EIB World Trade Headlines

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

September 2013 - Vol 5, Issue 14

Government Closed Today!

* **Licenses and Classifications by Commerce and State likely suspended or delayed.**

* **USATrade Online will be shutdown starting today until further notice.**

* **Post Office operates as independent business: NOT CLOSED**

* **Passports delayed or not at all**

* **Military paychecks may be delayed if there's a long shutdown.**

* **It's been 17 years since the last government shutdown**

* **Would Congress continue to be paid during a shutdown?** YES

  The 27th Amendment to the Constitution, ratified in 1992, holds that "No law, varying the compensation for the services of the Senators and Representatives, shall take effect, until an election of representatives shall have intervened." Intended to prevent Congress from voting itself a raise, it also protects members from a pay cut.

* **What effect would a shutdown have on the economy?**

  Economists say even a short shutdown — of three or four days — would begin to shave decimal points off economic growth. A sustained shutdown of three or four weeks "would do significant economic damage," economist Mark Zandi told USA TODAY

NEWSLETTER NOTES

Upcoming Export Control Seminars (Washington, D.C.)

The Bureau of Industry and Security invites you to register for one of these upcoming seminars to learn about export control requirements under the Export Administration Regulations.

Complying with U.S. Export Controls
Two Days
October 29-30, 2013
Alexandria, VA
$270

This two-day program 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 on commercial goods.

It 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 re-export without applying for a license; export clearance procedures and record keeping requirements; an overview of the Export Management and Compliance Program (EMCP) concepts; and real life examples in applying this information. Technical, policy, and enforcement professionals from BIS, as well as specialists from other agencies such as the Office of Foreign Assets Control and the Bureau of the Census will participate.

View "Complying with U.S. Export Controls" event details.

Export Control Reform
One Day
October 31, 2013
Alexandria, VA
$170

This one-day training course is designed to provide in-depth exposure to core elements of the Export Control Reform (ECR) initiative. Regulatory, compliance, and engineering officers will provide training on the key elements ranging from licensing issues to "specially designed" and license exceptions such as use of the Strategic Trade Authorization.

(Continued above)

The course will focus on new and different compliance requirements. This course will be useful to defense exporters with relatively limited exposure to the regulatory requirements of the Export Administration Regulations, and to exporters who now will be able to support U.S. military items without incurring International Traffic in Arms Regulations (ITAR) liability.

Prerequisite: Participants should, at a minimum, have a working knowledge of the Export Administration Regulations, and an understanding of what is required to comply with U.S. export requirements. Some basic information is available on the BIS website at www.bis.doc.gov as online training.

View "Export Control Reform" event details. Attend both Alexandria, VA seminars, Complying and Export Control Reform, for $400.00

For further details and registration, go to:http://www.bis.doc.gov/index.php/compliance-a-training/export-administration-regulations-training/current-seminar-schedule?id=43

Visit the BIS web site at www.bis.doc.gov

For general information about the BIS Seminar Program contact the Outreach and Educational Services Division at: OESDSeminar@bis.doc.gov , or 202/482-6031.
You can unsubscribe by clicking this URL
This email was sent at your request, based upon your subscription to the BIS Email Notification service.

The BIS Web Site Team

Eurocopter Reinforces its Capabilities in The United States With the Installation of an AS350 Assembly Line

Beginning in 2014, Eurocopter will install the necessary industrial capabilities to upgrade the American Eurocopter plant in Columbus, Mississippi, to a final assembly and test site for Eurocopter AS350 helicopters, the top-selling civil helicopter in the U.S. market.

The plan was developed with two main objectives in mind: First, as a way to offset the impact of the reduction in local production of UH-72A Lakota helicopters and second, to help provide a boost to sales in the U.S. market, especially with government and law enforcement agencies. "North America is the largest light helicopter market in the world for Eurocopter, and this new assembly line supports our industrial strategy by manufacturing the preferred AS350 'Made in the USA' in close proximity to our customers," said Joseph Saporito, Executive Vice President of the Global Supply Chain for Eurocopter. "This decision further supports our investments that have developed reliable and efficient local industrial capabilities in a market with strong expected growth."

He plan calls for the Columbus plant to become a final AS350 assembly and test site using parts produced by Eurocopter and its suppliers, in addition to the continued production and retrofit of UH-72A Lakotas for the U.S. Army, other federal agencies and foreign military customers. "I am extremely happy to be able to announce we will be able to maintain and expand the Columbus plant's operations and retain our skilled and dedicated workers," said American Eurocopter President and CEO Marc Paganini. "Our teams in Mississippi have done a superb job of producing the Lakota for the Army and we want to put their expertise to work building helicopters for the civil market in the U.S."

Preparations will begin almost immediately, with the final assembly line scheduled to begin production in the fourth quarter of 2014. Operations are set to expand in 2015 and the plant will produce up to 60 additional helicopters annually by 2016.

(Continued above)

The Columbus plant – American Eurocopter's second location in addition to its headquarters in Grand Prairie, Texas – is currently responsible for both the assembly and testing of the highly successful UH-72A Lakota aircraft, for which more than 280 aircraft have been delivered on budget and on or ahead of schedule. Its teams also handle the partial assembly of the AS350 from kits for certification flight tests before sending the aircraft to completion centers, where they are installed with customer-specified interiors, instrumentation and special equipment.

Eurocopter's international development allows the Group to better meet its customers' needs by remaining in close proximity, no matter where they are in the world. Opportunities that allow, in addition to this proximity, an in-sourcing of high-value business in key markets reinforce the Group's commitment to creating strong local industrial footholds in both emerging as well as established markets.

Representing nearly 40% of Eurocopter's worldwide in-service rotorcraft fleet, some 3,549 AS350s are currently flying around the globe – with nearly one quarter of them in the U.S. alone. American Eurocopter delivered 42 new AS350 helicopters in 2012.

The AS350 outclasses all other single-engine helicopters for performance, versatility, safety and competitive acquisition and maintenance costs. It is the first choice in the U.S. market for law enforcement agencies and helicopter emergency medical service providers.

Source: **Eurocopter, an EADS N.V. company (Paris: EAD.PA)**
Published on ASDNews: Sep 23, 2013

Boeing QF-16 Aerial Target Completes 1st Pilotless Flight

Provides Next Generation of Combat Training for US Air Force*

Boeing [NYSE: BA] and the U.S. Air Force have completed the first unmanned QF-16 Full Scale Aerial Target flight, demonstrating the next generation of combat training and testing.

Two U.S. Air Force test pilots in a ground control station remotely flew the QF-16, which is a retired F-16 jet modified to be an aerial target. The QF-16 mission profile included auto takeoff, a series of simulated maneuvers, supersonic flight, and an auto land, all without a pilot in the cockpit.

XCOR Aerospace and ULA Announce Important Milestone in Liquid Hydrogen Engine Program

XCOR Aerospace and United Launch Alliance announced significant progress today in the XCOR/ULA liquid hydrogen (LH2) engine development program.
"We are happy to announce that we have successfully operated our liquid hydrogen pump at full design flow rate and pressure conditions," said XCOR Chief Executive Officer Jeff Greason. "This milestone builds on our earlier success with liquid oxygen and kerosene pumps, which have powered many of our hotfires. Achieving this goal allows us to proceed with integrated testing of our liquid hydrogen demonstrator engine, fed by our liquid hydrogen and liquid oxygen piston pumps. The ultimate goal is a far more cost-effective upper-stage engine for ULA and their customers."

Read more: http://www.asdnews.com/news-51247/XCOR_Aerospace_and_ULA_Announce_Important_Milestone_in_Liquid_Hydrogen_Engine_Program.htm?HASH=c8f69915b03274a709972e2947c2767d&utm_source=ASDNews&utm_medium=email&utm_campaign=ASDNews+Daily+Z1&utm_content=jeanette%40eib.com#ixzz2gNh5uNh4

Aircraft Cabin of the Future Turns Heads in United States

Things Are Looking Up for Airline Passengers

Our IntelliCabin™ system made its U.S. debut this week at the Airline Passenger Experience (APEX) Expo — a trade show that brings together representatives from more than 120 airlines and hundreds of suppliers, all committed to improving the air travel experience for travelers around the world.

This cabin of the future integrates a variety of cabin functions to create a more premium experience for passengers and to benefit airline and OEM customers. These enhanced features include dynamic LED lighting, temperature control, seat control and power, and galley functions in one adaptive control panel or mobile device. IntelliCabin frees the crew to better serve their passengers and efficiently managing power throughout the cabin.

Related Research on ASDReports.com:
Electric Aircraft 2013-2023

"Our meetings with potential customers have yielded overwhelmingly positive feedback about IntelliCabin," said Faran Siddiqi, IntelliCabin business development lead at BAE Systems. "Its power management feature – with the ability to provide power to seats throughout the cabin – has been especially well received."
Our Commercial Aircraft Solutions team from Endicott, N.Y., first launched IntelliCabin at the Aircraft Interiors Expo in Hamburg, Germany earlier this year and then chose the APEX Expo for its North American launch, with high expectations for successful customer demos in the system's simulator.

IntelliCabin is in development now, and its power features will be available in the fourth quarter of 2014. So be on the lookout for this adaptable, scalable, and flexible system onboard a future flight — after all, it is the cabin of the future.
Source: **BAE Systems PLC (LSE: BAES.L)**

Read more: http://www.asdnews.com/news-51084/Aircraft_Cabin_of_the_Future_Turns_Heads_in_US.htm?utm_source=ASDNews&utm_medium=email&utm_campaign=Channel_12_16_09#ixzz2gNhfTvFw

Series of Webinars on Mexico

***For more information, contact:** Linda Abbruzzese at Linda.Abbruzzese@trade.gov

Webinar 2 of 7: Exporting to Mexico - Mexican Customs Topics: Taxes & Tariffs 101

Venue: Your Computer
Date: Thursday, October 17, 2013
Time: 2 - 3 p.m. EDT
Cost: $25
Register: https://emenuapps.ita.doc.gov/ePublic/event/editWebReg.do?SmartCode=4Q0M

In this webinar you will learn the Mexican customs definitions when paying value added taxes, paying an import tariff tax and dealing with customs tariff laws. Learn when to and when not to pay taxes and tariffs.

Webinar 3 of 7: Exporting to Mexico - NAFTA Certificate of Origin

Venue: Your Computer
Date: Wednesday, November 13, 2013
Time: 2 - 3 p.m. EDT
Cost: $25
Register: https://emenuapps.ita.doc.gov/ePublic/event/editWebReg.do?SmartCode=4Q0L

In this webinar you will learn why the NAFTA Certificate of Origin is essential and beneficial to U.S. exporters, and the benefits gained when using the NAFTA Certificate of Origin.

Webinar 4 of 7: Exporting to Mexico - INCOTERMS Review and INCOTERM Common Practices in Mexico

Venue: Your Computer
Date: Wednesday, December 18, 2013
Time: 2 - 3 p.m. EDT
Cost: $25
Register: https://emenuapps.ita.doc.gov/ePublic/event/editWebReg.do?SmartCode=4Q0N

In this webinar you will learn Incoterm best practices in Mexico and which is the most appropriate Incoterm to use when exporting to Mexico.

(Continued below)

Webinar 5 of 7: Exporting to Mexico - Exporting Goods to Mexico Using Courier Services and Postal Service

Venue: Your Computer
Date: Wednesday, January 15, 2014
Time: 2 - 3 p.m. EDT
Cost: $25
Register: https://emenuapps.ita.doc.gov/ePublic/event/editWebReg.do?SmartCode=4Q0P

In this webinar you will learn the advantages of using courier services and the postal service to send samples or specific goods into Mexico and the Mexican customs process of handling your exports into Mexico.

Webinar 6 of 7: Exporting to Mexico - Mexican Import Process

Venue: Your Computer
Date: Wednesday, February 12, 2014
Time: 2 - 3 p.m. EDT
Cost: $25
Register: https://emenuapps.ita.doc.gov/ePublic/event/editWebReg.do?SmartCode=4Q0Q

In this webinar you will learn if your client in Mexico is able to import, how the import process works, and other options and alternatives to send your products to your client in Mexico.

Webinar 7 of 7: Exporting to Mexico - How to Settle Disputes with Mexican Customs

Venue: Your Computer
Date: Wednesday, March 12, 2014
Time: 2 - 3 p.m. EDT
Cost: $25
Register: https://emenuapps.ita.doc.gov/ePublic/event/editWebReg.do?SmartCode=4Q0R

In this webinar you will learn how to solve controversies and misunderstandings about Harmonized System codes assignation, permits and requirements. You will learn about the U.S. and Mexican customs laws when exporting your products into Mexico and what tools you need to solve any disputes at the Mexican customs.

Series of Webinars on Canada:
For more information, contact: Tracey Ford at Tracey.Ford@trade.gov

(Continued above)

Webinar: Canada: Temporarily Moving U.S. Service Exporters across the Border

Venue: Your Computer
Date: Thursday, October 31, 2013
Register: https://emenuapps.ita.doc.gov/ePublic/event/editWebReg.do?SmartCode=4Q0D

This webinar will assist U.S. service companies, such as architects, engineers and technicians in identifying the process for sending temporary workers to Canada to perform after-sales warranty repairs, business development and other tasks. Topics include: temporary work visas, NAFTA, documentation requirements at the border, and tax implications for companies performing service work in Canada.

Webinar: Canada: Temporarily Moving Capital Equipment & Tools across the Border

Venue: Your Computer
Date: Thursday, November 7, 2013
Register: https://emenuapps.ita.doc.gov/ePublic/event/editWebReg.do?SmartCode=4Q0E

Temporary workers entering Canada are often required to bring tools and equipment with them across the border to complete their work. This webinar will address efficient ways to move equipment to/from Canada temporarily, tax implications and general import requirements and documentation.

Webinar: Canada: Handling Duties and Taxes - NAFTA, HST & Other Considerations

Venue: Your Computer
Date: Thursday, November 14, 2013
Learn
Register: https://emenuapps.ita.doc.gov/ePublic/event/editWebReg.do?SmartCode=3QAQ

This webinar will provide U.S. exporters with background on NAFTA and identifying duties and taxes that may be applicable on sales. For product-focused companies, understanding the 'hidden' costs of doing business cross border can be a daunting task for the U.S. shipper and a surprising cost for the importer. Understanding what these costs are and being able to provide a transparent sale to your Canadian customer can be the key to successfully doing business in Canada.

Webinar: Digital & Social Media Market Entry Strategies for Canada

Venue: Your Computer
Date: Thursday, November 21, 2013
Register: https://emenuapps.ita.doc.gov/ePublic/event/editWebReg.do?SmartCode=4Q0F

This webinar will provide tips on how to generate e-commerce sales to Canadian end-users, as well as strengthening their online presence to reach and capture new customers in this important market. For U.S. exporters, shipping to Canada opens the gate to over 28 million internet users. Statistics show that a large portion of Canadian consumer's online spending is conducted with establishments outside of the country, primarily in the United States.

US Navy Awards GD $26 M for USS Providence Maintenance and Modernization

The U.S. Navy has awarded General Dynamics Electric Boat a $25.7 million contract to prepare and perform maintenance and modernization work on the USS Providence (SSN-719), a Los Angeles-class attack submarine. Electric Boat is a wholly owned subsidiary of General Dynamics (NYSE: GD).

Under the terms of the contract, Electric Boat will perform a dry-docking continuous maintenance availability, which consists of maintenance work, upgrades and modernization activities required to ensure the submarine is operating at full technical capacity. The work will take place at the Electric Boat shipyard in Groton and involve up to 300 employees at its peak. The work is scheduled for completion in April 2014.

Read more: http://www.asdnews.com/news-51367/US_Navy_Awards_GD_USD26_M_for_USS_Providence_Maintenance_and_Modernization.htm?HASH=c8f69915b03274a709972e2947c2767d&utm_source=ASDNews&utm_medium=email&utm_campaign=ASDNews+Daily+Z1&utm_content=jeanette%40eib.com#ixzz2gO7opAwQ

DPAS PROGRAM

Statement of
Eric L. Hirschhorn
Under Secretary of Commerce for Industry and Security Before the
Committee on Banking, Housing, and Urban Affairs

U.S. Senate
July 16, 2013

Chairman Johnson, Senator Crapo, Members of the Committee:

I appreciate the opportunity to testify before the Committee this morning on the important role the Defense Production Act (DPA) continues to play in supporting our national defense. I will focus my comments on the non-permanent DPA authorities in Titles I and VII that are relevant to the Department of Commerce and the activities of the Department under those authorities.

The Department of Commerce plays several roles in implementing DPA authorities related to the defense industrial base. First, under Title I, the Department administers the Defense Priorities and Allocations System. Second, under Title VII, the Department analyzes the health of U.S. defense industrial base sectors. Third, also under Title VII, the Department submits an annual report to Congress on offsets in defense trade. All three DPA authorities need to be reauthorized before September 30, 2014. I will briefly discuss each of these roles.

I. Defense Priorities and Allocations System

Title I of the Defense Production Act authorizes the President to require acceptance and priority performance of contracts and orders (other than contracts of employment) to promote the national defense over performance of any other contracts or orders, and to allocate materials, services, and facilities as deemed necessary or appropriate to promote the national defense. These authorities to prioritize contracts and require allocations for industrial resources were most recently delegated to the Secretary of Commerce by Executive Order 13603, which was issued in March 2012. However, the Department has had similar authority since the DPA was first enacted in 1950.

(Continued below)

Today, the Bureau of Industry and Security implements these authorities through the Defense Priorities and Allocations System regulation (15 CFR Part 700) (most commonly known as the "DPAS"). The DPAS establishes procedures for the placement, acceptance, and performance of priority rated contracts and orders and for the allocation of materials, services and facilities and is regularly used to support the acquisition of industrial resources needed to support U.S. national defense requirements, especially by the Department of Defense.

All companies in the United States must comply with the provisions of the DPAS regulation. The key elements of the DPAS regulation are mandatory acceptance of rated orders, preferential scheduling, and extension of priority ratings throughout the supply chain. Under the DPAS, there are two levels of priority designated by the symbols "DO" and "DX." All "DO" rated orders have equal priority with each other and take preference over unrated orders. All "DX" 3 rated orders have equal priority with each other and take preference over "DO" rated orders and unrated orders.

A "priority rating" on a contract or order notifies a supplier that the contract is supporting an approved national defense program and that the supplier must accept and give the order priority over unrated commercial orders (or lower rated orders in the event of competing "DX" and "DO" orders), as necessary, to meet the required delivery date. A contractor in receipt of a rated order, in turn, places "priority rated orders" with its subcontractors for parts and components.

Our industrial base is well-versed in the DPAS based on more than 60 years of experience in receiving and placing priority rated contracts and orders to support Department of Defense requirements. The private sector also appreciates that the DPA includes a protection against claims in the event a contractor, subcontractor, or supplier is required to reschedule an unrated order after receipt of a rated order.

The Department of Commerce has delegated authority to the Departments of Defense (DOD), Energy (DOE), and Homeland Security (DHS), and the General Services Administration, to place priority ratings on contracts or orders for industrial resources to support programs determined by DOD, DOE, or DHS as "necessary or appropriate to promote the national defense." The Department of Commerce may also authorize other government agencies, foreign governments, owners and operators of critical infrastructure, or companies to place priority ratings on contracts or orders on a case-by-case basis. Such requests must first be determined as "necessary or appropriate to promote the national defense" by DOD, DOE, or DHS.

(Continued above)

Let me briefly highlight a few examples of the Department's work in administering the DPAS.

The Department of Defense remains the primary user of the DPAS. My Department has worked closely with DOD to support the U.S. Armed Forces through the DPAS to expedite the delivery of industrial resources needed to support critical operational requirements, including the Interceptor Body Armor, counter-improvised explosive devices, and the Mine Resistant Ambush Protected vehicle programs. In addition, Commerce, in coordination with the Department of Defense, has authorized foreign defense ministries to place priority ratings on contracts and orders with U.S. suppliers for equipment needed to support coalition operations in Iraq and Afghanistan.

My Department is very proud of the role we have played through the DPAS to support our servicemen and servicewomen and to assist our coalition partners.
The Department has also worked closely with the Department of Homeland Security's Federal Emergency Management Agency through the DPAS to support emergency preparedness and critical infrastructure protection and restoration requirements. For example, the Department worked with DHS to authorize the U.S. Army Corps of Engineers to use the DPAS to support the repair and expansion of the Hurricane Protection System for the Louisiana Gulf Coast Region.

The Corps of Engineers placed priority ratings on hundreds of contracts to expedite delivery of pumps, structural steel and concrete for levees and floodwalls, and other related flood control infrastructure to reduce the risk of floodwaters from future natural disasters.
The Department has also worked with DHS to authorize other Federal agencies (including the Department of State, the Federal Bureau of Investigation, and Commerce's National Oceanic and Atmospheric Administration) to place priority ratings on orders to expedite the delivery of industrial resources 5

(Continued below)

needed to enhance the protection of government facilities and to support systems designed to detect and track severe weather.
These examples, and the testimony from my DOD and DHS colleagues, demonstrate how the DPAS remains critically relevant to support our national defense, including military and homeland security requirements.

Since the 2009 reauthorization of the Defense Production Act, the Department has also collaborated with the five other federal departments that are delegated priorities and allocations authority with respect to other resources (Agriculture, Energy, Defense, Health and Human Services, and Transportation) and with DHS to develop and implement a consistent and unified Federal priorities and allocations system to the extent practicable.

The new rules being developed by the other departments for the resources under their priorities and allocations jurisdiction are based primarily on DPAS guidance and procedures and incorporate several key elements of the DPAS, including: mandatory acceptance of rated orders, preferential scheduling of rated orders to meet delivery requirements, and extension of priority ratings by contractors to lower-level suppliers and subcontractors. The Department of Commerce is also in the process of updating the DPAS regulation based on our collaboration with our interagency partners.

II. Defense Industrial Base Studies

Under Section 705 of the DPA and Executive Order 13603, the Department also conducts surveys and assessments of defense-related industries and technologies. These assessments are usually requested by the Department of Defense. Using these industrial base studies, the
Departments of Commerce and Defense can, for example, monitor trends, benchmark industry performance, and raise awareness of diminishing manufacturing capabilities. The studies also provide detailed data that are unavailable from other sources.

Currently, the Department of Commerce has a number of studies underway, including an assessment of the U.S space industry supply chain. Commerce has partnered with NASA, the U.S. Air Force, and the National Reconnaissance Office to gain an understanding of the complicated network supporting the development, production and sustainment of products and services across the defense, intelligence community, civil and commercial space sectors. Additionally, Commerce is assessing the cartridge and propellant actuated device (CAD/PAD) industry, and the underwater acoustics and transducers industry. When completed, these assessments will provide the requesting agency or agencies with information needed to understand the health and viability of the studied sector.

(Continued above)

III. Offsets in Defense Trade

Pursuant to Section 723 of the DPA, the Department also reports to Congress annually on the impact of offsets in defense trade. Offsets in defense trade encompass a range of industrial compensation practices required by foreign governments as a condition of the purchase of defense articles and services from a non-domestic source. This mandatory compensation can be directly related to the purchased defense article or service or it can involve activities or goods unrelated to the defense sale.

The Department collects data annually from U.S. firms involved in defense exports with associated offset agreements in order to assess the impact of offsets in defense trade. In February 2013, the Department submitted its 17th report to Congress on offsets in defense trade, with data covering the 1993-2011 period. U.S. industry submitted 2012 offset data to the Department in June 2013 in accordance with the offset reporting regulation (15 CFR Part 701). The Department will analyze this data and present its findings to Congress later this year.

IV. Defense Production Act Committee

The Department of Commerce is also a member of the interagency Defense Production Act Committee (DPAC) which was established pursuant to the 2009 DPA reauthorization to advise the President on the effective use of the act's authority. The President has designated Homeland Security and Defense as rotating chairs of the DPAC. Commerce plays an active role in the work of study groups established by the DPAC, including the group that is assessing the use of DPA authorities to support disaster preparedness and response and critical infrastructure protection and restoration activities.

Summary

In sum, the DPA provides authority for a variety of programs at the Department of Commerce of substantial importance to our nation's security.

(Continued below)

The DPAS continues to facilitate the timely delivery of industrial resources to support the Department of Defense, coalition partners, and increasingly, to meet Homeland Security requirements. The DPA also facilitates valuable assessments of the health of key sectors of the defense industrial base and the impact of offsets in defense trade.

The Department of Commerce looks forward to working with the Committee to reauthorize the non-permanent provisions of the Defense Production Act.

Thank you.

Samsung Smart TVs Can Be Hijacked, Researchers Warn

SoftPedia
August 5, 2013

Present at the Black Hat 2013 security conference last week, ISEC Partners engineers Aaron Grattafiori and Josh Yavor demonstrated how cybercriminals could hack Samsung Smart TVs.

The duo has shown that an attacker can leverage vulnerabilities in the TVs operating system and applications to steal sensitive information and even use the integrated webcam to spy on the victim, Security Ledger reports.

While some of the flaws can only be exploited by a local attacker, others can also be leveraged remotely. According to the experts, the devices do not have firewalls and strong authentication systems that could protect them against cyberattacks. Yavor and Grattafiori have discovered that they can exploit many well-known web-based vulnerabilities on Samsung TVs.

They've been able to leverage the bugs for drive-by download attacks and DNS poisoning. They've demonstrated that cybercriminals can steal local user credentials, local Wi-Fi credentials, the browsing history, cookies and cache. Even Skype accounts can be hijacked, and cybercriminals can take control and access the application program interfaces (APIs) linked to vulnerable Java apps.

The researchers reported their findings to Samsung in January. The company has taken some steps to address the problems in several models. The issues that affect the API will be fixed next year.

The Skype flaws were fixed shortly after being reported, the experts said. The ISEC Partners engineers admit that it's not easy to carry out the attacks they've presented. However, they want to warn manufacturers that building a framework on HTML and JavaScript applications comes with a risk that should not be disregarded.

This is not the first time experts find security holes in Samsung Smart TVs. Back in December 2012, ReVuln experts **demonstrated** that they could access sensitive information, monitor the devices and even gain complete control of them.

If Governments Ban China-Based Lenovo, Should Companies?

PC ADVISOR
August 5, 2013

If U.S. intelligence agencies ban the computers of a Chinese company from classified networks should companies also avoid the same products? What if the vendor is one of the world's largest PC makers? Those questions are not academic. Intelligence and defense agencies in the U.S. and several other Western countries have banned computers from China-based Lenovo from networks deemed "secret" or "top secret," says a recent report by The Australian Financial Review.

The ban has existed since the mid-2000s, when extensive testing found backdoor hardware and firmware in Lenovo chips that could be exploited by hackers and cyberspies, the report said. Countries banning the company's products include the U.S., Britain, Canada, New Zealand and Australia. The report is a reminder of the threats that exist within an organization's supply chain, which can span many countries.

To review the rest of the article click on the link: http://www.pcadvisor.co.uk/news/security/3462311/if-governments-ban-china-based-lenovo-should-companies/

Chinese National Sentenced for Illegally Exporting Military Electronics Components

DOJ.GOV
September 10, 2013

BOSTON - Zhen Zhou Wu, a Chinese national, was re-sentenced yesterday to 84 months in prison for conspiring over a 10-year-period to illegally export military and sophisticated electronics to the People's Republic of China (PRC).

Wu was also convicted of illegally exporting sensitive electronic components to the PRC on 12 occasions between 2004 and 2007. Several Chinese military entities were among those to whom the defendant exported the equipment, which is used in military phased array radar, electronic warfare, and missile systems. He was also ordered to pay a $15,000 fine. After serving his sentence Wu will be subject to deportation to the PRC.

On March 19, 2013, the U.S. Court of Appeals for the First Circuit affirmed Wu's conviction on 15 of the 17 counts of export violations for which a jury convicted him after a six-week trial in 2010. The First Circuit vacated two counts of conviction that charged Wu with illegally exporting parts designated on the United States Munitions List because it held that the jury instructions given were constitutionally inadequate.

However, the First Circuit observed that "from 1996 until 2008, Wu and his co-defendant, Yufeng Wei, shipped tens of millions of dollars worth of sophisticated electronic components from the United States to China, with little regard for whether the parts that they sold were export-controlled." Further, the First Circuit found that Wu's company "specifically pursued military customers; and Wu promoted himself as both an exporter of military supplies and an export compliance expert." Lastly, the First Circuit determined that "Wu and Wei repeatedly attempted to disguise the fact that they were exporting to China and that they lacked the necessary licenses to do so."

(Continued above)

Because two counts of the conviction were vacated, the case was remanded for a re-sentencing hearing. Wei's re-sentencing hearing has not yet been scheduled.

On May 17, 2010, Wu, his ex-wife, Wei, and his company, Chitron Electronics, Inc. were convicted of conspiring to unlawfully export to the PRC military electronics from 1997 to 2007 and export restricted electronics components and illegally exporting such parts to the PRC on numerous occasions between 2004 and 2007. The defendants' illegal enterprise involved the use of Chitron Electronics, Inc., a company Wu established in Waltham, Mass., as a front company for its parent company, Chitron Electronics Limited, headquartered in Shenzhen, PRC.

Wu used Chitron-US to procure export restricted equipment from US suppliers and then export the goods to from Waltham to China, through Hong Kong without the suppliers' knowledge. The exported equipment is used in electronic warfare, military radar, fire control, military guidance and control equipment, missile systems, and satellite communications. Many of Chitron's customers were Chinese military research institutes and military entities responsible for procuring, developing, and manufacturing electronic components for China's Army, Navy and Air Force.

The Department of Defense's Defense Technology Security Administration concluded in a report filed with the Court that the defendants' activities in this case seriously threatened "U.S. national and regional security interests." According to the Department of Defense, the parts the defendants were convicted of illegally exporting are "vital for Chinese military electronic warfare, military radar, fire control, military guidance and control equipment, and satellite communications." The report further concluded that the illegally exported parts are "precisely the [types of] items ... that the People's Liberation Army actively seeks to acquire."

(Continued below)

United States Attorney Carmen M. Ortiz; Acting Assistant Attorney General John P. Carlin of the Justice Department's National Security Division; John J. McKenna, Special Agent in Charge of the U.S. Department of Commerce, Office of Export Enforcement, Boston Field Office; Bruce Foucart, Special Agent in Charge of Homeland Security Investigations in Boston: Vincent B. Lisi, Special Agent in Charge of the Federal Bureau of Investigation, Boston Field Office; and Leigh-Alistair Barzey, Resident Agent in Charge of Defense Criminal Investigative Service in Boston made the announcement. The case is being prosecuted by Assistant U.S. Attorneys B. Stephanie Siegmann and John A. Capin of Ortiz's Anti-Terrorism and National Security Unit.

Chinese National Pleads Guilty to Illegally Exporting Radiation-Hardened Computer Circuits Used in Satellite Communications to China

DOJ.GOV
September 9, 2013

DENVER – Philip Chaohui HE, aka Philip Hope, who was residing in Oakland, California, pled guilty September 3, 2013, before Senior U.S. District Court Judge Wiley Y. Daniel to conspiracy to violate the Arms Export Control Act and to Smuggle Goods from the United States, United States Attorney John Walsh and U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI) Special Agent in Charge Kumar C. Kibble announced. HE is scheduled to be sentenced by Judge Daniel on December 18, 2013 at 10:00 a.m. He is in federal custody.

According to court documents, including the stipulated facts contained in the plea agreement, HE attempted to illegally export to China radiation-hardened computer memory circuits used in satellite communications with a value of almost $550,000. HE, the only employee of Oakland, California-based Sierra Electronic Instruments (SEI), purchased 312 radiation-hardened circuits from a Colorado manufacturer. The circuits purchased by HE are categorized as defense articles within the International Trafficking in Arms Regulations (ITAR). Lawfully exporting defense articles requires licensing from the U.S. State Department's Directorate of Defense Trade Controls.

(Continued above)

On April 28, 2011, an unindicted co-conspirator caused two wire transfers totaling about $489,720 to be sent to HE's bank account in California. On or about May 9, 2011, HE provided payment in full, $549,654, at the time HE placed the order with the Colorado manufacturer. According to the indictment, on or about May 17, 2011,

HE provided false certification to the Colorado manufacturer that his company was purchasing the integrated circuits for end-use in the United States only, and HE further acknowledged that the items were controlled by U.S. Export Laws and could not be transferred, transshipped or otherwise disposed of in any other country, without the prior written approval of the U.S. Department of State.

On December 11, 2011, HE drove to the Port of Long Beach, California, and met with two men in front of a docked ship bearing a Chinese flag. The Chinese-flagged ship was registered to Zhenhua Port Machinery Company LTD, a subsidiary of the China state-owned corporation China Communications Construction. The ship had recently arrived from Shanghai, China, and was scheduled to return on December 15, 2011.

HE concealed 200 integrated circuits in several plastic infant formula containers placed inside five boxes which were sealed and labeled as "milk powder" written in Chinese. HE transported the boxes in the trunk compartment of his vehicle. Neither HE, nor his company SEI had a license to export defense articles of any description.

"We have specific laws designed to protect sensitive American technology from getting into the wrong hands overseas," said U.S. Attorney John Walsh. "Defendant HE attempted to smuggle export-controlled radiation-hardened computer chips to China, and faces serious punishment for his criminal activity."

(Continued below)

"The Arms Export Control Act is designed to prevent having our technology illegally exported and ultimately used against us," said Kumar C. Kibble, special agent in charge of HSI Denver. "Our HSI special agents in Colorado Springs, San Francisco and Los Angeles worked together with our law enforcement partners to investigate Philip HE and eliminate the threat he posed to this country."

For conspiring to violate the Arms Export Control Act (AECA) and to Smuggle Goods from the U.S., HE faces not more than 5 years in federal prison, and a fine of up to $250,000.

Massachusetts Man Charged with Selling Counterfeit Semiconductors Intended for Use on Nuclear Submarines

DEPARTMENT OF JUSTICE
July 15, 2013

Peter Picone, 40, of Methuen, Mass., has been charged with importing counterfeit semiconductors from China for sale in the United States.

The charges were announced today by Acting Assistant Attorney General Mythili Raman of the Justice Department's Criminal Division; Acting U.S. Attorney for the District of Connecticut Deirdre M. Daly; Special Agent in Charge Bruce Foucart of U.S. Immigration and Customs Enforcement (ICE) - Homeland Security Investigations (HSI) in Boston; Acting Special Agent in Charge of Defense Criminal Investigative Service (DCIS) Northeast Field Office Craig W. Rupert; and Special Agent in Charge of the Naval Criminal Investigative Service (NCIS) Northeast Field Office Cheryl A. DiPrizio.

The eight-count indictment charges Picone with conspiring to traffic in counterfeit goods, conspiring to traffic in counterfeit military goods, trafficking in counterfeit goods, conspiring to commit wire fraud, wire fraud and conspiring to commit money laundering. The indictment was returned by a federal grand jury in New Haven on June 25, 2013, and was unsealed today.

The indictment charges that from February 2007 through April 2012, Picone, through two companies he owned and operated, Tytronix Inc. and Epic International Electronics, purchased counterfeit semiconductors from sources in Hong Kong and China.

According to the indictment, Picone made false representations about the semiconductors and sold them to customers throughout the United States, including companies believed by Picone to be defense contractors in Connecticut and Florida. Certain semiconductors sold by Picone were intended for use on nuclear submarines.

"By allegedly purchasing and reselling counterfeit semiconductors for military applications, Peter Picone put personal gain above the safety and well-being of dedicated U.S. servicemen and women," said Acting Assistant Attorney General Raman. "As charged in the indictment, Picone went to great lengths to conceal the true origin of counterfeit semiconductors in order to sell the devices as seemingly legitimate and reliable components for use in nuclear submarines and other complex machinery.

The charges unsealed today demonstrate our steadfast commitment to working with our law enforcement partners to prosecute counterfeiters and others who risk the security of the men and women of the U.S. military."

To review the rest of the article click on the link:
http://www.justice.gov/opa/pr/2013/July/13-crm-790.html

Hacker Group in China Linked to Big Cyber Attacks: Symantec

REUTERS
September 17, 2013

Researchers have discovered a group of highly sophisticated hackers operating for hire out of China, a U.S. computer security company said on Tuesday, and it linked them to some of the best-known espionage attacks in recent years. Symantec Corp said the group, which it dubbed "Hidden Lynx," was among the most technically advanced of several dozen believed to be running cyber espionage operations out of China. Unlike a previous report by another company, Symantec did not accuse the Chinese government of involvement in the cyber attacks.

Symantec's 28-page report described Hidden Lynx as a "professional organization" staffed by between 50 and 100 people with a variety of skills needed to breach networks and steal information, including valuable corporate secrets. The company said its researchers believed Hidden Lynx might have been involved with the 2009 Operation Aurora attacks, the most well-known cyber espionage campaign uncovered to date against U.S. companies.

To review the rest of the article click on the link:
http://www.reuters.com/article/2013/09/17/us-cyberattacks-china-idUSBRE98G0M720130917

Robot Parts Seized at Trade Show after iRobot Takes Legal Action against Chinese Firm

BOSTON BUSINESS JOURNAL
September 6, 2013

Legal documents were served and robot parts were seized at the IFA consumer electronics trade show in Berlin after a Chinese firm allegedly infringed patents owned by robotics firm iRobot Corp.

(Continued above)

According to Bedford, Mass.-based iRobot Corp. (Nasdaq: IRBT), Shenzhen Silver Star Intelligent Electronic Ltd. and Shenzhen Star Intelligent Technology Co. Ltd infringed four German parts of four European patents, EP 1 331 537 B1, EP 2 251 757 B1, EP 1 969 438 B1, and EP 1 395 888 B1. The District Court of Düsseldorf granted the preliminary injunctions against the company, confirming that the vacuum cleaner robots infringe all four named patents.

"iRobot has made significant investments to protect its intellectual property. The company has sold more than 10 million home robots worldwide and intends to protect its patent portfolio by the appropriate means available domestically and abroad," said Colin Angle, chairman and CEO of iRobot, in a statement. The company's Home Robots unit holds more than 100 patents, 37 of which cover the Roomba vacuum cleaning robot.

Earlier this year, iRobot sued four businesses that were allegedly selling the Solac Ecogenic AA3400 robotic vacuum cleaning robot based on five European patents held by iRobot and in 2011 iRobot achieved a successful settlement with New Majestic S.p.A. after enforcing patents EP 1 969 438 and EP 2 251 757 in Italy, according to the company.

To review the rest of the article click on the link:
http://www.bizjournals.com/boston/blog/techflash/2013/09/robot-parts-seized-at-ifa-tradeshow.html

Secure-Travel Advice for Black Hat... and Your Local Starbucks

GCN
July 26, 2013

The annual Black Hat USA conference being held in Las Vegas July 27-Aug. 1 is not exactly a hostile environment, but if you go, you will be with a lot of people eager to demonstrate their hacking skills on the less witting among them. The opening ceremonies typically include a reminder that although Wi-Fi connections are provided, attendees are responsible for their own security when connecting.

(Continued below)

So if you are representing your agency at the conference, don't neglect the basics for secure use of your laptop, tablet or any other Internet-enabled device you take with you.
Black Hat is not as rough a neighborhood as its older sibling, DEF CON, where "Spot the Fed" has been a popular game for 20 years. This year feds have been advised to sit out DEF CON (Aug. 1-4) in the wake of the Edward Snowden revelations that have increased some anti-government feelings. But government is always a juicy target for people interested in establishing their hacker creds. Not that attacks at Black Hat single out government. "What I've found is that it's more of a passive scanning," said Jeff Debrosse, director of advanced research projects for Websense Security Labs. "It's not targeted, it's targets of opportunity."

The crowd attending Black Hat is varied, Debrosse said. "I don't run into really dangerous people there; I run into serious people with varying degrees of expertise and skill," from script kiddies to those who set up their own femtocells to capture cellular traffic. That means you can't assume that any connection is secure. Even when plugging in at your hotel room, it's probable that the hotel is using a wireless bridge at some point that could expose you.

"Leverage VPNs," Debrosse advised those working at the conference. "I'm always about encryption, encryption, encryption." Debrosse offered some common-sense tips for protecting yourself at Black Hat. And even if you're not going, they also apply to just about any out-of-office experience you might have.

They include:

*Make sure your devices are fully patched and antivirus software is updated.

*Delete cookies and clear your browser history and cache to limit residual information about your habits.

*Encrypt sensitive files or — better yet — go with full-disk encryption.

*Do as little on the road as possible. Back up your devices before leaving and while on site, save work to the cloud or a removable drive, then revert to the back-up state when you return.

(Continued above)

*Turn off Bluetooth and Wi-Fi and any applications that use them whenever you can.

*Don't charge devices at public ports, which can give outsiders access to them.

*Don't take candy (or USB drives) from strangers.

*Leave any Radio Frequency ID devices such as badges, passports or cards in your room.

*Use wired connections when available and be careful when connecting wirelessly. Wi-Fi pineapples — rogue hotspots that indiscriminately identify themselves as any network your device is looking for — can deliver you into the enemy's hands.

*Avoid sending sensitive data while on site, use your VPN at all times and when roaming use a high-speed cellular connection if possible. It's not perfect, but can be safer than Wi-Fi.

In general, be careful about anything you do online, and do as little of it as possible. If you stay safe at Black Hat, you probably will be in good shape almost anywhere you go.

Personally, I favor a ballpoint pen and a notebook (paper) when traveling. They are easy to get through airport security, difficult to hack, and my handwriting is a match for any encryption.