Ways to Protect Yourself Against Ransomware

The lesson from the May 2017 global ransomware attack is that hundreds of thousands of computers were unprotected.

On May 12, hundreds of thousands of computer owners at home and at work – across 150 countries – woke to the unpleasant reality that their data was being held for ransom. Yikes.

Microsoft had released a patch for the appropriately named cryptoworm – WannaCry – but many didn't install it. And those who were understandably still attached to the oldie-but-goodie Windows XP didn't stand a chance, as Microsoft stopped releasing patches for it in 2014.

Few were surprised that the attack targeted Windows, since that ubiquitous OS is the favorite of most attackers. Windows dominates the market, so the more victims the merrier for the attack community. "Only Windows computers were affected by this attack," Ruby Gonzalez, head of communications at NordVPN, told Design News . "Historically, Windows has been more prone to attack. Apples and Linux as not attacked as often."

(*Continued On The Following Page)

Getting Your Patch Updates Automatically

Most Windows users receive their patches through the IT department at work, or they subscribe to receiving the patches automatically from Microsoft. Restart the computer every few days, and most of us watch the newest patches load. But not everyone, apparently. “The main reason people are vulnerable to ransomware is they don’t update their patches,” said Gonzalez. “If the users – companies or individuals – updated back when the patch came out, this attack probably wouldn’t have happened.”

You may not remember it, but you were asked if you wanted to receive automatic updates from Windows when you opened your new computer. If you took on a used computer, you might have missed this step. “What most security experts recommend is setting up automatic updates, which install as soon as they’re available,” said Gonzalez.

Protecting the Corporate Network

With WannaCry, one bad apple was able to spoil the network. “Research shows that human factors affect malware,” said Gonzalez. “In this case, it was enough for one person on the network to open an email that was infected. Training employees is very important.”

One of the thorny issues for manufacturing and process plants is dealing with production facilities that run three shifts. If you’re operating 24/7, when are you going to restart so the patches take affect? “Most of the updates require restarting. That’s an issue for production facilities and large companies that need to run 24/7,” said Gonzalez. “For them, we recommend they work with a company or hire an expert who can schedule updates that don’t affect operations.”

NordVPN offers seven simple ways to protect yourself against ramsomware:

1. Don’t forget to install latest security updates. Security updates often contain patches for latest vulnerabilities, which hackers are looking to exploit.

2. Don’t open anything suspicious you receive through email. Delete dubious emails from your bank, ISP, or credit card company. Never click on any links or attachments in emails you’re not expecting. Never give your personal details if asked via email.

3. Back up all data. Back up your data in an alternate device and keep it unplugged and stored away. Backing up data regularly is the best way to protect yourself from ransomware because only unique information is valuable.

*(*Continued On The Following Column)*

4. Use a VPN for additional safety. Using a VPN when browsing can protect you against malware that targets online access points. That’s especially relevant when using a public hotspot. However, keep in mind that a VPN cannot protect you from downloading malware. While a VPN encrypts your activity online, you should be careful when downloading and opening certain files or links.

5. Close pop-up windows safely. Ransomware developers often use pop-up windows that warn you of some kind of malware. Don’t click on the window - instead, close it with a keyboard command or by clicking on your task bar

6. Use strong passwords and a password manager. Perhaps the most basic requirement for any online account setup is using strong passwords, and choosing different passwords for different accounts. Weak passwords make it simple for hackers to break into an account. A strong password has a minimum of 12 characters, and includes a strong mix of letters, numbers and characters. It’s not easy to remember strong passwords for each site, so it’s recommended to use a password manager, such as truekey.com, LastPass and 1Password.

7. Use anti-virus programs. Make sure you have installed one of the latest reputable anti-virus programs to make sure you are fully protected.

NEW NASA TECHNOLOGY

3D printing is the most viable solution to the heavy burden of equipment transport and manufacture in deep space. After all it'll be a lot easier to let astronauts build what they need themselves rather than sending it all along with them. In 2015, as part of a project NASA calls the Zero-G Technology Demonstration, a 3D printer on board the ISS manufactured the first the first 3-D printed object in space (a printhead faceplate). The ultimate goal is to create what NASA calls a “machine shop in space” capable of manufacturing all of the tools and parts astronauts may need, without them needing to be shipped from Earth.

While the 3D printer on board ISS uses your typical plastic filament extrusion, NASA's Crusan told the audience at ESC that NASA is actively working to create a multimaterial 3D printing facility (dubbed a “FabLab”) on the ISS that will be capable of printing metals and even circuits.

"NASA is great at planning for component failures and contingencies; however, there’s always the potential for unknown scenarios that you couldn’t possibly think of ahead of time," Ken Cooper, the principal investigator for 3D Printing at NASA's Marshall Space Flight Center, said in a statement. "That’s where a 3D printer in space can pay off. While the first experiment is designed to test the 3D printing process in microgravity, it is the first step in sustaining longer missions beyond low-Earth orbit."

Free Malware-as-a-Service (MaaS) Hits Mac OS

Cybercriminals don't usually target operating systems (OS) other than Windows, so it's interesting when they do. While Mac OS is far less likely to be attacked or infected by malware than Windows, it is not entirely immune from it.

Security firms Fortinet and AlienVault recently identified two Malware-as-a-Service (MaaS) programs targeting the Mac OS X operating system – "MacSpy" and "MacRansom." Both became available on the Dark Web June 9th.

What You Need to Know About the New Malware for Mac

While Malicious Software (Malware) is software with the goal of stealing or scamming data from the user, Malware-as-a-Service (MaaS) uses someone else's malware to launch an attack.

Both MacSpy and MacRansom appear to have been created by the same developer. To get access to either program, the scammer must email the developer directly and request a copy.

The Malware creator(s) claim that they created these programs because of the popularity of Apple products and that there is a lack of "sophisticated malware for Mac users."

Once executed on a target's computer, MacSpy and MacRansom check to see which operating system is being run. If it's a non-Mac environment, it terminates. If it is a Mac environment, the malware initiates as follows:

*(*Continued On The Following Column)*

- The "free version" of MaaS captures a screenshot every 30 seconds, logs every keystroke, acquires photos synced from iPhone to Mac, obtains browser history, among other things. The "paid version" does even more. Basically, it gives the attacker access to the entire computer and any accounts stored on it. Get details here.
- One of the first ransomware-as-a-service (RaaS) programs for the OS X platform, this nasty piece of work holds your Mac hostage. It first creates a launch point in the computer's Library, then runs at every startup until the encryption is triggered at a specified time. Once executed, you'll have to pay to get your files back. However, Fortinet is not convinced the encrypted files can actually be decrypted, again, save by brute force. Get details here.

How to Protect Yourself

Although there is no fool-proof method of eliminating malware, you can minimize the impact and prevent significant data loss by doing the following:

- Back up your computer regularly to an external drive.
- Remove all external drives that are connected to your computer so that they do not become infected.
- DO NOT click, open, or download unknown files from suspicious or untrusted sources.
- Limit physical access to your computer and require a password every time it starts or wakes up.
- Download apps and programs only from Apple's own Mac App Store.

Contact Us

Since 2005, JPMerc has helped small to mid-sized businesses use technology more effectively — so it fuels their productivity and success, instead of getting in the way. Contact us to discuss your company's IT needs.

Apple Security, Cyber Security, MaaS, Mac Security, MacRansom, MacSpy, Malware-as-a-Service, RaaS, Ransomware-as-a-Service

STEVE JOBS DID NOT INVENT THE iPHONE

Brian Merchant

An important lesson in innovation—and teamwork—on the 10th birthday of the most popular product of all time.

The iPhone just turned 10 years old, and if you were anywhere near a magazine, newspaper, or screen—swipeable or otherwise—you probably saw a story or nine celebrating its advent. That story would likely run alongside an image of one man in particular. There he is, Steve Jobs on stage at the Moscone Center in San Francisco. Steve Jobs with an aluminum-backed rectangle in his palm. Steve Jobs handing the iPhone down unto the world.

The narrative is clear: Steve Jobs gave us the iPhone, which, at over 1.2 billion units sold, has become the single best selling product of all time. But that narrative also happens to be rather flawed, even misleading. And that's well worth noting, all these years after the iPhone was set upon its trajectory for world domination—because Steve Jobs did not invent the iPhone.

Rarely is it worth going to the trouble to point out that someone did not invent something. 'Brian Merchant Did Not Invent the Cuisinart' is a headline that is unlikely to generate much interest anywhere, ever, even inside the whirring world of cuisinart aficionados. So why pick on Steve Jobs? Why the iPhone? Because the myth is becoming inextricable from the man. Jobs may have never claimed outright that he alone invented the one device—though he did seem to insist on putting his name first on many of its patents—but history is beginning to conflate the art of invention with CEOship, marketing prowess with innovation.

Think back to those photos of the iPhone. There are few, if any, images of the team(s) of impossibly hard-working designers, engineers, and hardware hackers who deserve the lion's share of the credit for bringing it to life. (And I'm not just talking about Jony Ive, either!) We are being encouraged to believe a version of a myth that has been promulgated for decades, if not centuries: The myth of the sole, or lone, inventor.

At least since Edison—and probably since Newton and beyond—the public has glommed onto narratives of great men with great ideas, overcoming adversity and uncertainty to transform the world with the invention of the light bulb, the telephone, the iPhone. This isn't anyone's fault, and everyone's guilty; our brains just tidily compute such appealing narratives, suffused as they are with moral rectitude and justified outcomes. But in a research paper published in 2012, the renowned patent scholar and Stanford professor

*(*Continued On The Following Column)*

Mark Lemley found thatthe vast, vast majority of inventions were achieved not just by people working in teams, but often simultaneously, by different teams, even sometimes working in different parts of the world. Ideas are truly "in the air" as he says.

We now know, for instance, that Edison most certainly did not invent the lightbulb—he simply perfected it as a consumer product. His team found the ideal bamboo filament that made his bulb's glow much more appealing than the competition. And even then, Edison manned a large lab staffed by brilliant researchers; but who remembers a name besides Edison's when we think of the bulb, going off, signifying the spark of a new idea?

So it is with Steve Jobs and the iPhone. In fact, some of the parallels are almost eerie. There was work being done on smartphone products at least a decade and a half before the iPhone was launched—Frank Canova Jr. built the IBM Simon, which was a large black rectangle with touchscreen buttons, apps, and a web browser. Sound familiar? It should—but it was launched in 1993, and flopped. It was ahead of its time, and the technology wasn't ready.

What Jobs did at Apple with the iPhone was take a smattering of percolating technologies, and drove his team to integrate them in a way never executed so elegantly before. The key word is "team"; the iPhone, in fact, grew out of a series of clandestine meetings, under even Jobs' radar, in the bowels of Apple's 2 Infinite Loop building—where designers, user interface experts, and hardware engineers experimented with a collection of technologies until they'd come up with the set of demos that would form the core of the iPhone experience: Multitouch finger sensors married to custom Apple software that would bring the pixels to dance underneath your fingers.

I had a chance to meet many of these pioneers over the course of reporting my book: Bas Ording, Imran Chaudhri, Greg Christie, Brian Huppi, Josh Strickon—any of those names ring a bell? Probably not—yet they're the forefathers of the iPhone. They prototyped what would become the "one device" long before Steve Jobs even had a whiff of its existence. And then a whole slew of software engineers—Scott Herz, Richard Williamson, Nitin Ganatra, And Grignon and so on, organized by product manager Kim Vorrath—took those experiments and built the world's most stealthy mobile computer around it. And then a crack team of hardware engineers, including David Tupman, Michael Culbert, and—okay, you're getting the point. There's a small city worth of people who contributed to the iPhone, who made it tick, who unfurled its innovations, who designed the most popular software interface of all time, who made it sing on a tiny handheld device. And that is to say nothing of the miners, laborers, and manufacturers who collect and convert the raw materials into tiny components and finished products around the globe.

*(*Continued On The Following Page)*

Steve Jobs made crucial decisions. His business maneuverings—especially absorbing info from the carriers and then winning near-total freedom to build his iPhone any way he liked, and winning favorable contract terms—and his aesthetic tastes in the space were unparalleled. He deserves a lot of credit. Just nowhere near all of it.

"The thing that concerns me about the Steve Jobs and Edison complex," Bill Buxton, who helped pioneer multitouch in the 1980s (Jobs said Apple invented it in 2007), told me, "is that young people who are being trained as innovators or designers are being sold the Edison myth, the genius designer, the great innovator, the Steve Jobs, the Bill Gates, or whatever," Buxton says. See: The current myth of the founder-hero, that is partly to blame for steering companies like Uber into peril. "They're never being taught the notion of the collective, the team, the history."

Which is why it pains me a bit to see the story of the iPhone reduced to Jobs, brilliant as he may have been. The true version is more intense, messy, convoluted—and human. And it's not just a matter of doling out credit, either; it's a matter of understanding how innovation actually happens, so we might facilitate it better in the future. There are lessons here for anyone who might try to build a product, advance a technology, stir progress—or understand how innovation really unfurls. The iPhone is the product of a collaboration carried out on a scale that's so massive it can seem almost incomprehensible—but it makes more sense than the lone inventor myth. And we can learn more about where we're headed if we look into the iPhone's black mirror and try to see the huge host of faces reflected back—not just Steve Jobs'.

Brian Merchant is the author of The One Device: The Secret History of the iPhone.

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)

"I will face whatever comes today with a positive attitude."

Public Hearings on the Renegotiation of NAFTA

Link to Testimonies given : https://ustr.gov/about-us/policy-offices/press-office/press-releases/2017/june/public-hearing-nafta-renegotiation
The Office of the U.S. Trade Representative (USTR) held public hearings June 27-29, 2017 regarding the upcoming negotiations of the North American Free Trade Agreement (NAFTA).

The hearings took place at the U.S. International Trade Commission, 500 E Street SW, Washington, DC 20436.

The public hearings followed USTR's 90-day notification to Congress on May 18, 2017 regarding intent to renegotiate NAFTA as well as USTR's Federal Register notice published May 23, 2017 requesting public comment.

The public hearings were held at the following times:

- Tuesday, June 27, 2017 from 8:45 AM – 8 PM EDT
- Wednesday, June 28, 2017 from 9 AM – 6:30 PM EDT

Thursday, June 29, 2017 from 10 AM – 3 PM

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