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 2012 - Vol 4, Issue 1

BIS Posts Advisory Opinion Guidance Document on Carbon Fiber Organic Matrix Composite Item Classification Requests

The Bureau of Industry and Security (BIS) posted an "advisory opinion" guidance document for the public to use when preparing commodity classification ("CCATS") requests for information pertaining to the development or production of carbon fiber organic matrix composite items. BIS hopes to begin building a public collection of carbon fiber organic matrix composite-related classification determinations that will be the foundation for common understandings between industry and government. The 14-page guidance document is divided into five sections:

1) Background - Classification Requests (formal determinations)

2) Purpose of Document (building a public collection of classification determinations)

3) Background - EAR Provisions Pertaining to Composite Technology (rules for determining when the export of technology is and is not "required" for purposes of ECCN 1E001)

4) Factors to Consider and Address when Drafting Composite Technology- Related Classification Requests (technology for the development or production of 1C010.e materials, 1C210 materials for 1C010.b fibers, etc.)

5) Conclusion (guidance limited to the EAR in effect at the time of publication)

BIS notes, exporters still need to refer to the EAR to determine export control obligations pertaining to any particular export; questions can be referred to (202) 482-4811.
BIS
notice: http://www.bis.doc.gov/policiesandregulations/advisoryopinions/oct25_2011_guidance.pdf

NEWSLETTER NOTES

State Department Issues Proposed Notice to Modify ITAR with New Definitions of Broker and Brokering Activities

The State Department issued a proposed rule to amend 22 CFR Parts 120, 122, 126, 127 and 129 of the International Traffic in Arms Regulations (ITAR) regarding the definitions of broker and brokering activity and related provisions. The proposed revisions are intended to clarify the scope of brokering activities, registration, prior approval and guidance, requirements and exemptions, reporting and recordkeeping, etc. The State Department is also proposing certain revisions to the DS-2032 form, the annual brokering report, and the brokering prior approval application. As reported, the proposed rule would broaden the definition of "broker" in 22 CFR 129.2 to mean any person (natural person or corporation, partnership, etc.) who engages in brokering activities. The proposed revision to the definition of "brokering activities" in 22 CFR 129.2 would more closely track its statutory definition in the Arms Export Control Act (AECA) The proposed revisions would also clearly indicate when a foreign person's brokering activities are subject to the ITAR. Full details are posted for review. Written comments on the proposed rule are due by 02/17/12.
State Dept contact: Daniel L. Cook (202) 632-2871
State Dept FR
Notice http://www.gpo.gov/fdsys/pkg/FR-2011-12-19/pdf/2011-32432.pdf

ITA Asserts That U.S. Exports Have Grown 25% Since Beginning of National Export Initiative

The International Trade Administration (ITA) highlighted its work towards accomplishing the President's National Export Initiative (NEI) goal of doubling exports by the end of 2014. The ITA reports there has been a 25 percent growth in exports since the launch of the NEI in January 2010. ITA also notes in 2011, there has been six record-breaking months of exports (January, March, April, July, August, and September).
ITA
notice: http://www.commerce.gov/blog/2011/12/16/international-trade-administration%E2%80%99s-four-big-numbers-2011

Export-Import Bank's Lending for Exports Sets Record in FY 2011

The Export-Import Bank of the United States posted its third straight record year in 2011 for financing exports from U.S. companies. According to the bank's annual report, they exceeded $32 billion in financing that supported $42 billion in exports. More than 3,600 companies employing some 290,000 workers received financing. As reported, small business financing in 2011 was $6 billion, up 70 percent since fiscal 2008. The bank financed $23 billion in infrastructure-related projects and $13.2 billion in the transportation sector. "Our financing of U.S. exports supports good-paying American jobs that sustain communities," reported Ex-Im Chairman and President Fred P. Hochberg. The bank could do even better next year if Congress agrees to increase the financial institution's lending limit.
www.joc.com (12/22/11)

WTO Develops New Application for Trade Policy Information by Countries

The World Trade Organization (WTO) posted the following notices:

The WTO has developed a new application that will allow the public to access via one portal all trade policy information notified to the WTO by its members. Known as the Integrated Trade Intelligence Portal (I-TIP), the new application will encompass tariffs, non-tariff measures and related trade statistics.
http://www.wto.org/english/news_e/news11_e/anti_14dec11_e.htm

Guess Who: The 25 Worst Passwords of 2011

GOVERNMENT COMPUTER NEWS
November 18, 2011 I

It probably won't surprise you that the most common password used online is password, followed by the ever-popular 123456. It wouldn't surprise a hacker trying to steal your personal information, either.

Security company SplashData has published its list of the worst passwords of 2011, compiled from millions of stolen passwords that hackers had posted online, according to Daily Finance.

Use of bad, easily guessed passwords has been a complaint of security experts since the dawn of the Web, but little seems to have changed. Password and the numbers 1 through 8 in varying lengths but always in order litter the list, along with gems such as qwerty, abc123 and even 111111.

This year, for some reason, words such as "monkey", "dragon" and "sunshine" also appear, along with common first names "ashley" and "michael".

Weak passwords can make life easy for hackers looking to get into your bank records and other sensitive information.

The company recommends that users use passwords of eight characters or more, mixing in letters, numbers and special characters when allowed, separate short words with spaces or underscored and don't use the same user name and password for multiple websites.

(Continued above)

But then everybody knows that. Doing it is another story. Below are SplashData's 25 worst passwords of the year:

1. password
2. 123456
3. 12345678
4. qwerty
5. abc123
6. monkey
7. 1234567
8. letmein
9. trustno1
10. dragon
11. baseball
12. 111111
13. iloveyou
14. master
15. sunshine
16. ashley
17. bailey
18. passwOrd
19. shadow
20. 123123
21. 654321
22. superman
23. qazwsx
24. michael
25. football

China and The Economic Espionage Act of 1996

STRATEGY PAGE
November 2, 2011

On October 18th, Chinese-born Kexue Huang pled guilty in an American court to stealing trade secrets from his employers (Dow Chemical Company and Cargill) and sending them to China and Germany. This was the eighth time someone was charged under the Economic Espionage Act of 1996, a law which made it a federal criminal offense to steal trade secrets. Most of these prosecutions have involved China.

Sometimes the Chinese connection is cleverly concealed. Four years ago, a Chinese engineer (Yuefei Ge) and a Chinese-American one (Lan Lee) were prosecuted for stealing military laser and communications technology, and then seeking backing from a company owned by the Chinese military, to finance the development of military equipment, based on the stolen technology. The two were tried for economic espionage, based on the 1996 Economic Espionage Act.

What was clever about Ge and Lee was that they were not stealing technology for a foreign power, but for the purpose of developing militarily useful applications of the technology. These items would then be sold to China, particularly if the Chinese came through with the research and development money. China has thus mobilized the power of venture capital to encourage their spies. Up until that point, only three people had been convicted of economic espionage, as defined by this Act, but the FBI was finding there was a lot more of it out there. The first conviction in a trial only occurred last year. Most of those caught tend to plead guilty in order to avoid a harsher sentence.

Some of these investigations are uncovering espionage efforts that have gone on for decades. Two years ago, a U.S. court convicted a Chinese born American citizen of spying for China for over 30 years. Born in China in 1936, Dongfan Chung arrived in Taiwan in 1948, and came to the United States in 1962. He then spent four decades working for aerospace firms, mainly Boeing, before he was arrested in 2006.

(Continued above)

Documents found in his home detailed his long relationship with Chinese intelligence, and his passing on technical details of the Space Shuttle (which Chung spent most of his career working on), in addition to the Delta IV satellite launcher, the F-15 fighter, B-52 bomber, CH-46/47 helicopters, and several other military systems. Chung was still working as a consultant for Boeing when he was arrested. He was sentenced to 16 years in prison, a sentence that was upheld on appeal this year.

Chung was the second person, and first American, convicted under the 1996 Economic Espionage Act. His lawyers admitted that Chung possessed thousands of classified documents in his home, but tried to make the case that he never actually transferred any of this material to Chinese intelligence. The jurors did not believe this defense.

Why Smart Phones are Targets (Popularity Up, Security Down)

GOVERNMENT COMPUTER NEWS
October 20, 2011

Smart phones and tablets will increasingly become targets for malware attacks not only because of their growing popularity but because security steps for the devices are often difficult or ignored, according to a newly released security advisory report out of Georgia Tech. "Mobile applications are increasingly reliant on the browser," said Patrick Traynor, GTISC researcher and assistant professor at the Georgia Tech School of Computer Science. "As a result, we expect more Web-based attacks against mobile devices to be launched in the coming year."

(Continued below)

The Emerging Cyber Threats Report 2012, presented at last week's Georgia Tech Cyber Security Summit 2011, focused specifically on the rise of vulnerabilities from mobile browsers and applications that are reliant on an Internet connection. In one example, researchers discussed that smart phone users aren't as aware as desktop and laptop users when a malicious link is clicked due to the smaller screen size and disappearing address bar.

Another reason is the fact that Internet security protocol information is either lacking or hard to access on mobile devices. "If you're a security expert and you want to see the [Secure Sockets Layer] certificates for a site from your mobile phone browser, it is extremely difficult to find that information -- if it's there at all," said Traynor. "And if a security expert can't verify a connection and a certificate, how do we expect the average user to avoid compromise?"

The report points to not only the lack of verification by security experts, but also the lack of overall problem solving when vulnerabilities do arise. The report cited that device constraints and "tension between usability and security" make it difficult for security experts to devote time to debug issues.

This is evident in that, unlike traditional Web browsers, mobile browsers rarely get fixes for issues that arise over time. "One of the biggest problems with mobile browsers is that they never get updated," said Dan Kuykendall, co-CEO and Chief Technology Officer for NT OBJECTives. "For most users, their operating system and mobile browser is the same as it was on the phone's manufacture date. That gives the attackers a big advantage."

Another disadvantage to mobile security is in the case of how quickly a patch or fix can be applied on the rare instances of updates. While fixes can be turned around in a matter of days for a specific vulnerability, it can take months to roll out, due to OS limitations and carrier testing and regulations, giving would-be attackers plenty of time to exploit the hole before going unpatched.

(Continued above)

Georgia Tech's security report forecasts that attacks will become more sophisticated and numerous in the next few months, especially for those targeting the Android and iOS platforms. During the study, researchers have noticed an evolution of attacks on these two mobile OSes that rival computer viruses.

"The Zeus-in-the-Mobile (ZitMo) and several other examples of Android malware are acting more like traditional bots by communicating with a command-and-control (C2) architecture," said Gunter Ollmann, Vice President of Research for Damballa, in the report. "This marks an evolution beyond premium rate fraud and other tactics that do not rely on C2, and makes mobile devices as susceptible to criminal breach activity as desktops."

While criminal breeches of tablets and smartphones and the spreading of malware are growing risks in the mobile security landscape, researchers at Georgia Tech also point to these same devices being used to spread harmful programs to desktops.

Researchers noticed an uptick of security incidents involving the upload of harmful software through a mobile device connected to a traditional PC. This attack, while not new, had previously been associated with the transfer of malware through USB devices. The threats report advises that with the growing increase of smartphone and tablet attacks, security protocols need to evolve with the attacks, especially in the enterprise setting.

"As mobile devices become an increasingly attractive target in the integrated economy, it is critical for organizations to adopt a multi-faceted strategy that leverages the right combination of security best practices with business technology requirements," said Tony Spinelli, Senior Vice President and Chief Security Officer of Equifax.

Devens Company Seeks $1.2b from Chinese Firm

BOSTON GLOBE
November 10, 2011

American Superconductor Corporation is seeking more than $1.2 billion in damages and payments for contracted shipments from its once-largest customer, a Chinese wind turbine maker accused of stealing the Devens firm's technology.

During a call with investors yesterday, American Superconductor chief executive Daniel P. McGahn said the company has filed several lawsuits in China against Sinovel Wind Group Co. of Beijing, alleging copyright infringement and theft of trade secrets.

Court and arbitration proceedings are expected to begin in the next few months, as the company tries to collect damages as well as nearly $70 million owed for past shipments ordered by Sinovel and $700 million in undelivered parts.

"We believe the strength of our cases is undeniable," McGahn said.

American Superconductor, which makes control systems for wind turbines and other advanced technologies for utilities, began to suspect Sinovel of theft in June, following the Devens company's discovery of an imperfect replica of it's software in a Sinovel wind turbine in China. Months before, the Chinese company had stopped accepting shipments of parts from American Superconductor, causing it's revenues to plunge.

An investigation eventually led the company to an engineer at an American Superconductor subsidiary in Austria, who was later found guilty of stealing proprietary software and sentenced by Austrian authorities to a year in jail. Sinovel could not be reached for comment yesterday. The Chinese company has explicitly denied stealing American Superconductor's technology, and says American Superconductor's products had become subpar and failed to meet requirements for China's power grid. It has filed a counterclaim with the Beijing Arbitration Commission against American Superconductor, alleging breach of contract.

(Continued above)

But yesterday, McGahn told investors he believes his company has strong evidence against Sinovel, including —hundreds of e-mails between senior Sinovel staff members and our now incarcerated former employee," and Chinese officials will rule in favor of American Superconductor.

"These messages give a detailed account and timetable of the crime, "McGahn said. "They show that certain senior level Sinovel employees knew that this (intellectual property) was obtained illegally."

Those details helped boost the company's stock, which rose about 11 percent to close at $4.53 per share.

Chun Sentenced for Illegally Exporting Defense Articles Without a License

U.S. DEPARTMENT OF JUSTICE
November 10, 2011

Kue Sang Chun, age 67, of Avon Lake, Ohio, was sentenced to 14 months in prison for illegally shipping components used in infrared rifle scopes to South Korea, federal law enforcement officials announced today.

Chun previously pleaded guilty to one count of exporting defense articles on the U.S. Munitions List without first obtaining an export license or written authorization from the U.S. Department of State, and one count of knowingly making and subscribing a false U.S. Individual Income Tax return.

This defendant violated important regulations designed to protect national security, ‖ said Steven M. Dettelbach, United States Attorney for the Northern District of Ohio. He did it for money and intentionally failed to pay taxes on the money he made from his crimes.

(Continued below)

Steven Anthony, Special Agent in Charge of the Federal Bureau of Investigation's Cleveland Field Office, said: Investigations surrounding the foreign acquisition of U.S. defense articles outside of legitimate channels are among the most serious matters the FBI handles. Helping to maintain the technological advantage of the U.S. defense industry and our military demands our very best effort in these regards.

Whether an individual infrared detector or 100 of them, the American public can be assured that the FBI will exhaust every available avenue to recover any item exported illegally and to hold all involved accountable," Anthony said.

Chun is a former employee at the NASA Glenn Research Center, though he is not accused of taking technology or related materials from there.

Chun, between 2000 and 2005, knowingly exported and caused the export from the United States to the Republic of Korea (South Korea) of Infra Red Focal Plane Array detectors and Infra Red camera engines which were designated as defense articles on the United States Munitions List, according to court documents. Chun did so without first obtaining an export license or written authorization for such export from the U.S. Department of State.

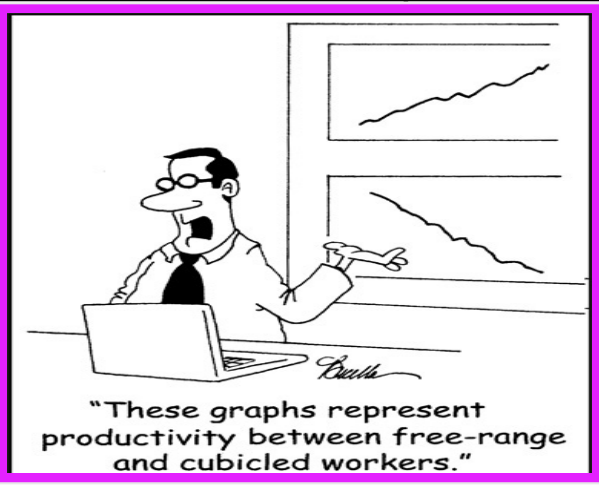
Count two charges Chun with knowingly making and subscribing a false U.S. Individual Income Tax return for the year 2005, which failed to report approximately $83,399.08 of taxable income he earned during said tax year.

Five Individuals Indicted in Fraud Conspiracy Involving Exports to Iran of U.S. Components Later Found in Bombs in Iraq: Indictment Also Alleges Fraud Conspiracy Involving Illegal Exports of Military Antennas to Singapore and Hong Kong

U.S. DEPARTMENT OF JUSTICE
October 25, 2011 WASHINGTON

Five individuals and four of their companies have been indicted as part of a conspiracy to defraud the United States that allegedly caused thousands of radio frequency modules to be illegally exported from the United States to Iran, at least 16 of which were later found in unexploded improvised explosive devices (IEDs) in Iraq. Some of the defendants are also charged in a fraud conspiracy involving exports of military antennas to Singapore and Hong Kong.

(Continued below)



Yesterday, authorities in Singapore arrested Wong Yuh Lan (Wong), Lim Yong Nam (Nam), Lim Kow Seng (Seng), and Hia Soo Gan Benson (Hia), all citizens of Singapore, in connection with a U.S. request for extradition. The United States is seeking their extradition to stand trial in the District of Columbia. The remaining individual defendant, Hossein Larijani, is a citizen and resident of Iran who remains at large.

The arrests and the indictment were announced by Lisa Monaco, Assistant Attorney General for National Security; Ronald C. Machen Jr., U.S. Attorney for the District of Columbia; John Morton, Director of the Department of Homeland Security's U.S. Immigration and Customs Enforcement (ICE); Mark Giuliano, Executive Assistant Director of the FBI's National Security Branch; Eric L. Hirschhorn, Under Secretary of Commerce; and David Adelman, U.S. Ambassador to Singapore.

Today's charges allege that the defendants conspired to defraud the United States and defeat our export controls by sending U.S.-origin components to Iran rather than to their stated final destination of Singapore. Ultimately, several of these components were found in unexploded improvised explosive devices in Iraq, said Assistant Attorney General Monaco. This case underscores the continuing threat posed by Iranian procurement networks seeking to obtain U.S. technology through fraud and the importance of safeguarding that technology. I applaud the many agents, analysts and prosecutors who worked on this extensive investigation.

These defendants misled U.S. companies in buying parts that they shipped to Iran and that ended up in IEDs on the battlefield in Iraq, said U.S. Attorney Machen. This prosecution demonstrates why the U.S. Attorney's Office takes cases involving misrepresentations regarding the intended use of sensitive technology so seriously. We hope for a swift response from Singapore to our request for extradition."

(Continued above)

One of Homeland Security Investigations' (HSI) top enforcement priorities is preventing sensitive technology from falling into the hands of those who might seek to harm American personnel or interests whether at home or abroad said ICE Director Morton. This international investigation conducted by ICE's HSI and our law enforcement partners demonstrates the importance of preventing U.S. technology from falling into the wrong hands, where it could potentially be used to kill or injure our military members and our allies. Our agency will continue to work closely through our attachés to identify these criminals, dismantle their networks, and ensure they are fully prosecuted.

This multi-year investigation highlights that acquiring property by deceit has ramifications that resonate beyond the bottom line and affects our national security and the safety of Americans worldwide, said FBI Executive Assistant Director Giuliano. We continue to work side-by-side with our many partners in a coordinated effort to bring justice to those who have sought to harm Americans. We consider this investigation as the model of how we work cases jointly with the Department of Homeland Security/Immigration and Customs Enforcement and the Department of Commerce/Office of Export Enforcement and collectively with our foreign partners to address the threats posed by Iranian procurement networks to the national security interests of the United States both here and abroad."

These cases are the product of vigorous, cooperative law enforcement focused on denying to Iran items that endanger our coalition forces on the battlefield in Iraq, said Under Secretary of Commerce Hirschhorn. We will continue aggressively to go after such perpetrators -- no matter where they operate -- to guard against these types of threats."

(Continued below)

U.S. Ambassador to Singapore, David Adelman, praised the cooperation within the U.S. executive branch agencies and with the Singaporean authorities. Twenty-first century law enforcement is most effective when countries work collaboratively as evidenced by this strong, cooperative effort between the U.S. and Singapore. Congratulations to all the officials in both our countries who made this happen, he said.

Woman Sentenced in Effort to Smuggle Scopes to Russia

NY TIMES
October 24, 2011

She would always be —the other Anna, her alleged criminal misdeeds and her personal life not quite the measure of the Anna who came before her.

But Anna Fermanova would nonetheless be linked to Anna Chapman, for reasons beyond given names. Ms. Chapman was one of 10 members of a Russian spy ring brought down by the Federal Bureau of Investigation last year. Her nights on the town and alluring photographs on Facebook enthralled the media and evoked a character out of a James Bond movie.

Ms. Fermanova was arrested in July 2010, shortly after Ms. Chapman was, for trying to smuggle night-vision weapon scopes to Russia. Ms. Fermanova, who had a similar predilection for posting stunning pictures on Facebook, became a news media darling herself, inspiring headlines like, Anna Fermanova Is America's New Sexy Russian Outlaw.

But that is where the two cases diverge. Ms. Chapman and her comrades pleaded guilty to conspiracy to act as unregistered agents and were returned to Russia less than two weeks after their arrest as part of a prisoner swap, the likes of which have not been seen since the cold war. They were hailed as heroes in Russia, where Ms. Chapman began hosting a weekly television program.

(Continued above)

Ms. Fermanova, 25, also pleaded guilty, but the prosecution and her lawyers agreed that she was not a spy. Her defense lawyer, Scott H. Palmer, said that being foolish was more like it. Ms. Fermanova was before a Federal District Court judge in Brooklyn on Monday, begging for leniency in a sentencing hearing.

Mr. Palmer said his client, with the help of her soon-to-be ex-husband, bought the scopes legally in the United States and tried to sell them illegally to men in Russia who, she believed, were hunters. Ms. Fermanova has pleaded guilty to the unlicensed export of an item on the United States Munitions List, military defense items subject to government control. I just wanted to say that I was truly sorry for what I did, Ms. Fermanova said, wiping away tears. I completely realize it was a really foolish act. It was a means to make a little extra cash. Mr. Palmer argued for a sentence of probation because, he said, Ms. Fermanova, who was born in Latvia but is a United States citizen living in Texas, did not know that the items could have slipped into the wrong hands. The recommended sentence in such a case is 46 months in prison.

As far as she is concerned, the hunters that were buying them were rich, Mr. Palmer said. The judge, Carol Bagley Amon, seemed less than sympathetic to the argument. The court recognizes that these items are not as dangerous as other items on the list, he said. But, she said, they could have easily gotten out of the hands of hunters into another stream of commerce. It is the court's view the judge added, that deporting munitions, particularly something such as night vision goggles his is a very serious offense. The sentence imposed has to promote a respect for the law. The prosecutor, Seth DuCharme, also recommended a shorter sentence, though not because the government believed the crime was not serious. Ms. Fermanova had cooperated with the government, Judge Amon said. Judge Amon ordered a sentence of four months in federal prison followed by three years of probation, including four months of being subject to home arrest. She also ordered a $1,000 fine. Ms. Fermanova must surrender by Dec. 5.

Could Hackers Steal Information and Start a Fire Using Your Printer?

GOVERNMENT COMPUTER NEWS
November 30, 2011

Networked printers have long been seen by security experts as a potential, although to date unexploited, entry point into networks.

But now a team of researchers at Columbia University's School of Engineering and Applied Science say they have discovered a flaw in certain Hewlett-Packard LaserJet printers that would make it easier for hackers to gain control of the devices, potentially stealing personal information, executing attacks on networks and even giving it instructions that might make it overheat enough to catch fire, researchers said.

Exploiting the flaw, the researchers were able to give the printer so many rapid instructions that the fuser (the device that heats up to dry the ink on the paper) got hot enough to make paper smoke, MSNBC reported.

HP at first denied any possibility of this flaw existing, citing zero customer complaints of printers being hacked by outside users. Then the company issued a statement admitting there was a security flaw and said it was working on firmware updates but that it was impossible for their printers to cause a fire. Again, HP emphasized that there have been no complaints from customers about their printers being hacked. HP may have a point about the fire part. Even in the researchers' private demonstration before several federal agencies earlier this month, a thermal switch shut the printer down before anything actually caught fire.

HP says this switch is in all of the company's LaserJet models, so none of them could start a fire that way. However, shutting down the printer this way effectively disables it, at least until certain parts are replaced. HP said the vulnerability applies to some LaserJets that are connected to the Internet without a firewall. In a private network, some printers may be vulnerable if a malicious effort is made to modify the firmware of the device by a trusted party on the network, the company said. In some Linux or Mac environments, it may be possible for a specially formatted corrupt print job to trigger a firmware upgrade."

(Continued above)

The company said it is working on a firmware upgrade and will notify customers who could be affected. Meanwhile, HP recommends putting printers behind a firewall and disabling remote firmware upload on exposed printers when possible.

Although few, if any, network attacks have ever occurred via printers, this security flaw sheds light on their vulnerability to intrusion, which could open the doorway to viruses and the like. Right now, no antivirus solution on the market could detect, let alone fix, a virus that might reside on a printer's firmware. This is something to think about.

But the real question is: If a printer were hacked like this, could it finish printing its explosive detector before catching fire? And is that dramatic irony? I always get confused about literary devices.

FBI Busts Clickjacking Ring - Could The Crime Have Been Prevented?

GOVERNMENT COMPUTER NEWS
November 10, 2011

The massive clickjacking ring the Justice Department busted this week was the kind of criminal operation that Internet overseers and the government have been aiming to prevent by increasing security in the Internet's Domain Name System. But although the protocol that would authenticate DNS queries has made its way to significant parts of the Internet, the full deployment that would make it truly effective is still a ways off.

Justice on Nov. 9 arrested six people in Estonia and issued an indictment for a seventh in Russia on charges of running a clickjacking ring that infected 4 million computers in 100 countries and netted the defendants $14 million since it started operating in 2007, the FBI said.

(Continued below)

About 500,000 computers in the United States were infected, including some at government agencies such as NASA.

The alleged crime ring, operating under the company name Rove Digital and based in Estonia, made its money by using malware called DNSChanger to redirect searches for such sites as Netflix, Apple iTunes, the IRS or the Wall Street Journal to sites that paid the defendants for the traffic. For example, the FBI said, someone clicking on a link to the iTunes store would be redirected to a sham site that purported to sell Apple software.

The DNSChanger malware changed DNS settings, routing traffic to rogue DNS servers the thieves had set up in Chicago and New York, which redirected users to malicious or unintended websites, the FBI said. The ring was broken up after a two-year investigation, dubbed Operation Ghost Click, by the FBI along with NASA's Office of Inspector General, the Estonian Police and Border Guard Board, the National High Tech Crime Unit of the Dutch National Police Agency, and a number of academic and private-sector contributors, the FBI said.

If you think your computer may have been compromised, the FBI offers detailed instructions on how you can check here, or you can ask the FBI to check it here. The Domain Name System, which underpins Internet activity, translates website names such as gcn.com and e-mail addresses to numerical IP addresses so computers can communicate with one another. Concern about its security arose in 2008 after security researcher Dan Kaminsky discovered a vulnerability that would allow for cache poisoning and for Web requests to be misdirected.

Kaminsky helped engineer a patch, but it was only a temporary fix, and the drumbeat began for widespread deployment of DNS Security Extensions, a protocol that allows DNS queries and answers to be digitally signed and authenticated, guaranteeing the origin of DNS data, data integrity, and authenticated denial of existence for an address that cannot be found.

(Continued above)

When fully deployed, DNSSEC would help prevent such malicious tactics as such as pharming, cache poisoning and DNS redirection.

DNSSEC has made steady, if slow, progress, being deployed on the root zones of top-level domains such as .com, .gov and .net as well as on the Internet's authoritative root zone. But for it to work properly, it has to be deployed throughout the Internet's domains, and that's where it has run into hurdles.

The federal government, for instance, has pushed for DNSSEC deployment, with the Office of Management and Budget setting a deadline of December 2009 for deployment on all federal systems. But in July 2011, the General Services Administration said agencies had been stuck as 50 percent deployment for a year. Among the problems agencies face are orphan websites that are outdated or have been abandoned, GSA's .gov program manager said then, adding that a White House plan to consolidate websites and eliminate duplicative sites could help.

UAV Computer Virus Might Be From Gaming Malware - Ground Control Systems for Air Force UAVs Likely Infected by Malware Used to Steal Log-ins and Passwords

DEFENSE SYSTEMS
October 14, 2011

The computer virus that worked its way into the systems used to remotely pilot the Air Force's armed unmanned aerial vehicles in September was not an intentional attack on the systems but likely a result of malware used to steal log-ins and passwords used in online gaming, the Associated Press reports.

(Continued below)

Air Force Space Command officials responsible for the service's cybersecurity efforts said Oct. 12 the virus did not invade the flight controls for the drones, but instead infiltrated the ground control systems for the drones flown remotely from Creech Air Force Base, Nev., according to the news network.

The virus came from malware that routinely tries to steal information from people who gamble or play games like Mafia Wars online, a defense official told the Associated Press on condition of anonymity. The infection was discovered on a portable hard drive used to transfer information among systems at Creech, said AFSC spokeswoman Col. Kathleen Cook.

The defense official might have been speaking generally or referring to something targeting Facebook logins if Mafia Wars is indeed involved, because computer users play the game via their Facebook account, gaming security expert Chris Boyd of GFI Software told The Register.

If that's the case, the malware might have been a phishing toolbar, according to The Register. Still, it's difficult to pin down all of the details of what occurred unless more information is released, the Register noted.

Mafia Wars maker Zynga quickly weighed in on the matter, dismissing that its product was connected with the malware that infected the Air Force's UAV systems, reports The Atlantic Wire. We actively take steps to maintain and protect the trust of our customers, including educating players about the risks associated with visiting untrusted sites and downloading untrusted applications, Zynga said in a statement.

DDTC Updates FAQs on Commodity Jurisdiction

The Directorate of Defense Trade Controls (DDTC) recently posted a version of its frequently asked questions on commodity jurisdiction (CJ) which includes new information on providing supplemental information to an already submitted CJ via e-mail. DDTC has also added a new FAQ on uploading supplemental documents to the DS-4076 submission package. As reported, DDTC has added new information to its answer for submitting supplemental information to an already submitted CJ. DDTC has also added a new FAQ on uploading supplemental documents to the DS-4076 submission package.
CJ FAQs
(10/28/11): http://pmddtc.state.gov/faqs/commodity_jurisdiction.html

FDA Issues Notice on Increased Sampling for Arsenic in Apple and Other Juices

The Food and Drug Administration (FDA) announced that it has decided to widen its look at arsenic in apple juice and other juices, as it is seeing a small percentage of individual samples tested that contain higher levels of arsenic than the 10 parts per billion limit allowed in public drinking water. FDA plans to consider all the relevant evidence and, based on this work, may set a guidance or other maximum level to further reduce arsenic in apple juice and juice products. As part of this effort, FDA will enhance surveillance in apple juice and concentrate, continue to test samples of apple juice imported into the U.S. from China, begin to sample additional types of juice and concentrate, and work with the Environmental Protection Agency (EPA) to coordinate the review of a risk assessment being prepared and discuss other steps the two agencies can take to reduce the overall levels of arsenic in the environment and in foods.
FDA notice:
http://www.fda.gov/ForConsumers/ConsumerUpdates/ucm283235.htm

U.S. Could Impose $10 Billion in Sanctions Against EU Due to Aircraft Subsidy Ruling

U.S. Trade Representative (USTR) Ron Kirk recently announced that the U.S. is requesting consultations with the European Union concerning its claim of compliance with a World Trade Organization ruling against subsidies provided by European authorities to large civil aircraft manufacturer Airbus. A USTR press release reports that the "limited information" in the EU's compliance notification to the WTO "appears to show that the EU has not withdrawn the subsidies in question and has, in fact, granted new subsidies to Airbus' development and production of large civil aircraft." In addition, the U.S. is also requesting WTO authorization to impose countermeasures in this case, which according to USTR would vary annually but in a recent period would have been in the range of $7-10 billion. USTR notes that any actual imposition of countermeasures would not occur until after further WTO proceedings, and many observers believe the dispute will never get that far. USTR Kirk said the U.S. "remains prepared to engage in any meaningful efforts, through formal consultation and otherwise, that will lead to the goal of ending subsidized financing at the earliest possible date." http://www.strtrade.com/wti/wti.asp?pub=0&story=38761&date=12%2F13%2F2011&company

ITA Issues FR Notice on Clean Energy Trade Mission to Saudi Arabia

The International Trade Administration (ITA) and the Commerce Department's U.S. and Foreign Commercial Service (FCS) and Manufacturing Services (MAS) are organizing an Executive-Led Clean Energy and Energy Efficiency Trade Mission to Saudi Arabia scheduled for April 14-18, 2012. The goal of the Mission is to promote the export of U.S. goods and services.
ITA notice: http://www.gpo.gov/fdsys/pkg/FR-2011-12-15/pdf/2011-32131.pdf

USTR Posts Report on China's WTO Compliance Issues

The Office of the U.S. Trade Representative (USTR) issued its 2011 report to Congress on China's compliance with its World Trade Organization commitments and provided testimony on its findings. USTR's major concerns include China's lack of intellectual property rights enforcement; pursuit of nationalistic policies such as subsidies, export restraints, unique standards, and indigenous innovation; lack of transparency and predictability, especially in agricultural trade; and apparent discrimination against foreign enterprises. In addition to the specific concerns laid out in the report, Assistant USTR noted in her testimony a troubling trend over the past five years in China toward intensified state intervention in the economy. She noted that increasingly, trade frictions with China can be traced to its pursuit of industrial policies that rely on trade-distorting government actions to promote or protect China's state-owned enterprises and domestic industries. As reported, China has timely implemented its tariff commitments for industrial goods each year; issued measures that bring its legal regime for making customs valuation determinations and rules of origin determinations into compliance with WTO rules; adhered to the agreed schedule for eliminating non-tariff measures; and largely brought its antidumping (AD) and countervailing (CV) duty regime into compliance with WTO rules. However, the following significant problems remain:

*Inconsistent customs procedures - implementation of customs valuation determinations has been inconsistent from port to port, both in terms of customs clearance procedures and valuation determinations;

*Import licensing compliance - there are continuing compliance issues on China's import licensing procedures such as those for iron ore imports;

(Continued below)

*Transparency of TRQs - concerns about transparency and administrative guidance have plagued China's tariff-rate quota system for industrial products, particularly fertilizer, since China's accession to the WTO;

*Fairness of AD/CV rules - China still needs to issue additional procedural guidance such as rules governing expiry reviews. It appears that China also needs to improve its commitment to the transparency and procedural fairness requirements embodied in WTO rules and avoid invoking AD/CV duties under "troubling circumstances."

USTR reports that China maintains numerous export restraints that raise serious concerns under WTO rules, including specific commitments that China made in its Protocol of Accession to the WTO. In 2011, China continued to deploy export quotas, export license restrictions, minimum export prices, export duties and other export restraints on a number of raw material inputs where it holds the advantage of being one of the world's leading producers. Through these export restraints, it appears that China is able to provide substantial economic advantages to a wide range of downstream producers in China, at the expense of foreign downstream producers, while simultaneously creating incentives for these foreign downstream producers to move their operations and technologies to China. According to the USTR, while China has revised many laws, regulations and other measures to make them consistent with WTO rules relating to Most Favored Nation (MFN) and national treatment, concerns about China's WTO compliance in the following areas:

Most Favored Nation (MFN) and national treatment, concerns about China's WTO compliance in the following areas:

*Uses taxes to discriminate against imports.
*Maintains & doesn't report subsidies.
*Still has price controls.
*Lighter enforcement for domestics.
*Unique national standards.
*Requiring in-country testing.
*Not all regulations notified.

(Continued above)

While China has timely implemented its tariff commitments for agricultural goods, a variety of non-tariff barriers continue to impede market access, particularly in the areas of Sanitary and Phytosanitary (SPS) measures and inspection-related requirements Complete details of USTR's report posted for review.

Testimony of Assistant USTR Reade before the Congressional Executive Commission on China (12/13/11) http://www.ustr.gov/about-us/press-office/speeches/transcripts/2011/december/testimony-assistant-united-states-trade-rep

USTR press release (12/12/11) http://www.ustr.gov/about-us/press-office/press-releases/2011/december/ustr-release-2011-report-congress-chinas-wto-comp

USTR notice: http://www.ustr.gov/webfm_send/3189

China Announces Anti-Dumping Duties on U.S. Autos - Retaliation for Tire Anti-Dumping Duties

As reported, China plans to impose anti-dumping (AD) duties on some vehicles imported from the U.S. after failing to block a U.S.-imposed tariff on Chinese tires. China will impose punitive duties as high as 12.9 percent for autos from General Motors and 8.8 percent for Chrysler, according to the announcement on China's commerce ministry website. Imports of BMWs and Mercedes Benzes produced in U.S. plants will face duties of 2 percent and 2.7 percent respectively. The move comes three months after the World Trade Organization rejected China's appeal of a ruling backing U.S. duties on tire imports. The taxes affect vehicles with engines that are more than 2.5 liters. China currently imposes tariffs of 25 percent on imported cars. www.joc.com (12/14/11)

CBP Posts Fact Sheet on Benefits to Importers of ACE Portal Account

U.S. Customs and Border Protection (CBP) issued a fact sheet inviting importers to take part in the many advantages of establishing an Automated Commercial Environment (ACE) portal account. Benefits of an importer ACE portal account include access to numerous reports, improved communications with CBP and a consolidated management approach facilitated by the tracking of import activity in a single, comprehensive, account based view. Additional benefits for importers include:

*Periodic Monthly Statement for Duties and Fees

*Transition to an interest-free monthly statement process from a transaction-by-transaction payment process

*Pay for eligible shipments released during a month by the 15th working day of the following month for your account on either a national or a port monthly statement including compliance, transactional and financial data such as:

*Access over 125 reports on company specific compliance, transactional and financial data

*Schedule large customized bulk data download reports

*Review CBP entry summary data in near real-time

*Review the status of your bills of lading refreshed every two hours

*In the future share customized reports with all users within your account who have access to reports

*Link to the Importer Security Filing Portal to view ISF reports and for importers who file infrequently the ability to file up to 12 ISFs annually through the ISF Portal.

(Continued above)

Account Management options available including:

*Create an account based on your company's organizational structure and restrict user access to select account information

*Offer cross account access to other ACE portal accounts (e.g., brokers) while maintaining control over access privileges

*View, sort, and print account lists by name and number; create CBP Form 5106 (Importer ID Input Record) information; and access an expanded number of reference files, including port and country codes and Manufacturer ID

*Attach electronic information (e.g., pdf, Word, Excel, etc.), track or respond to CBP on compliance and operational issues via the Business Activity Log

*Respond to a CBP Form 28, 29, and 4647 via the Portal for both ACS and ACE entry summaries.

*Create blanket declarations via the Portal

*View and search bond information

*Search, display and print AD/CVD case information and AD/CVD messages

*Record and track the life cycle of an AD/CVD case by accessing important case information such as duty deposit rates, entry summary suspension status, bond / cash status, administrative review information and events related to the case history (e.g., "Initiation," "Preliminary," "Final," "Order," "Terminated").

*Access AD/CVD messages with additional useful information in one easy location such as additional message header data elements (e.g., "message status," "Federal Register Notice cite," "Federal Register Notice publication date," "court order number")
CBP Importer Fact Sheet (12/14/11)http://www.cbp.gov/xp/cgov/newsroom/fact_sheets/trade/ace_factsheets/ace_overview/importers_fact_sheet.xml

FDA Posts Presentation on Entry Process, Detention, and Sampling

The Food and Drug Administration (FDA) posted a presentation with a broad overview of its import operations and how it regulates imported products. It describes in general terms the statutory authority of Section 801 of the Federal Food Drug & Cosmetic (FFD&CA), FDA's entry review process, detentions, examinations and sampling, refusal of admission, etc. According to the FDA, Section 801 of the FFD&CA on imports and exports provides FDA with its general statutory authority to refuse admission to imported FDA-regulated products. FDA has this authority if it appears from the examination of the article or otherwise that it:

*has been manufactured, processed, or packed under insanitary conditions; or

*is forbidden or restricted in sale in the country in which it was produced; or

*is adulterated (such as by containing a substance that makes a product inferior, impure, not genuine, etc.), misbranded (falsely or misleadingly labeled), or in violation of section 505 (New Drugs).

FDA notes that the "or otherwise" part of this authority means that FDA can also refuse admission based on historical data or information or evidence from other sources. FDA remains that refused products must either be exported or destroyed and that civil penalties apply if they are not. In addition, FDA notes that it also has the authority to seize products and then seek their destruction through court order if certain conditions are met.
FDA notice:
http://www.fda.gov/downloads/AboutFDA/Transparency/Basics/UCM281623.pdf

CBP Issues FR Notice Seeking Comments on NAFTA Certificate of Origin Information Collection

U.S. Customs and Border Protection (CBP) is requesting comments by 02/07/12, on an existing information collection on the NAFTA Regulations and Certificate of Origin (CBP Forms 434 and 446). CBP is proposing to extend the expiration date of these forms and to add CBP Form 447. The CBP Form 434, NAFTA Certificate of Origin, is used to certify that a good being exported either from the U.S. into Canada or Mexico or from Canada or Mexico into the U.S. qualifies as an originating good for purposes of preferential tariff treatment under the NAFTA. This form is completed by exporters and/or producers and furnished to CBP upon request. CBP Form 434: http://forms.cbp.gov/pdf/CBP_Form_434.pdf

In addition, the CBP Form 446, NAFTA Verification of Origin Questionnaire, is a questionnaire that CBP personnel use to gather sufficient information from exporters and/or producers to determine whether goods imported into the U.S. qualify as originating goods for the purposes of preferential tariff treatment under NAFTA. CBP Form 446: http://forms.cbp.gov/pdf/CBP_Form_446.pdf

CBP is also seeking approval of CBP Form 447, NAFTA Motor Vehicle Averaging Election, in order to gather information required by 19 CFR 181 Appendix, Section 11(2), "Information Required When Producer Chooses to Average for Motor Vehicles." This form is provided to CBP when a manufacturer chooses to average motor vehicles for the purpose of obtaining NAFTA preference. CBP has requested comments from the general public and other Federal agencies on:

*whether the collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility;

(Continued below)

*the accuracy of the agency's estimates of the burden of the collection of information;

*ways to enhance the quality, utility, and clarity of the information to be collected;

*ways to minimize the burden including the use of automated collection techniques or the use of other forms of information technology; and

*the annual cost burden to respondents or record keepers from the collection of information (total capital/startup costs and operations and maintenance costs).
CBP Contact – Tracey Denning (202) 325-0265
CBP FR Notice:
http://www.gpo.gov/fdsys/pkg/FR-2011-12-09/pdf/2011-31668.pdf

DHS Posts Information on Proposed United States/Canada Border Action Plan

Details of the "Beyond the Border" Action Plan agreed to by President Obama and Prime Minister Harper on 12/7/11 have been posted. The plan includes specific actions and 2012-2014 target dates to achieve goals such as:

*common data elements for advance cargo screening;

*mutual recognition of air cargo security programs for passenger aircraft;

*attempted alignment of Canada's Customs Self Assessment (CSA) and the U.S. Importer Self Assessment (ISA) programs; and

*assessment on ways to move wood packaging material inspections away from the border.

(Continued above)

The U.S. and Canada will work to develop a harmonized approach to screening inbound cargo arriving from offshore that will result in increased security and the expedited movement of secure cargo across the U.S.–Canada border, under the principle of "cleared once, accepted twice." This work will include the following elements:

*Mutual Recognition of Air Cargo Security Programs for Passenger Aircraft by March 2012

*Implement Common Data Elements for Advance Cargo Screening, Etc. by 2013

*Implement Integrated Cargo Security Strategy Based on Risk in 2014

The U.S. and Canada anticipate that the pilots will inform the ICCS, which they expect to begin implementing in 2014. Depending on the results of a study they will conduct on wood packaging material (WPM), inspections of such material at the perimeter could also be included in the ICSS. In addition, the two countries will work toward adopting a common framework for trusted trader programs that will align requirements, enhance member benefits, and provide applicants with the opportunity to submit one application to multiple programs. Full details have been posted for review.
DHS notice:
http://www.dhs.gov/xlibrary/assets/wh/us-canada-btb-action-plan.pdf

Homeland Security

BIS Issues Final Rule Amending EAR for Syria Controls

The Bureau of Industry and Security (BIS) issued a final rule, effective 12/12/11, which amends the Export Administration Regulations (EAR) by moving the substantive provisions of the comprehensive sanctions on Syria from General Order No. 2 in Supplement No. 1 to 15 CFR Part 736 to a revised 15 CFR 746.9. The final rule also makes conforming changes to the Export Administration Regulations. According to BIS, this rule will facilitate compliance with the comprehensive sanctions on Syria.
BIS contact – Director, Foreign Policy Division (202) 482-4252
BIS notice (FR Pub 12/12/11)
http://www.gpo.gov/fdsys/pkg/FR-2011-12-12/pdf/2011-31682.pdf

DHS Posts OIG Report on CBP Issues with ISA and STBs

The Department of Homeland Security's Office of Inspector General (OIG) issued a November 2011 report identifying the major management and other challenges the department faces. As reported, U.S. Customs and Border Protection's (CBP's) lack of oversight tools to ensure that participants in the Importer Self-Assessment (ISA) program comply with federal requirements; and CBP's lack of controls over the Single Transaction Bonds (STB) process. In addition, challenges also remain with agencies' examination of high-risk cargo. CBP revenue remains the second largest source of revenue for the U.S. government. In fiscal year 2010, CBP collected an estimated $32 billion in duties, fees, and taxes (revenue), an increase of 9.5% over FY 2009. OIG reported that in the current economic environment, it is imperative CBP ensure that importers comply with federal trade requirements and that government revenues are protected.

(Continued above)

OIG has concluded that issues with the targeting and examination of high-risk shipments continue to be challenge. Recommendations include:

*Updated exam guidance needed;

*More funding needed;

*Covert test finds passenger aircraft cargo vulnerable;

*Unqualified highway carriers receiving the Free and Secure Trade (FAST) program benefits;

*Customs and Trade Partnership against Terrorism (C-TPAT) supply chain security specialists has not always followed established procedures when determining the initial eligibility of highway carriers.

OIG's report also highlights challenges with CBP's Western Hemisphere Travel Initiative (WHTI), overseas screening of foreign nationals, information technology management, etc. See full report for details.
DHS report (OIG-12-08, November 2011)
http://www.oig.dhs.gov/assets/Mgmt/OIG_12-08_Nov11.pdf